O‘ZBEKISTON RESPUBLIKASI
OLIY TA’LIM, FAN VA INNOVATSIYALAR VAZIRLIGI

MUHAMMAD AL-XORAZMIY NOMIDAGI TOSHKENT AXBOROT TEXNOLOGIYALARI UNIVERSITETI

N.N.SAFOYEV, M.K.SEIDULLAYEV, M.SH.RADJABOVA, B.B.TURDIBEKOV

KIBERXAVFSIZLIK SIYOSATI

(O‘quv qo‘llanma)

O‘zbekiston Respublikasi Oliy ta’lim, fan va innovatsiyalar vazirligi tomonidan oliy o‘quv yurtining “5330300 – Axborot xavfsizligi (sohalar bo‘yicha)” ta’lim yo‘nalish talabalari uchun o‘quv qo‘llanma sifatida tavsiya etilgan

TOSHKENT- 2023

UO‘K: 000(000)
KBK 00.00
M00

N.N.Safoyev, M.K.Seidullayev, M.Sh.Radjabova, B.B.Turdibekov Kiberxavfsizlik siyosati. O‘quv qo‘llanma. 2023. – 252 b.

O’quv qo‘llanma kiberxavfsizlikni ta’minlash sohasida siyosat tushunchasining dolzarbligi va uning ahamiyati kabi muhim masalalarini ko‘rib chiqishga bag‘ishlangan bo‘lib, axborot tizimlari va texnologiyalaridagi ma’muriy, apparat va dasturiy ta’minotda qo’llaniladigan siyosatlarni yoritib beradi. Xususan, o’quv qo’llanmada kiberxavfsizlik tushunchasi, evolyutsiyasi, maqsadlari, qaror qabul qiluvchilar uchun zarur hujjatlar va kataloglar, kiberxavfsizlik siyosatini ishlab chiqishda xalqaro yondashuvlar, milliy qonunchilik, kiberxavfsizlikni ta’minlashda geopolitikaning ahamiyati, kiberxavfsizlik siyosatini amalga oshirish va rivojlantirish masalalari, korporatsiya, jismoniy shaxslar va huquqni muxofaza qilish organlarining kiberxavfsizlikni ta’minlashdagi o’rni, axborot tizimlari va ularni boshqarish jarayonlaridagi siyosatlar, kiberxavfsizlik vositalari, xodimlarni kiberxavfsizlik bo’yicha o’qitish kabi qator masalalar keltirib o‘tilgan.

O‘quv qo‘llanma 5330300 – Axborot xavfsizligi (sohalar bo‘yicha) yo‘nalishida tahsil olayotgan bakalavrlarga mo‘ljallangan bo‘lib, faoliyati axborot xavfsizligini ta’minlash bilan bog‘liq bo‘lgan keng doiradagi mutaxassislar xam foydalanishlari mumkin.

UO‘K: 000(000)
KBK 00.00

Taqrizchilar:

X.K.Samarov – Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universitetining “Axborot xavfsizligi” kafedrasi t.f.n. dotsenti.

N.B.Nasrullayev – Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti Nurafshon filiali direktori vazifasini bajaruvchi, Ph.D., dotsent.

ISBN 987000-000-0000

MUNDARIJA

Kirish

Texnologiya hayotimizning barcha jabhalariga kirib borayotgan bugungi raqamli asrda axborot va axborot tizimlari xavfsizligi birinchi o‘ringa chiqdi. Texnologiyalarning jadal rivojlanishi ko‘plab foyda keltirishi bilan birgalikda, balki bizni yangi va rivojlanayotgan tahdidlarga xam duchor qildi. Natijada, samarali kiberxavfsizlik siyosatiga bo‘lgan ehtiyoj hech qachon bugungidek katta bo'lmagan.

Ushbu o’quv qo’llanma kiberxavfsizlik siyosatining murakkab sohasini tushunish va uni amaliyotga joriy etishdagi qator savollarga javob topishga harakat qiladigan qo‘llanma bo‘lib xizmat qiladi. Bu sizga kiberxavfsizlik siyosatini ishlab chiqish va amalga oshirish tamoyillari, amaliyotlari va muammolarida mustahkam asos yaratish uchun ishlab chiqilgan. Kiberxavfsizlik siyosati sohasi dinamik va doimo rivojlanib bormoqda. Ya‘ni, yangi tahdidlar paydo bo‘lmoqda, texnologiyalar rivojlanib bormoqda va albatta qoidalar xam yangilanib bormoqda. Ushbu o‘quv qo‘llanma sizni ushbu o‘zgarishlarga moslashish uchun zarur bo‘lgan bilim va ko‘nikmalar bilan ta’minlash hamda mustahkam va samarali kiberxavfsizlik siyosatini ishlab chiqishga tayyorlashga yordam beradi.

Ushbu o‘quv qo‘llanma texnologik fan hisoblansada, milliy va xalqaro huquqiy sohalar, geopolitika, menejment va boshqa turdagi fanlar bilan o‘zaro bog‘liqlikda ishlab chiqilganligini ko’rishingiz mumkin. Kiberxavfsizlik asoslari va siyosatni ishlab chiqish tamoyillaridan tortib, risklarni boshqarish, huquqiy va ahloqiy mulohazalar va xalqaro hamkorlikgacha kiberxavfsizlik siyosatining ko‘p qirrali mohiyatini har tomonlama tushunishga yordam beradi. Shuningdek, bu sohada ishlayotgan mutaxassislar, siyosatchilar va raqamli dunyomiz xavfsizligini ta‘minlashda kiberxavfsizlik siyosatining muhim rolini tushunishga qiziqqan har bir shaxs uchun manba sifatida xam ishlatilishi mumkin.

O‘rganish tajribangizni oshirish uchun mavzular real hayotiy misollarni, xalqaro tajriba va yondashuvlarni va fikrlashga undaydigan savollarni o’z ichiga oladi. Ushbu elementlar siz o‘rgangan tushunchalarni qo‘llashga yordam beradi va turli kontekstlarda kiberxavfsizlik siyosati qanday ishlashi haqida amaliy tushunchani rivojlantiradi.

Respublikamizda ham davlat, ham xo‘jalik boshqaruvida axborot texnologiyalari taraqqiyoti davom etar ekan, axborot xavfsizligini ta’minlashga alohida e’tibor qaratilmoqda. Bu e’tibor turli

tashabbuslarda, jumladan, O‘zbekiston Respublikasi Prezidentining 2017-yil 8-fevraldagi “Qonun hujjatlarini tarqatish tizimini tubdan takomillashtirish chora-tadbirlari to‘g‘risida”gi qarorida xam yaqqol namoyon bo‘lmoqda. Bundan tashqari, 2017-2021-yillarda O‘zbekiston Respublikasini yanada rivojlantirish bo‘yicha Harakatlar strategiyasida axborot xavfsizligini ta’minlash masalasiga alohida e’tibor qaratilgan bo‘lib, axborotni himoya qilish tizimini takomillashtirish, axborot sohasidagi tahdidlarga tezkor va munosib javob berishga alohida e’tibor qaratilgan. Shubhasiz, bu vazifalarni muvaffaqiyatli amalga oshirish siyosatimizning hal qiluvchi, ya’ni ustuvor yo‘nalishi bo‘lib xizmat qiladi.

Ushbu o‘quv qo‘llanma 5330300 – “Axborot xavfsizligi” mutaxassisligi bo‘yicha tahsil olayotgan bakalavrlar uchun tavsiya etilgan bo‘lib, faoliyati axborot xavfsizligini ta’minlash bilan bog‘liq bo‘lgan keng doiradagi mutaxassislar xam foydalanishlari mumkin.

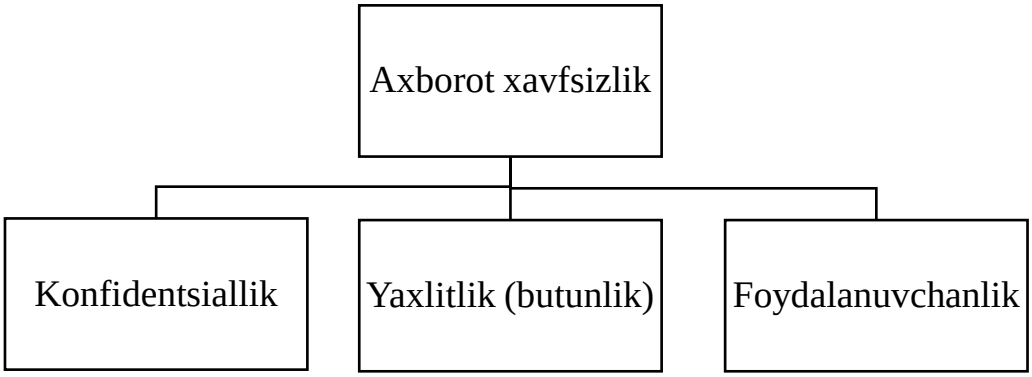
I BOB. KIBERXAVFSIZLIK SIYOSATI HAQIDA UMUMIY MA’LUMOTLAR

1.1-§. Kiberxavfsizlik siyosati tushunchasi va fanga kirish

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.

Hatto xavfsizlik soxasida ishlaydigan shaxslar ham, ular shaxsan o‘zaro aloqada bo‘lgan kibermakon jihatlariga qarab kiberxavfsizlikka boshqacha qarashadi. Tizim jismoniy ob’ekt bo‘ladimi yoki kibermakon komponentlari to‘plami bo‘ladimi, ushbu tizimga tayinlangan xavfsizlik bo‘yicha mutaxassisning roli potentsial hujumni rejalashtirish va uning oqibatlariga tayyorgarlik ko‘rishdan iborat. Garchi “kiber” so‘zi asosan xalq tilida bo‘lsa-da, uning aniq nimani anglatishini tushunish qiyin. Bir paytlar kibernetika deb nomlanuvchi kompyuter boshqaruvi va aloqaning o‘sha vaqtda paydo bo‘lgan soxasiga asoslangan ilmiy fantastika atamasi, hozirda esa elektron avtomatlashtirishni anglatadi.

Tizimlar o‘z vazifalarini bajarishi uchun 3 ta operator belgilangan tartiblarga rioya qilishlari kerak. Xavfsizlikka tatbiq etilganda, bu uchlik xavfsizlikka faqat xavfsizlik mutaxassislari tomonidan erishilmasligini, shuningdek, kiberxavfsizlikni faqat texnologiya bilan amalga oshirish mumkin emasligini ta’kidlaydi. Himoya qilinishi kerak bo‘lgan tizim yoki tashkilot qarorlari va harakatlari xavfsizlik dasturlari muvaffaqiyatida muhim rol o‘ynaydigan boshqa insoniy elementlarni o‘z ichiga olishi lozim. Agar bu odamlarning barchasida o‘zini xavfsiz tutish uchun motivatsiya va qiziqish bo‘lsa ham, ular oldindan rejalashtirilgan jarayonsiz zararni oldini olish, aniqlash va tiklash uchun birgalikda qanday harakat qilishni bilishmaydi. Shunday qilib, xavfsizlik bo‘yicha mutaxassislar mavjud tashkiliy jarayonlarga xavfsizlik dasturlarini kiritishlari va kiberxavfsizlik maqsadlarini qo‘llab-quvvatlash uchun texnologiyadan strategik foydalanishlari lozim.



1.1-rasm. Axborot xavfsizligi maqsadlari

Axborotga xos bo‘lgan xavfsizlik maqsadlariga quyidagilar qaratilgan:

1. Konfidentsiallik;
2. Yaxlitlik (butunlik);
3. Foydalanuvchanlik.

Konfidentsiallik – Mazkur qoidalar axborotni faqat qonuniy foydalanuvchilar tomonidan “o’qilishini” ta’minlaydi va tizim ma’lumotlarining tarqalishini ruxsat etilgan foydalanish bilan cheklash qobiliyati tushuniladi.

Yaxlitlik (butunlik) – qayd etilgan va xabar qilingan ma’lumotlarning haqiqiyligi, to‘g‘riligi va manbasini saqlab qolish qobiliyatini anglatadi, ya’ni, axborotni ruxsat etilmagan o’zgartirishdan yoki “yozish” dan himoyalashdir.

Foydalanuvchanlik – funktsional imkoniyatlarni o‘z vaqtida yetkazib berishni anglatgan holda ma’lumotni aniq va ishonchli ekanligiga ishonch hosil qilish, ma’lumot, axborot va tizimdan foydalanishning mumkinligi, ya’ni, ruxsat etilmagan “bajarish” dan himoyalashdir.

Axborot xavfsizligini ta’minlashning ushbu maqsadlari kompyuterlar paydo bo‘lishidan oldin ham axborotga nisbatan qo‘llanilgan, ammo kiberfazoning paydo bo‘lishi maqsadlarga erishish usullarini, shuningdek, maqsadga erishishning nisbiy qiyinligini o‘zgartirdi. Konfidentsiallik, yaxlitlik (butunlik), foydalanuvchanlikni qo‘llab-quvvatlaydigan texnologiyalar ko‘pincha bir-biriga zid keladi. Masalan, kibermakonda ma’lumotlarning yuqori darajada mavjudligiga erishishga qaratilgan harakatlar ko‘pincha ma’lumotlarning maxfiyligini saqlashni qiyinlashtiradi.

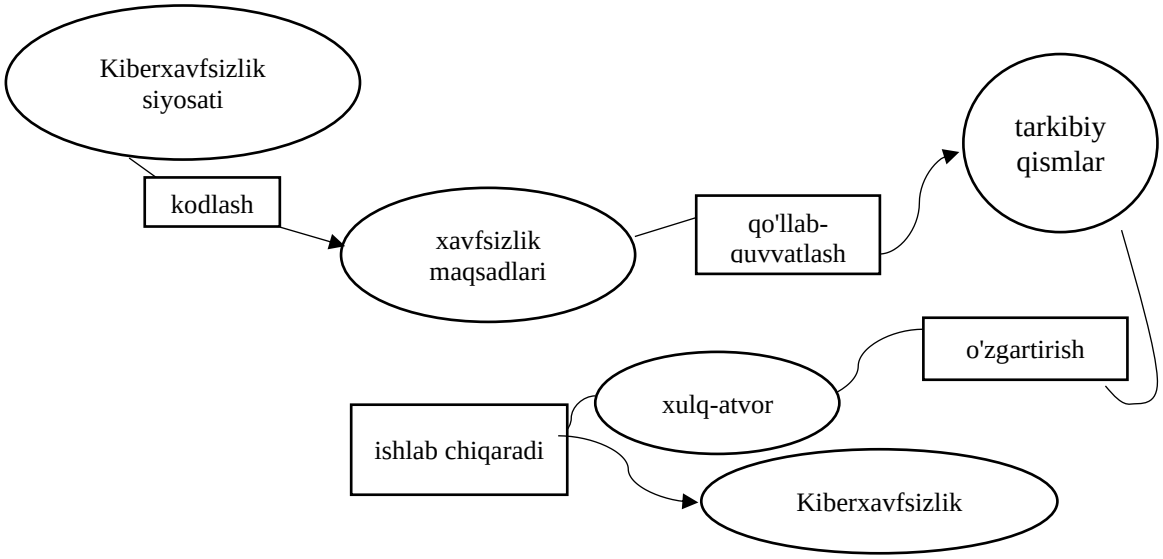
Muayyan tizimdagi ma’lumotlarning har bir turi uchun konfidentsiallik, yaxlitlik (butunlik) va foydalanuvchanliknimani nimani anglatishini saralash kiberxavfsizlik bo‘yicha mutaxassisning ixtisosligi

hisoblanadi. Kiberxavfsizlik, umuman olganda, kibermakondagi ma’lumotlarning konfidentsiallik, yaxlitlik (butunlik), foydalanuvchanliliga yetkazilgan zararning oldini olish, aniqlash va tiklash uchun odamlar, jarayonlar va texnologiyalardan foydalanish usullarini anglatadi.

Kibermakon butun jamiyatda mahsuldorlikni oshirib, ma’lumotni o‘z vaqtida samarali tarqatdi. Qaysi sohada yoki qaysi dasturda kibermakon joriy etilishidan qat’i nazar, samaradorlikni oshirish asosiy e’tiborda bo‘ladi. Axborotni kibermakonga tez yetkazib berish ko‘pincha umumiy tizim xavfsizligini pasaytiradi. Hosildorlikni oshirish bilan shug‘ullanuvchi mutahassislar uchun xavfsizlik choralari ko‘pincha foydalanuvchi kirishini kamaytiradigan, to‘xtatuvchi yoki kechiktiradigan oldini olish choralari, muhim tizim resurslarini sarflaydigan aniqlash choralari va boshqaruv e’tiborini tizim xususiyatlaridan chalg‘itadigan javob talablari tufayli taraqqiyotga bevosita zid bo‘lib tuyuladi.

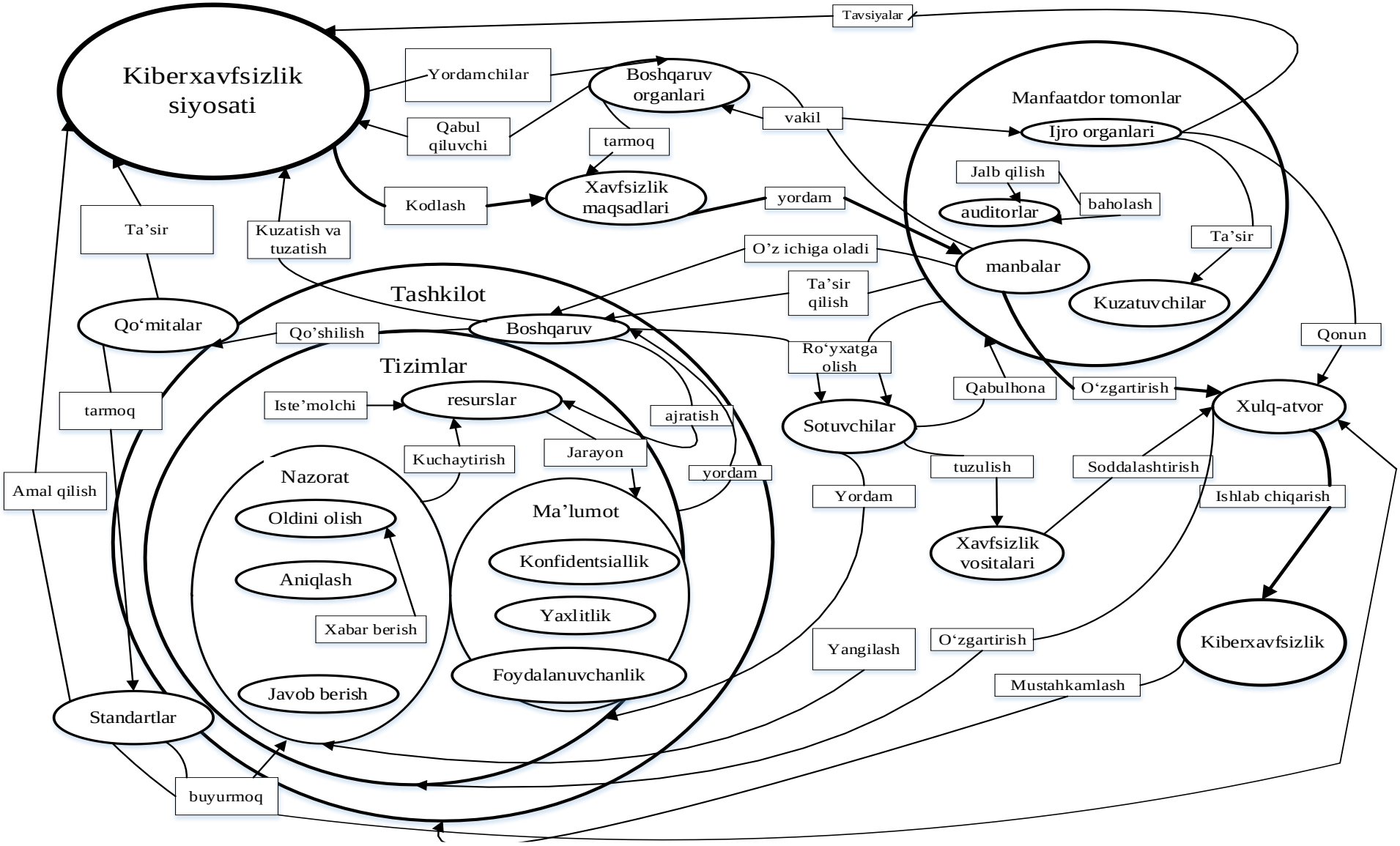
“Siyosat” so‘zi kiberxavfsizlik bilan bog‘liq bo‘lgan turli vaziyatlarga nisbatan qo‘llaniladi. U axborotni tarqatish, axborotni himoya qilish bo‘yicha xususiy korxona maqsadlari, texnologiyani boshqarish uchun kompyuter operatsiyalari usullari va elektron qurilmalardagi konfiguratsiya o‘zgaruvchilari bilan bog‘liq qonun va qoidalarga murojaat qilish uchun ishlatilgan. Ammo adabiyotlarda kiberxavfsizlik siyosati iborasini ishlatishning ko‘plab boshqa usullari mavjud. “Kibermakon” atamasida bo‘lgani kabi, yagona ta’rif mavjud emas, lekin kiberxavfsizlik atamasi siyosat sifatida qo‘llanilganda umumiy mavzu sifatida qo‘llaniladi.

Ushbu qo‘llanmaning maqsadi o‘quvchiga mavzuni va uning hosilalarini tushunish va fikrlash uchun yetarli ma’lumot berishdadir. Uni o‘qiganlar kiberxavfsizlik siyosatining ko‘p turlarini ishonchli tarzda ochishlari kerak. Umuman olganda, “kiberxavfsizlik siyosati” atamasi kiberxavfsizlikni ta’minlash uchun mo‘ljallangan ko‘rsatmalarga ishora qiladi.



1.2-rasm. Kiberxavfsizlik siyosatining ta’rifi.

Asosiy tayanch oddiy odamlarning kontseptsiyaga bo‘lgan nuqtai nazarini egallashi kutilmoqda. Aniqlanishi kerak bo‘lgan kontseptsiyaning boshqa istiqbollari murakkab kontseptsiyaning qo‘shimcha istiqbollari sifatida ifodalanishi mumkin. 1.2-rasmda kiberxavfsizlik siyosati kiberxavfsizlikni yaratish siyosatiga muvofiq o‘z xatti-harakatlarini o‘zgartirishi kutilayotgan tarkibiy qismlarni qo‘llab-quvvatlash uchun xavfsizlik maqsadlarini kodlaydigan muhim jihat sifatida taqdim etilgan. 1.3-rasmda kiberxavfsizlik siyosatidagi turlicha qarashlarni birlashtirilgan holda, kontseptsiyani aks ettiradi. Garchi barcha qo‘shimcha tugunlar va havolalar kiberxavfsizlik siyosatining ta’rifi doirasida bo‘lmasa-da, ular 1.2- rasmdagi tizimligrammaning asosiy qismida ko‘rsatilgan doirani tushunish imkonini beradi. 1.3-rasmda “boshqaruv organlari” tuguniga havolalar kiberxavfsizlik siyosati xavfsizlik maqsadlariga erishish usuli sifatida boshqaruv organlari tomonidan qabul qilinishini ko‘rsatadi. Bu raqam ataylab umumiydir, chunki boshqaruv organlari ko‘pincha ular boshqaradigan tashkilotlardan tashqarida mavjuddir. Masalan, 1.3-rasm



1.3-rasm. Kiberxavfsizlik siyosati istiqbollari

E’tibor bering, 1.3-rasmda ko‘rsatilganidek, siyosatning roli kiberxavfsizlikka erishish kutilayotgan xatti-harakatlar qoidalarini belgilash uchun asos yaratishdir. Turli xil siyosat bayonotlari va tegishli qoidalarga ega bo‘lgan juda ko‘p kiberdomenlar mavjud. Ushbu domenlar 1.3-rasmda batafsil tavsiflangan.

Kiberxavfsizlik maqsadlari bevosita xulq-atvorga tayanmaydi, biroq kiberxavfsizlik maqsadlariga asoslangan kiberxavfsizlik strategiyasi yanada yaxshi kiberxavfsizlik siyosati bilan yakunlanishi kutilmoqda. Tashkilotlar texnologiya nazorati va tegishli operatsion jarayonlarni amalga oshirish uchun standartlar yaratadi va tarkibiy qismlar siyosatga rioya qilish uchun ushbu standartlardan foydalanadi. Standartlarning o‘zi siyosat emas. Aksincha, ular siyosat maqsadlarida texnologiyalar va operatsion jarayonlar to‘plamiga ishoradir. Agar standart siyosatga muvofiqlikka qaratilgan bo‘lsa, u siyosatga muvofiqlikni ta’minlaydigan jarayon va texnologiya konfiguratsiyasi kombinatsiyasini belgilaydi. Biroq, siyosatning biron bir aniq maqsadiga yo‘naltirilmagan standartlar chiqarilishi mumkin va siyosatlarda tegishli standartlar bo‘lmasligi mumkin.

Kiberxavfsizlik siyosati istiqbollari. “Majburiy organlar” tugunidan kelib chiqadigan aloqalar siyosatni qo‘llash organlarining rolini ko‘rsatadi, ular qonun-qoidalarni o‘rnatadilar, nafaqat ta’sischilarning xatti-harakatlariga ta’sir qiladi, balki boshqalarga ham ta’sir qiladi va shu bilan siyosatning manfaatdor tomonlariga aylanadigan jarayondir. Eng chap tomondagi havolalar boshqaruv organlari tomonidan siyosatga rioya qilishga majbur bo‘lgan tashkilotlar rahbariyati tomonidan o‘rnatiladigan standartlarning rolini tan oladi. “Sotuvchilar” deb belgilangan tugundan chiqadigan havolalar xavfsizlik siyosatiga muvofiqlik vositalarini taqdim etuvchi va mahsulotlar va xizmatlar bilan tizim xavfsizligini qo‘llab-quvvatlovchi sotuvchilarga ta’sir ko‘rsatadigan va ta’sir qiladigan tarkibiy qismlar va boshqaruvning sotuvchi munosabatlarini tasvirlaydi.

“Tashkilotlar” tugunidagi va unga tutashadigan tugunlar va bog‘lanishlar klasterlari siyosatga bo‘ysunadigan tashkilotga ishora qiladi. Bu shuni ko‘rsatadiki, bunday tashkilotlar boshqaruv organlari tomonidan e’lon qilingan kiberxavfsizlik siyosatlariga rioya qilishadi, shuningdek, o‘zlarining ichki kiberxavfsizlik siyosatlarini o‘rnatadilar. Bundan tashqari, tashkilot boshqaruvi xavfsizlik siyosati ta’siri ostida bo‘lgan tizimlar tomonidan qo‘llab-quvvatlanayotganini ko‘rsatadi.

“Tizimlar” tugunlari xavfsizlikni boshqarish va tizim resurslari

o‘rtasidagi o‘zaro bog‘liqlikni ta’kidlab, kibermakonni boshqarish uchun ishlatiladigan tizimlarga ishora qiladi. Bu xavfsizlikni boshqarish vositalariga ajratilgan tizim resurslari va axborotni qayta ishlash uchun zarur bo‘lgan resurslar o‘rtasida o‘zaro kelishuv mavjudligini ko‘rsatadi; ya’ni tizimlar faoliyatiga xavfsizlikni nazorat qilish jarayonlari qanchalik ko‘p integratsiya qilinsa, resurslarni yo‘qotish xavfsizligi shunchalik kam bo‘ladi. Ichki tashkiliy kiberxavfsizlik strategiyasining odatiy maqsadi hujjatlashtirilgan siyosatdan bunday qarorlar qabul qilinganligi to‘g‘risida xabardorlikni yaratish uchun aloqa vositasi sifatida foydalanib, ushbu kelishuvni optimallashtirishdir.

Qonunlar va qoidalar. Har bir davlatning kiberxavfsizlik siyosati hozirda milliy xavfsizlik siyosatining quyi qismi hisoblanadi. Davlatning kiberxavfsizlik siyosati tashqi siyosat yoki iqtisodiy siyosat bilan bir xil tarzda hisoblangan bo‘lsa ham, bu siyosatlar qonun bilan bir xil kuchga ega emas. Aksincha, siyosatlar hisobotlar va nutqlar, suhbatlar va muzokaralar orqali o‘rnatiladi va ifodalanadi. Siyosat qanday qonunlar va qoidalarni ko‘rib chiqish kerakligi haqida qaror qabul qilish uchun ishlatiladi. Bu qonunlar va qoidalarning o‘ziga tegishli emas. Albatta, dunyoda shartnomalar, qonunlar va qoidalar eng yaxshi va oqilona o‘ylangan siyosatni aks ettiradi. Shunga qaramay, kiberxavfsizlik siyosatini umuman ifodalamasdan turib kiberxavfsizlik bo‘yicha ijro direktivalari, qonunlari va qoidalariga ega bo‘lish mumkin. Masalan, Xitoy milliy davlat operatsiyalari uchun muhim bo‘lgan kiberkosmos faoliyati nazorat qilinishi kerakligi haqidagi siyosatni aniq belgilab qo‘ydi. Ushbu siyosatda Internet iqtisodiyot va davlat manfaatlariga xizmat qilishi aniq belgilab qo‘yilgan. Siyosat Xitoy hukumati telekommunikatsiya vositalarini ajratish, kuzatish va nazorat qilish, shuningdek, o‘z manfaatlariga zid deb aniqlagan internet saytlariga kirishni bloklash imkonini beruvchi qonun va qoidalarga olib keldi.

Hukumatning kiberxavfsizlik siyosati ishlab chiqilganmi yoki yo‘qmi, uning kiberxavfsizlik qoidalari boshqaruv doirasi bilan chegaralanadi. Ya’ni, hukumatning filiali yoki agentligi har qanday davlat miqyosidagi tartibga solish doirasida bo‘ladi va shuning uchun uning siyosati va qoidalari ushbu kengroq doiraga mos kelishi kerak. Filial yoki agentlik faqat o‘z saylov okrugi uchun va o‘z ustavi doirasida yangi qonunchilikni yaratishi mumkin. Masalan , sanoatni tartibga soluvchi organ tomonidan chiqarilgan kiberxavfsizlik siyosati faqat uning tartibga soluvchi sohasiga tegishli bo‘ladi. Energiya regulyatori energiya ob’ektidan ortiqcha aloqaga ega bo‘lishini talab qila oladi, lekin

telekommunikatsiya provayderlaridan har bir energiya ob’ektiga ortiqcha kabel yotqizishini talab qila olmaydi. Faqat telekommunikatsiya sohasini tartibga soluvchi organ telekommunikatsiya sohasi uchun qoidalarni belgilashi mumkin va nizom boshqa tartibga soluvchi organning domeniga ko‘rsatiladigan xizmatlarni o‘z ichiga olmaydi.

Korxona siyosati. Xususiy sektor tashkilotlari odatda hukumatlar kabi yuqori boshqaruv siyosatini amaldagi qoidalarga aylantirishda cheklangan emas. Korporativ muhitda, qoida tariqasida, sanktsiya tahdidi bilan, shu jumladan ishdan bo‘shatishgacha bo‘lgan siyosatga rioya qilish kutiladi. Masalan, inson resurslari, huquqiy yoki buxgalteriya siyosati har qanday nomuvofiqlik holatlari tugatish uchun sabab bo‘lishi mumkin bo‘lgan darajada himoyalangan. O‘rta darajadagi menejerlar xodimlarni yollash yoki xarajatlarni to‘lash kabi jarayonlarni qo‘llab-quvvatlasa, ular bo‘lim faoliyatini ushbu siyosatlarga muvofiqlashtirishi mumkin va ko‘pincha muvofiqlik uchun bo‘lim darajasidagi o‘lchovlarni o‘rnatishlari kerak bo‘ladi. Hukumat misolida bo‘lgani kabi, har qanday bunday subtashkilot ham vakolat doirasidagi cheklovlarga duchor bo‘ladi. Axborot tasnifiga juda jiddiy yondashadigan joylarda istisnolar mavjud bo‘lsa-da, bosh ijrochi direktor tomonidan chiqarilgan korporatsiya xavfsizlik siyosati odatda butun korporatsiyaga nisbatan qo‘llaniladi, lekin Bosh Axborot direktori tomonidan chiqarilgan siyosat odatda faqat texnologiya xodimlariga nisbatan qo‘llaniladi. Tashkiliy landshaftdagi yaqinda sodir bo‘lgan o‘zgarish - bu tashkilotning xavfsizlik pozitsiyasining tanlangan jihatlari uchun mas’ul bo‘lgan bosh axborot xavfsizligi xodimi yoki xavfsizlik bo‘yicha bosh direktorning tayinlanishidadir.

Aksariyat korporativ kiberxavfsizlik siyosatlari va yuridik yoki inson resurslari bo‘limi tomonidan chiqarilgan siyosatlar o‘rtasidagi farq shundaki, kiberxavfsizlik siyosati ko‘pincha kiberxavfsizlik xatarlarini baholashni o‘rta darajaga qo‘yadi. Bunga asosiy sabab kiberxavfsizlik yoki xavflarni boshqarish tushunchalari bilan tanish bo‘lmagan menejerlar hisoblanadi.

Masalan, kiberxavfsizlik siyosatida “axborot konfidensialligini buzish xavfi yuqori bo‘lgan joyda, ma’lumotni sotuvchining axborotni himoya qilish qobiliyatini sinchkovlik bilan tekshirmasdan turib, sotuvchi bilan bo‘lishishiga yo‘l qo‘yilmasligi kerak” deb belgilanishi mumkin. Ushbu turdagi siyosat axborot xavfini baholashni bo‘lim axborot oqimining bir qismini autsorsing qilish orqali xarajatlarni kamaytirishga undashi mumkin bo‘lgan menejerga qoldiradi. Ushbu xarajatlarni yanada

kamaytirish uchun o‘sha menejer tegishli tekshiruvni ko‘rib chiqishga kafolat bermaydi deb qaror qilish mumkin.

Texnologiya konfiguratsiyasi. Ko‘pgina texnologik operatsiyalar standartlari maxsus xavfsizlik dasturiy ta’minoti va qurilmalari yordamida amalga oshirilganligi sababli, texnologiya operatorlari odatda ushbu qurilmalarning standart tomonidan belgilangan texnik konfiguratsiyasini “xavfsizlik siyosati” deb atashadi . Ushbu spetsifikatsiyalar yillar davomida sotuvchilar va xizmat ko‘rsatuvchi provayderlar tomonidan amalga oshirildi, ular tizim ma’murlariga turli standartlarga muvofiqligini da’vo qilish imkonini beradigan hisoblash qurilmalarining texnik konfiguratsiyasini ishlab chiqdilar. Bu sotuvchilarni o‘z mahsulotlari uchun muqobil texnik konfiguratsiyalarni “xavfsizlik siyosati” deb belgilashga olib keldi. Sotuvchining marketing adabiyoti ushbu texnik konfiguratsiyalarni “siyosat” sifatida taqdim etadi va ularning yechimlarini umumiy xavfsizlik strategiyasiga moslashtirishga harakat qiladi.

Strategiya siyosatga qarshi. Kiberxavfsizlik siyosati kiberxavfsizlik maqsadlariga erishish strategiyasini ifodalaydi va uning tarkibiy qismlariga kiberxavfsizlik choralaridan to‘g‘ri foydalanish bo‘yicha ko‘rsatmalar beradi. Yo‘nalish ijtimoiy kelishuv yoki boshqaruv organi tomonidan belgilanishi mumkin. Biz, shuningdek, mustaqil korxonalar kiberxavfsizlik strategiyasini qo‘llab-quvvatlash uchun boshqaruv ko‘rsatmalarini o‘rnatishi kerakligini tan olamiz va biz o‘zgartirilgan “korxona siyosati” atamasidan faqat ma’lum bir korxona hamjamiyatida amal qiladigan siyosatlarga ishora qilish uchun foydalanamiz. Odatda bunday korporativ siyosat ko‘pincha Xalqaro Standartlashtirish Tashkiloti (ISO) va NIST tomonidan o‘rnatilgan kiberxavfsizlik standartlariga asoslanadi, bu standartlar o‘z-o‘zidan siyosat emas. Bunday standartlar odatda texnologik nazorat bo‘yicha tavsiyalar bilan texnologik yo‘riqnomaning kombinatsiyasini o‘z ichiga oladi. Jarayon bo‘yicha yo‘riqnoma siyosatni o‘rnatishni tavsiya qiladi, lekin to‘g‘ridan to‘g‘ri siyosat deb atash mumkin emas.

Barcha siyosatlar ular qo‘llanilayotgan amalga oshirish standartlaridan farq qiladigan ma’noda siyosat taxminiy bo‘lishi mumkin, chunki siyosatning oddiy qabul qilinishi xavfsizlik maqsadlariga erishish uchun to‘g‘ri mos qoidalar o‘rnatilishini kafolatlamaydi. Kiberxavfsizlik ta’sirining aniq kontseptual ko‘rinishisiz kiberxavfsizlik strategiyasini va tegishli siyosatni ishlab chiqish qiyin bo‘ladi. Siyosatni qo‘llash mexanizmlari bo‘yicha keng ko‘lamli kelishuvlar mavjud bo‘lsa ham va

ularni bevosita siyosat ko‘rsatmalariga qarab kuzatish mumkin bo‘lsa ham, jamoaviy qaror noto‘g‘ri bo‘lishi mumkin va bu mexanizmlar xavfsizlik siyosati maqsadlariga erisha olmasligi mumkin.

Kiberxavfsizlik siyosatini shakllantirishning kaliti xavfsizlikni nazorat qilish qarorlari rasmiy siyosat mavjudligidan qat’i nazar qabul qilinishini tan olish,siyosat bir nechta mustaqil ravishda qabul qilingan xavfsizlik qarorlarini boshqarish uchun mos vosita ekanligini tushunish va xavfsizlik strategiyasini ishlab chiqish jarayonida xavfsizlik bo‘yicha qarorlar qanday ta’sir qilishi haqida imkon qadar ko‘proq ma’lumot olishdadir.

1.2-§. Kiberxavfsizlik evolyutsiyasi

Kiberxavfsizlik siyosatini tushunish uchun kiberxavfsizlik qanday rivojlanganligini haqida tushinchaga ega bo‘lishimiz kerak. Kompyuterlar birinchi avtomatlashtirilgan jarayonlarni ishga tushirganda, bunday loyihalarning barchasida asosiy maqsad inson kalkulyatorlarini aniqroq natijalarni beradigan avtomatlashtirilgan dasturlarga almashtirish natijasida unumdorlikni oshirish edi. Ko‘proq dasturiy ta’minot mavjud bo‘lganda, kompyuterlarning unumdorlik afzalliklari oshadi. Internetning joriy etilishi, ma’lumotlarni tez va to‘g‘ri uzatish imkonini berib, unumdorlikni yanada oshirdi. Bu to‘g‘ridan-to‘g‘ri biznes operatsiyalarini onlayn tarzda qayta ishlash imkoniyatiga olib keldi. Bu qobiliyat elektron tijorat deb nomlandi. 2000-yilga kelib, iqtisodiyot elektron tijoratga shunchalik qaram bo‘lib qoldiki, u tez-tez kiber jinoyatchilar nishoniga aylandi va xavfsizlik texnologiyasi firibgarlik operatsiyalarini amalga oshirish uchun ishlatilishi mumkin bo‘lgan ma’lumotlarni himoya qilish uchun rivojlandi. Bunday texnologiya odatda *qarshi choralar* deb ataladi, chunki ular ma’lum bir tahdidga qarshi turish uchun mo‘ljallangan xavfsizlik choralaridir. Bugungi kunda kiberxavfsizlik texnologiyasining rivojlanishi dunyoda kiber qurollanish poygasini keltirib chiqardi, bunda qarshi choralar ortda qolmoqda.

Hosildorlik. Kiberxavfsizlik tarixi 1960-yillarda meynfreymdan boshlanadi. Bu elektron ma’lumotlarni qayta ishlash tizimlaridan investitsiya daromadini ko‘rish uchun korxonalar uchun yetarlicha arzon bo‘lgan birinchi kompyuter edi. Bu vaqtgacha “kompyuter” so‘zi hisob-kitoblarni amalga oshiruvchi shaxsni nazarda tutgan va “kiber” so‘zi ilmiy fantastika sohasi edi. O‘sha kunlarda kompyuterlar qo‘riqchilar va maxsus usullar bilan himoyalangan. Jismoniy xavfsizlik tartib-qoidalari

faqat kompyuterlarda ishlashga ruxsat berilgan odamlarning ularga jismoniy kirishini ta’minlash uchun ishlab chiqilgan. Kompyuterlar shunchalik katta ediki, yuzlab kvadrat fut maydonlar maxsus xavfsizlik xodimlari bilan ishlashi uchun moslashtirilardi. Qo‘riqchi funktsiyasi ba’zan kompyuter operatori roli bilan birlashtirilib, ishni boshqarish bo‘yicha texnik deb atalardi. Kompyuterdan foydalanishi kerak bo‘lgan odamlar o‘z ma’lumotlari va dasturlarini perfokartalar to‘plamida ushlab, qo‘riqchi oldida navbatda turishardi. Qo‘riqchi foydalanuvchining kompyuterdan foydalanishga ruxsatini tekshiradi, kartalar to‘plamini oladi va uni kartalardagi teshiklarni bit va baytlarga avtomatik ravishda tarjima qiladigan kartani o‘quvchiga joylashtiradi. 1960-yillarning oxiriga kelib, masofadan ulanish orqali asosiy kompyuterga kabel orqali ulangan bir nechta ofis joylaridan perfokartalarni qabul qilish imkoni yaratildi. Keyin kompyuter xavfsizligi xodimlari ushbu kabellarni baland pollar ostida, devor bo‘shliqlari va uzatish kanallari orqali vakolatli shaxs boshqa uchida o‘tirganiga ishonch hosil qilish uchun qo‘shimcha mas’uliyatga ega edilar.

Ushbu dastlabki avtomatlashtirilgan kompyuter tizimlarining menejerlari xavfsizlik xavfini juda yaxshi bilishgan, ammo konfidentsiallik, yaxlitlik (butunlik), foydalanuvchanlik triadasi hali sanoat standarti emas edi. Harbiy va razvedkadagi bir nechta qurilmalardan tashqari, konfidentsiallik asosiy xavfsizlik talabi emas edi. Garchi korxonalar mijozlar ro‘yxatini maxfiy saqlashni xohlashsa-da, turli sinovlardan o‘tmagan dasturiy ta’minot doimo ishlamay qolar edi, shuning uchun ularning asosiy tashvishi konfidentsiallik emas, balki yaxlitlik edi. Ma’lumotlarning yaxlitligidagi halokatli xatolarga olib kelishi mumkin bo‘lgan inson xatosi ehtimoli har doim kompyuter dasturlarini ishlab chiqish va operatsiyalarida aniq bo‘lgan.

Dasturiy ta’minot muhandisligi tashkilotlari xavfsizlik signalini birinchi bo‘lib ko‘tardilar, chunki kompyuterlarda noto‘g‘ri ishlash hayotni xavf ostiga qo‘yishi mumkin bo‘lgan tizimlarni boshqarishni boshladi. Bundan tashqari, moliyaviy firibgarlik ko‘rinishidagi kompyuter jinoyati 1970-yillarning boshlariga kelib keng tarqalgan bo‘lib, uni badiiy adabiyot va televideniyening asosiy oqimiga aylantirdi. Xavfsizlik tahdidlari doirasidan inson omili yo‘q qilingan deb hisoblasak ham, tizimdagi nosozliklar kompyuter tizimidagi vakuum naychalari orasida aniqlangan birinchi haqiqiy xatolikdan boshlab aybsiz sodir bo‘lishi ma’lum edi. 1970-yillarda perfokartalar klaviatura va terminallar orqali elektron kiritish va chiqarish bilan almashtirildi. Kabellar va

terminallar ruxsat etilgan foydalanuvchilar ma’lumotlarni qayta ishlash vaqtida o‘tirishlari mumkin bo‘lgan diapazonni yanada kengaytirdi. Tizimlar xavfsizligi kengayib, kabellar vakolatli kompyuter foydalanuvchilari egallagan ofislarda tugatilishini ta’minlash uchun devor bo‘laklari va uzatish kanallari orqali kabellarni kuzatishni o‘z ichiga oladi. Bu haqiqiy kompyuterdan uzoqda joylashgan ofislardagi odamlarga kirtish-chiqarish portiga ulanishi va undan ish stolidan foydalanish imkonini berdi. Kompyuter xonasi eshigi oldida qo‘riqchi qoldi, lekin asosan kompyuter xonasini aylanib chiqadigan tashrif buyuruvchilar yoki texnik xizmat ko‘rsatgan sotuvchilarni ro‘yxatdan o‘tkazish uchun qoldi. Axborot xavfsizligi moslashtirilgan biznes mantig‘i sohasiga o‘tkazildi.

Foydalanuvchilarga o‘zlarining ish funksiyalarini bajarishlari uchun zarur bo‘lgan ekranlarni taqdim etadigan menyular bilan bog‘liq bo‘lgan login nomlari berildi. Buning ta’siri shundaki, ko‘pchilik foydalanuvchilar bir xil asosiy ekranni ko‘rar edilar, ammo turli xil ma’lumotlar maydonlari va menyu tanlovlari turli foydalanuvchilar uchun mavjud edi. Ekranlar dasturiy ta’minotga kodlangan *biznes mantig‘i* bilan cheklangan. Misol uchun, agar xizmatchilar mijozlarga xizmat ko‘rsatish ekraniga ega bo‘lsa, ular mijozlar yozuvlarini ko‘rishlari mumkin, ammo balanslarini o‘zgartiraolmaydilar. Biroq, biznes mantiqiy ekranlari ko‘pincha bekor qilishlarni o‘z ichiga oladi. Misol uchun, mijozlarga xizmat ko‘rsatuvchi xodimni kuzatayotgan nazoratchi ekranning cheklangan funksiyasi orqali balansni bir martalik o‘zgartirishga ruxsat berish uchun maxsus kod kiritishi mumkin. Klaviatura texnologiyasi yordamida ishlaydigan kompyuterlarning keng qo‘llanilishi konfidentsiallikni nazorat qilish masalasiga e’tibor qaratdi. Harbiy va razvedka kompyuterlaridan foydalanish ko‘paydi. Hukumat tomonidan moliyalashtiriladigan kriptografiya bo‘yicha tadqiqotlar ma’lumotlarni blokirovka qiladigan va ochadigan “kalitlar” deb nomlangan bitlarning uzun ketma-ketligidan foydalangan holda ma’lumotlarni o‘qib bo‘lmaydigan formatlarga aylantiradigan bir nechta algoritmlarni ishlab chiqdi.

Bunday kriptografik algoritmlar *diffuziyaga*, xabarni statistik jihatdan uzoqroq va noaniqroq formatlarga tarqatishga va *chalkashlikka*, shifrlangan xabar va tegishli kalit o‘rtasidagi munosabatlarni juda uzoq va taxmin qilish uchun jalb qilishga asoslangan. Biroq, kompyuter quvvatidagi yutuqlar qat’iy raqibning xabarlar va kalitlar o‘rtasidagi munosabatni aniqlash qobiliyatini sezilarli darajada oshirdi. Mavjud avtomatlashtirilgan kriptografiya usullari avtomatlashtirilgan statistik

tahlilni buzadigan darajada murakkab bo‘lmagan kunni tasavvur qilish oson edi. Bundan tashqari, AQSh Ijtimoiy xavfsizlik ma’muriyati va ichki daromad xizmati kabi davlat idoralari tomonidan qaydlarni avtomatlashtirish, kibermakondagi manfaatdor tomonlar jismoniy hayoti ularni ifodalovchi bit va baytlarga chambarchas bog‘langan shaxslarni o‘z ichiga olganligini tan olishga yordam berdi.

Konfidentsiallik talablarining ortib borayotganini e’tirof etgan holda, lekin ularni qondirishning yaxshi usuli bo‘lmagan holda, AQSh Milliy Standartlar Byurosi (hozirgi Milliy Standartlar va Texnologiyalar Instituti (NIST)) ushbu maqsadga erishish uchun harakat boshladi.

1974 yilda AQShning Kompyuter xavfsizligi to‘g‘risidagi qonuni (Maxfiylik to‘g‘risidagi qonun) axborot tarqalishi ustidan nazoratni o‘rnatish uchun mo‘ljallangan birinchi qonun edi. Hujjat faqat davlat tomonidan kompyuterlardan foydalanishni va faqat bugungi kunda shaxsiy identifikatsiya qilinadigan ma’lumot deb ataladigan ma’lumotlarni qamrab oldi. Ammo u kiberxavfsizlikning asosiy maqsadlari sifatida konfidensiallikni va shifrlash texnologiyasini takomillashtirish bo‘yicha tegishli sa’y-harakatlarni qat’iy belgiladi. 1970-yillar davomida texnologiya rivojlanib borar ekan, DEC PDP-11 kabi mini-kompyuterlar tez-tez yirik kompaniyalarning meynfreymlarini to‘ldirib va tez orada kichik kompaniyalarga aylanib borar edi, endi ularga matnni qayta ishlash kabi ofis vazifalarini avtomatlashtirish imkoniyatini bera olardi. Hali har qanday o‘lchamdagi kompyuterni sotib olishga qodir bo‘lmaganlar uchun texnologiyani yaxshi biladigan tadbirkorlar odamlarga kompyuterni ma’lum vaqtga ijaraga olish imkonini beradigan xizmatlarni ishga tushirishgan. Bular “timeshareing xizmatlari” deb nomlandi, chunki bu biznesdagi kompaniyalar o‘z mijozlaridan kompyuter sarflagan vaqtiga qarab haq olishardi.

Terminal va klaviatura texnologiyasi IO qurilmalarini kabellar orqali kengaytirishga imkon yaratgandan so‘ng, ular analog modulyatsiya demodulyatsiyasi texnologiyasidan (modemlar va multipleksorlar) foydalanib, kompyuter terminalining bino devorlaridan tashqariga chiqishini kengaytirish uchun oddiy telefon liniyalaridan foydalanganlar. Bu kompaniyalar ish haqi solig‘i hisob-kitoblari va tijorat ijarasi hisob - kitoblari kabi murakkab dasturiy ta’minotni ishlab chiqib, sanoat bo‘yicha ixtisoslasha boshladilar.

Bunday dasturiy ta’minotni ishlab chiqish dasturiy ta’minot biznesida bo‘lmagan kompaniya uchun foyda-xarajat tahlilida yaxshi natija berishi dargumon, ammo bu ko‘plab korxonalar tomonidan

boshqariladigan vaqtni talab qiluvchi qo‘lda ishlov berish jarayoni edi. Vaqtni taqsimlash xizmatlari biznesning asosiy qismi bo‘lmagan bo‘limlarga avtomatlashtirishdan foydalanishga imkon berdi, garchi ular buni amalga oshirish uchun boshqa birovning kompyuteriga kirishlari kerak edi. Bugungi kunda ushbu xizmatlar Internet orqali mavjud, ammo ularning zaryadlash modellari o‘zgargan va ular endi “vaqtni taqsimlash” emas, balki “bulutli hisoblash” deb nomlanadi.

Ushbu vaqt taqsimlash xizmatlari foydalanuvchi faoliyatiga asoslangan resurslarni hisoblash uchun haq olinadi, shuning uchun ular hisob-kitob qilish uchun foydalanuvchilarni aniqlash usuliga ega bo‘lishlari kerak edi. Ko‘pincha, bu foydalanuvchi identifikatori shunchaki kompaniya nomi edi, lekin parol ba’zan vaqt taqsimlash xizmatlarida raqobatchilar bo‘lgan mijozlarga ega bo‘lgan joylarda chiqariladi. Biroq, mijozning foydalanuvchisi nuqtai nazaridan, foydalanuvchi nomi ularni kompyuterdagi ma’lumotlariga bog‘ladi va modemga ulanishi xavfsizlikka xavf tug‘dirmaydi. O‘sha paytda kompyuterga egalik qilish uchun yetarlicha katta bo‘lgan har qanday kompaniya ma’lum bir mulk va mazmunga ega bo‘lgan firma edi, shuning uchun timesharing xizmati kompaniyalari o‘z kompyuterlari atrofida jismoniy xavfsizlikka muhtoj deb taxmin qilgan va parollar ularning xavfsizligini sinchkovlik bilan tekshirishning yana bir dalili edi. Timesharing xizmati sotuvchisi uchun mijozlarga mantiqiy kirishga ruxsat berish xavfli deb hisoblangan va ularning boyligi va mohiyatini hisobga olgan holda, ular o‘z aktivlarini shunga mos ravishda himoya qilishlarini kutish mumkin edi. 1970-yillardan 1980-yillarga qadar mini-kompyuterlar arzonroq bo‘ldi va oxir-oqibat odamlarga o‘zlari foydalanishi uchun butun kompyuterga ega bo‘lish imkonini berdi. Apple shaxsiy kompyuterlarini 1970-yillarning oxirida taqdim etdi. Tez orada ular ma’lumotlarni qayta ishlash muhitiga kirdi va 1981 yilda IBM shaxsiy kompyuteri paydo bo‘ldi. Bu kichik kompyuterlar uchun jismoniy xavfsizlik hali ham norma bo‘lib qoldi va qulflangan ofis eshiklari asosiy himoya mexanizmi edi.

Tarmoq texnologiyalari keyinchalik bir binodagi ish stoli kompyuterlariga bir-biri bilan ma’lumot almashish imkonini berdi va kompyuterlarning nomlari odamlar tarmoqdagi boshqa kompyuterlar bilan axborot almashishi uchun muhim bo‘la boshladi. Mahalliy tarmoq (LAN) kabellari xuddi kompyuter terminallarining meynfreymga ulanishi kabi himoyalangan edi, bundan tashqari yangi turdagi tarmoq uskunasi “hub” deb nomlangan aloqani amalga oshirishga imkon berdi va hublar

xavfsiz hududda saqlanishi kerak edi. Biror kishiga o‘z kompyuterini LANga ulash imkonini beradigan markazlar qulflangan shkaflar orqali himoyalangan. LANlar joriy etilgunga qadar, hisoblash muhitiga kirish boshqaruvlari normadan ko‘ra istisno edi. Agar login identifikatorlari tarqatilgan bo‘lsa, ular kamdan-kam hollarda o‘chirilgan.

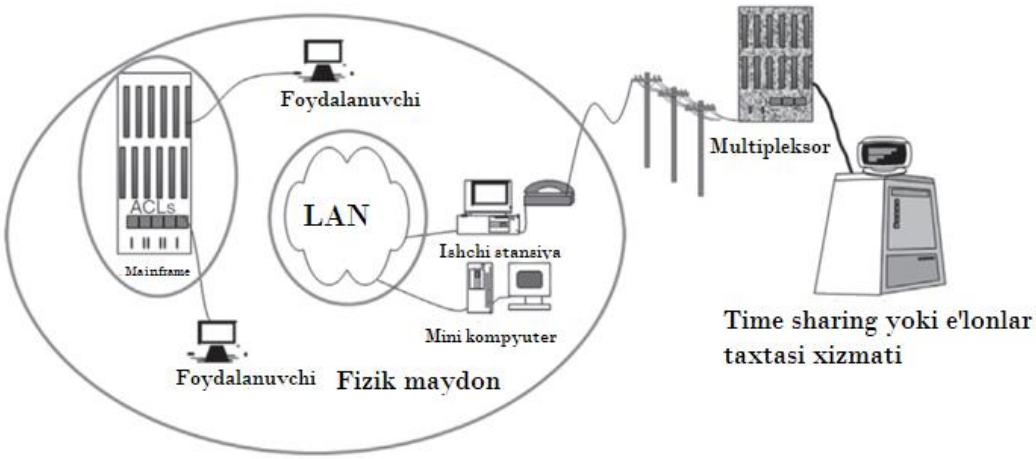
Ular ma’lumotlarga kirishni cheklashdan ko‘ra, kimga tegishli ekanligini bilish uchun ko‘proq ma’lumotlarni belgilashning qulay usuli sifatida ishlatilardi. Biroq, LANga ulangan hisoblash muhitlari va tegishli shaxsiy kompyuterlarning ko‘pligi tarmoqdagi kompyuter faolligini alohida shaxslarga kuzatishni juda qiyinlashtirdi, chunki ular odatda faqat ish stolidagi mashinaga kirishgan. LANlar kattalashgan sari, davlat tadqiqot laboratoriyalarining markazlashtirilgan boshqaruv sxemalari korporativ meynfreymlar uchun ishlab chiqildi. Majburiy kirishni boshqarish tizim kompyuter ob’ektlarini (dasturlar va fayllar) belgilash va ularga kirish mumkin bo‘lgan sub’ektlarni (foydalanuvchilarni) nazoratlash imkonini berdi. Ular ixtiyoriy sxemalar bilan to‘ldirildi, bu har bir foydalanuvchiga o‘z fayllariga yana kim kirishi mumkinligini belgilash imkonini berdi.

Ko‘pgina LAN kompyuter foydalanuvchilarining stollarida asosiy kompyuter terminali bo‘lganligi sababli, ko‘p o‘tmay, bu kompyuterlar terminal funksiyasini o‘zlashtirdilar va LAN asosiy kompyuterga ulandi. Aynan mana shu rivojlanish kiberxavfsizlikni texnologiya boshqaruvida dolzarb mavzuga aylantirdi. LAN tarmog‘ida ba’zi vaqt almashinuvi tipidagi parol texnologiyasidan foydalanilgan bo‘lsa-da, LAN foydalanuvchi nomlari, birinchi navbatda, aniqlangan hujumlarning oldini olish uchun emas, balki katalog xizmatlarini osonlashtirish uchun qo‘llab-quvvatlandi. Ya’ni, ma’lum bir faylni yozgan yoki mijozning yozuviga eslatma joylashtirgan shaxsning ismini bilish foydali bo‘ldi. Kompyuter foydalanuvchilariga kirish nomlarini belgilash dasturlarga to‘g‘ri menyu va ekranlarni taqdim etish uchun biznes mantig‘ining bir qismi sifatida ushbu nomdan foydalanishga imkon berdi.

Kibermakon evolyutsiyasining shu nuqtasiga qadar, meynfreymdagi tranzaktsiyalar ma’lum bir jismoniy joylashuvdagi individual terminalda kuzatilishi mumkin edi, jismoniy va raqamli kriminalistikaekspertizasi yordamida keyingi tergov gumonlanuvchini aniqlash uchun jangovar imkoniyatga ega edi. Biroq, LAN va modemlar foydalanuvchilar o‘rtasidagi muloqotni yashirin qildi va jinoyatchi uchun LAN ish stoli orqali amalga oshirilgan faoliyatni *rad* etish yoki so‘zning tez tarqaladigan kompyuter xavfsizligi versiyasidan foydalanish oson edi .

Parollar talab qilingan joylarda ham ular taxmin qilish uchun yetarlicha zaif edi.

Tarmoqni shifrlash tushunchasi yo‘q edi, shuning uchun markazlarga kirish huquqiga ega bo‘lgan har bir kishi tarmoqda sayohat qilayotgan parollarni ko‘rishi mumkin edi. Bundan tashqari, ko‘plab tarmoq dasturlari anonim kirishga ruxsat berdi, shuning uchun foydalanuvchi nomlari har bir ulanish uchun mavjud emas edi. Rahbariyatga joriy vaziyat barqaror bo‘lishi uchun juda katta xavf mavjudligini tushunish uchun bir necha insayder firibgarlik holatlari kerak bo‘ldi. Shunday qilib, shu paytgacha harbiy tadqiqotlar mavzusi bo‘lgan xavfsizlik texnologiyasi yirik kompyuter sotuvchilari tomonidan shoshilinch ravishda amalga oshirildi va asosiy kompyuter ma’lumotlar to‘plamlari va LAN fayl resurslariga tatbiq etildi. Bularga foydalanuvchi identifikatori, tobora qiyinlashib borayotgan parollar ko‘rinishidagi autentifikatsiya va kompyuterga kirish uchun boshqaruv ruxsati kiradi. Tez orada AQSH Mudofaa vazirligining qarori asosida “Apelsin kitobi” nomli muhitda ishlashni ta’minlash uchun zarur bo‘lgan tizim funksiyalarining to‘liq to‘plami osongina mavjud bo‘ldi. To‘liq xususiyatlar to‘plami kiritilgan texnik amalga oshirish uchun standartlar va murakkab terminologiya, foydalanuvchilarning aniqlanishi va autentifikatsiya qilinishini ta’minlash uchun jarayonlar tekshirildi. Shifrlash ham a uchun aniq yechim sifatida e’lon qilindi va turli xil kompyuter xavfsizligi muammolari yechimi topildi, lekin bu hashamat edi armiyadan tashqarida kam sonlilar yetarlicha zaxira kompyuterga ega edilar, shuning uchun kompyuter qanchalik kichik bo‘lsa, sotuvchining shifrlash algoritmlari shunchalik zaif bo‘lishi mumkin edi va shifrlash aniqlik bilan qo‘llanildi. Garchi tranzaktsiyalarni qayta ishlash uchun javobgarlik tez bo‘lib qolgan bo‘lsa-da firibgarlik konferentsiyalarida dolzarb mavzu, domendagi huquqni muhofaza qilish faoliyati kompyuterning ishlashi cheklangan edi. Shunga qaramay, 1980-yillarning boshlari ham raqamli dalillar davrining boshlanishi edi.



1.4-rasm. 1980-yillardagi kibermakon arxitekturasi

Huquqni muhofaza qilish organlari bilan hamkorligida texnologiya sotuvchilari jinoyatchilar fayllarini qayta tiklaydigan dasturiy ta’minot ishlab chiqarish uchun kompyuterlardan o‘chirishga harakat qilgan.

1.4-rasmda odatda konfiguratsiya qilinganidek kibermakon arxitekturasi tasvirlangan 1980-yillarning boshlarida. Mainframe, mikro va mini-kompyuterlar yonma-yon mavjud bo‘lib, ular tarmoq orqali ulanishi shart emas edi. Biroq, mini-kompyuterlar ko‘pincha ovozli qo‘ng‘iroqlarni amalga oshiradigan bir xil turdagi telefon liniyalari orqali masofaviy kompyuterlarga ulanish uchun ishlatilgan. Biroq, texnologiya innovatsiyalarining tez sur’atda rivojlanishi sababli, bu holat doimo rivojlanib borardi va o‘zgarish muqarrar edi.

1.3-§. Kiberxavfsizlik maqsadlari

Kiberxavfsizlik texnologiyasining murakkab tabiati va kiberxavfsizlik tahdidlari tobora kuchayib borayotganini hisobga olsak, siyosatchilar doimiy ravishda so‘nggi tahdidga qanday munosabatda bo‘lish bo‘yicha qarorlar bilan to‘qnash kelishlarini kutish mumkin. Biroq, kiberxavfsizlik choralariga oid qarorlar ko‘pincha texnologlarga topshirilganligi sababli, siyosatchi bu qarorlar qabul qilinayotganini ko‘rmasligi va shu sababli turli xil muqobil yondashuvlarning tashkiliy ta’sirini o‘lchash imkoniga ega bo‘lmasligi mumkin.

Aslida, kiberxavfsizlik qurollari poygasi ko‘pincha juda kam muqobil variantlarni taklif qiladi. Kiberxavfsizlik texnologiyasi joriy etilgandan so‘ng deyarli darhol uning qo‘llanilishi ba’zi bir tartibga soluvchi organ tomonidan sanoat standarti deb e’lon qilinadi va bu tashkilotlarni aniqlangan qarshi choralar yondashuviga to‘sqinlik qiladi. Masalan, agar tartibga solinadigan tashkilot xavfsizlik devorlaridan

foydalanmagan kiberxavfsizlik yondashuvidan foydalanishga qaror qilsa, ular tartibga soluvchi auditorlar tomonidan batafsil tekshiruvga duch kelishadi. Kiberxavfsizlik mutaxassislariga tashkiliy yondashuvni qayta ko‘rib chiqishdan ko‘ra, eng yangi xavfsizlik vositalari va texnologiyalaridan xabardor bo‘lishni davom ettirish osonroq ko‘rinadi.

E’tibor bering, bu kiberxavfsizlik siyosati maqsadlari o‘sha paytda kiberxavfsizlik bo‘yicha tashkiliy maqsadlarga mos kelmagan va hozir ham mos kelmasligi kerak. Shunga qaramay, ushbu bobda biz kiberxavfsizlik siyosati maqsadlariga erishilganligini aniqlash uchun foydalanilgan usullarni ham ko‘rib chiqamiz. Xavfsizlik maqsadlarini qo‘yganlar ko‘pincha xavfsizlik maqsadlariga erishish uchun xato qilishlarini kuzatamiz. Biz hozirgi kiberxavfsizlik ko‘rsatkichlari xavfsizlikni umuman o‘lchamaydi degan xulosaga keldik. Bob kiberxavfsizlik maqsadlari qanday belgilanishi va kiberxavfsizlik maqsadlariga erishish qanday o‘lchanishi mumkinligini ko‘rsatadigan uchta amaliy tadqiqotlar bilan yakunlanadi.

Kiberxavfsizlik ko‘rsatkichlari. O‘lchov - bu empirik dunyodan rasmiy munosabatlar dunyosiga xaritalash jarayoni hisoblanib, natijalari ko‘rib chiqilayotgan ob’ektning atributini tavsiflaydi.

Tutib bo‘lmaydigan atributga mos keladigan o‘lchovlar kombinatsiyasi olingan o‘lchovlar hisoblanadi va o‘lchanadigan narsaning mavhum modeli konteksida talqin qilinishi kerak. Ko‘rsatkichlar umumiy atama bo‘lib, ma’lum bir sohani tavsiflovchi o‘lchovlar to‘plamini anglatadi . Kiberxavfsizlik to‘g‘ridan-to‘g‘ri o‘lchov ob’ekti emas yoki olingan o‘lchovlar yoki ko‘rsatkichlarni osongina aniqlash uchun tizimning yetarlicha tushunilgan atributi.

Shunday qilib, kiberxavfsizlik ko‘rsatkichlari bilan shug‘ullanuvchilar boshqa narsalarni o‘lchaydilar va ulardan xavfsizlik maqsadlariga erishish haqida xulosa chiqaradilar. Ushbu muammo xavfsizlik ko‘rsatkichlari deb nomlangan tadqiqot sohasini yaratdi. Jismoniy xavfsizlik ko‘rsatkichlari an’anaviy ravishda tizimning dizayn tahdidiga (DBT) qarshi turish maqsadiga erishish qobiliyatiga qaratilgan. DBT eng kuchli va innovatsion raqibning xususiyatlarini tavsiflaydi, undan himoya qilishni kutish mumkin.

Nyu-York shahrida bu murakkab aloqa vositalari va portlovchi qurilmalar bilan jihozlangan terrorchi shaxs bo‘lishi mumkin. Aydaxoda bu mototsikllarda avtomatik hujum qurollarini olib yurgan 20 kishilik bezorilar bo‘lishi mumkin. Xavfsizlikka DBT yondashuvini qabul qilish tizim tomonidan talab qilinadigan xavfsizlikni himoya qilishning kuchini

uning qanday hujumga uchrashi mumkinligining texnik tavsifiga qarab hisoblash kerakligini anglatadi. Jismoniy xavfsizlikda bu jarayon oddiy. Agar DBT ma’lum turdagi portlovchi moddalarga ega bo‘lgan 20 kishidan iborat bo‘lsa, unda ruxsatsiz kirish uchun jismoniy to‘siqlarning kuchi ushbu 20 kishi qo‘llashi mumkin bo‘lgan tonna kuchga bardosh berishi kerak .

To‘siqni himoya qilish materiallari ko‘rsatilgan, tahdidni kechiktirish va javob berish tizimlari ishlab chiqilgan va shunga muvofiq tekshirish sinovlari o‘tkaziladi. Kiberxavfsizlikda quyidagi atamalari mavjud:

— Jinoyatchi;
— Tahdid;
— Ekspluatatsiya;
— Zaiflik.

Bu atamalari savdo shartlari bo‘lib, ularning ma’nosi alohida va o‘zaro bir biriga bog‘liqdir. 1.4- rasmdagi sistemagrammada ko‘rsatilganidek, jinoyatchi jismoniy yoki yuridik shaxsdir.

Tahdid - bu jinoyatchi tomonidan sodir etilishi mumkin bo‘lgan yoki amalga oshirilmasligi mumkin bo‘lgan potentsial harakat. Ekspluatatsiya hujumni o‘z ichiga olgan texnik tafsilotlarga ishora qiladi.

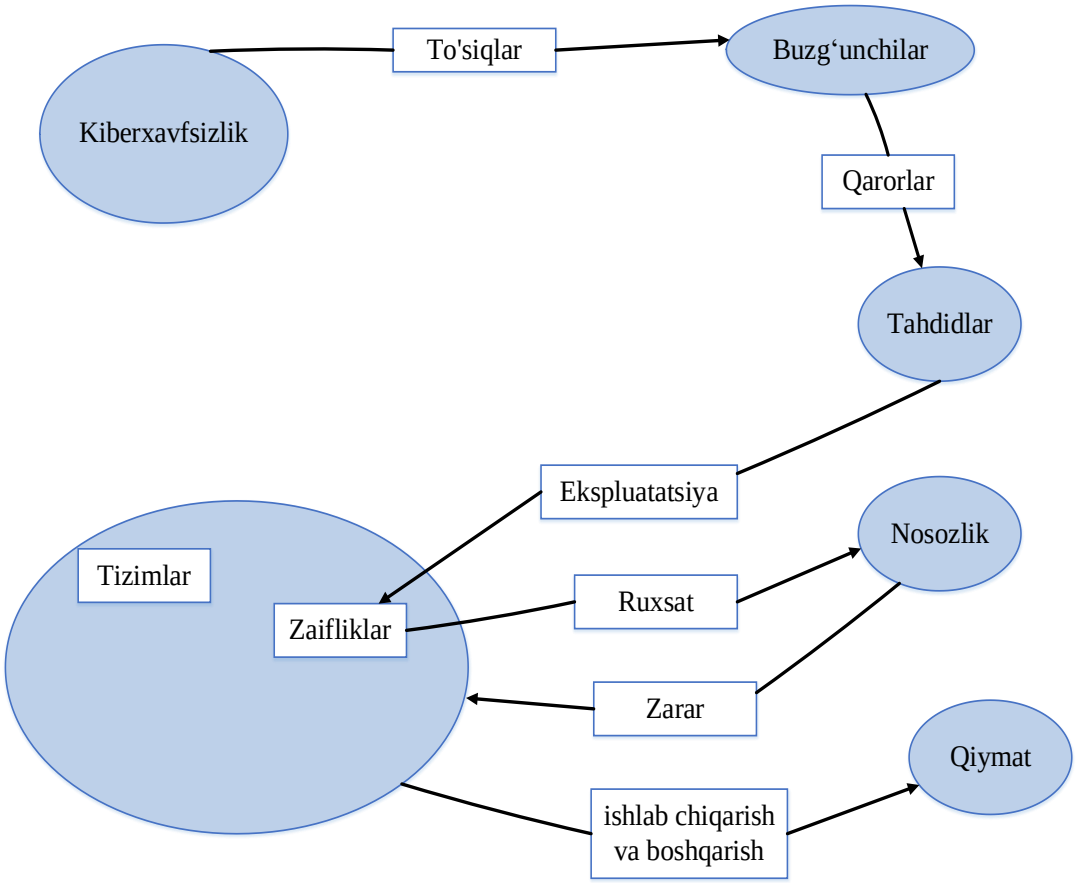
Zaiflik - bu ekspluatatsiyaning muvaffaqiyatli bo‘lishiga imkon beruvchi tizim xarakteristikasi.

Shunday qilib, 1.4-rasmdagi sistemagrammaning asosiy tayanchi shunday o‘qiladi: “Xavfsizlik tizim zaifliklaridan foydalanib, qiymatga salbiy ta’sir ko‘rsatadigan zararni keltirib chiqaradigan tahdidlarni amalga oshiradigan jinoyatchilarni to‘xtatadi”.

Kompyuter tizimlari paydo bo‘lganidan beri, kompyuter xavfsizligi uchun DBTlar potentsial jinoyatchilarni, masalan, joyriderlar, kiber yo‘q qilishning zararli agentlari va josuslik agentlari ko‘rinishidagi xakerlarni ko‘rib chiqdilar.

Biroq, DBTning jismoniy xavfsizligini tahlil qilishdan farqli o‘laroq, tahdidga javoban ishlab chiqilgan qarshi choralar tahdid ishtirokchilarining o‘ziga va ularning eng so‘nggi taktikalari qanday bo‘lishi mumkinligiga emas, balki eng so‘nggi tahdidni amalga oshirish uchun foydalanilgan texnologiya zaifliklariga e’tibor qaratdi. Tizim zaifligining har bir turi xavfsizlik bo‘yicha hamjamiyat xabardor bo‘lish bosqichiga yetganligi sababli, bozorga xavfsizlikka qarshi choralar ko‘rish bo‘yicha tegishli texnologiyalar to‘plami paydo bo‘ldi va tobora ortib borayotgan eng yaxshi amaliyot tavsiyalarining bir qismiga aylandi.

Tizimning zaif qismlariga qarshi choralar qo‘llanildi va tizimlarga tahdidlar ularning barchasini amalga oshirishning umumiy natijasi bilan qoplanadi deb taxmin qilingan.



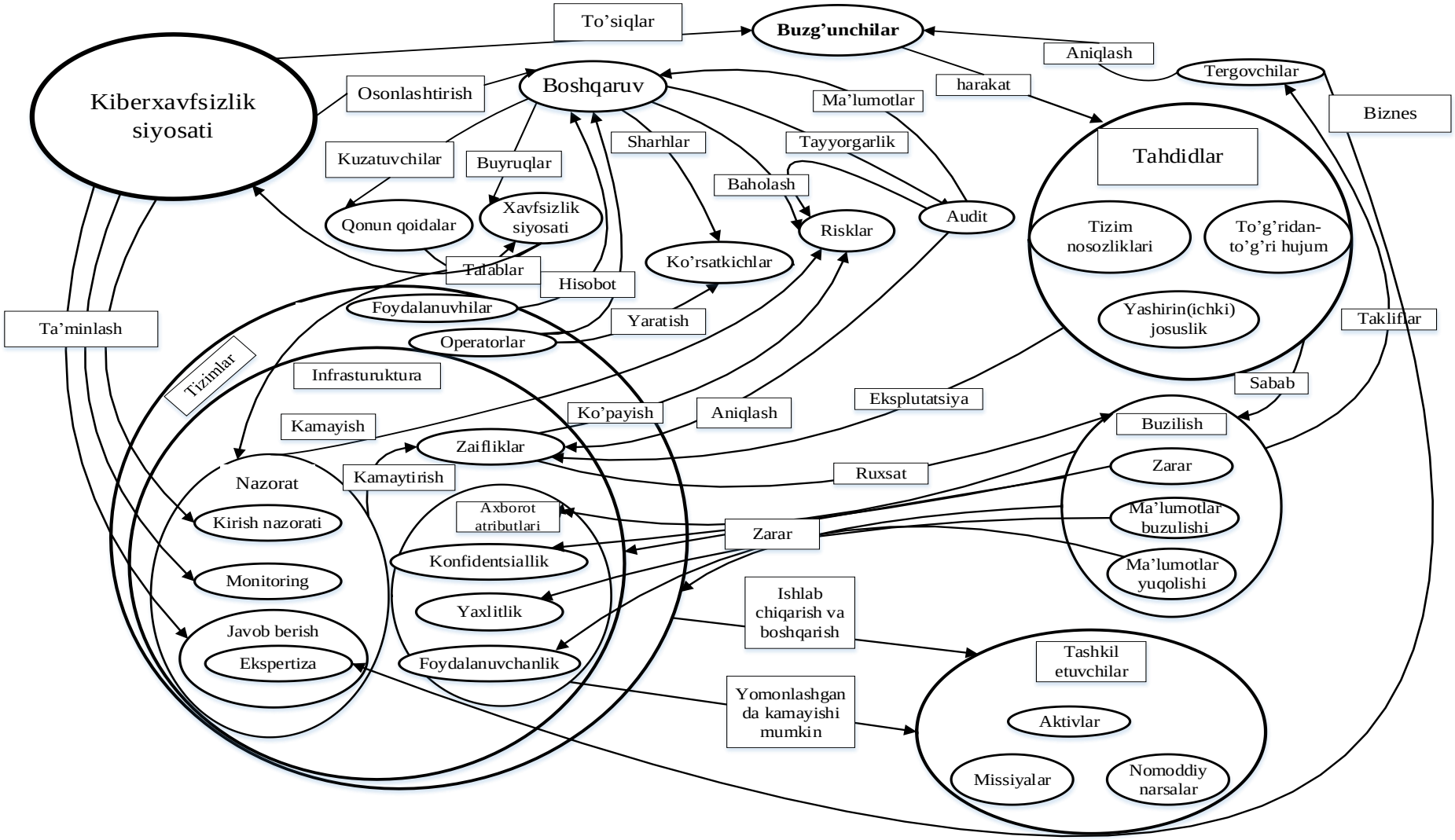
1.5-rasm. Kiberxavfsizlik sistemagrammasi

1.6-rasmdagi ushbu tushunchalar va ular o‘rtasidagi munosabatlar 1.5-rasmdagi sistemagrammaga qo‘shilgan holda ushbu yondashuv tasvirlangan.

1.6-rasmda kiberxavfsizlik ko‘rsatkichlari, boshqaruv yondashuvlari, auditlar va tergov usullari xavfsizlik vositalari va usullariga asoslanganligini ko‘rsatadi.

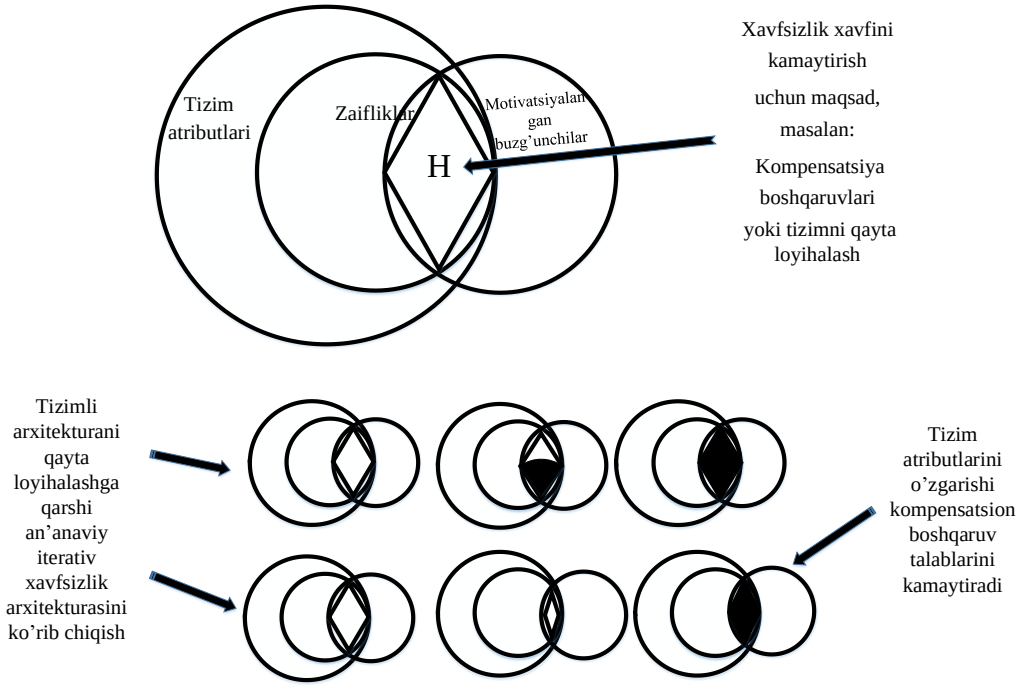
Xavfsizlik maqsadlariga qarshi choralar texnologiyasi bilan erishilishi haqidagi konsensus tizim dizaynining bir qismi sifatida DBTlarga murojaat qilish hisobiga keladi. 1.7-rasmda xavfsizlik arxitekturasiga ushbu an’anaviy yondashuv va tizim darajasidagi yaxlit yondashuv o‘rtasidagi farq ko‘rsatilgan. U tizimning zaif atributlarini tizim atributlarining kichik to‘plami sifatida va jinoyatchilarning maqsadlarini tizimning zaif atributlarining kichik to‘plami sifatida tasvirlaydi.

An’anaga ko‘ra, xavfsizlik muhandisligi ushbu muammoga maxsus xavfsizlik bilan hujum qiladi kamsituvchi tarzda “boltonlar” deb ataladigan komponentlar.



1.6-rasm. To‘liq sistemagramma

Boltonlar, ta’rifiga ko‘ra, tizimning o‘ziga tegishli bo‘lmagan, masalan, 1-bobda tasvirlangan xavfsizlik devorlari bo‘lgan ishlov berish vositalaridir. 1.7-rasmning pastki qismida xavfsizlik muammolarini hal qilishda muruvatli yondashuv va xavfsizlik dizayni o‘rtasidagi ziddiyat tasvirlangan. zaiflikni yo‘q qilish yoki kamaytirish uchun tizim darajasidagi atributlarni o‘zgartirishi kutilayotgan yondashuv. Agar ushbu yondashuv birinchi bo‘lib sinab ko‘rilsa, xavfsizlikka oid kompensatsiya boshqaruvlari soni minimal bo‘lishi kerak. Shunga qaramay, 1-bobda ta’riflanganidek, xavfsizlik texnologiyalari ro‘yxati deyarli ongsiz ravishda qabul qilingan ko‘rinadi. Buning ta’siri shundaki, xavfsizlik maqsadlarining odatiy taqdimoti biznes sohasi va kompyuter operatsion tizimi tomonidan sanab o‘tilgan xavfsizlik texnologiyalarini joriy etish jarayonini ko‘rsatadi. 1.8-rasm odatiy misoldir. Odatda bu ko‘rsatkichga hamroh bo‘ladigan tahlilda marketing biznesi sohasi moliya sohasi kabi xavfsizlikka ega emasligi marketingning moliyaga nisbatan yuqori xavf-xatarlarga chidamliligi bilan izohlanishi mumkin.



1.7-rasm. Bolt bilan bog‘langan dizayn

Xavfsizlikni boshqarish maqsadlari. Ko‘pgina rahbarlarda xavfsizlik uchun “Men xavfsiz bo‘lishni xohlayman” degan fikrdan boshqa aniq maqsad yo‘q. Bunday hollarda maqsadning shunday bir elementi borki, uni to‘liq ifodalash odatda shunday bo‘lishi mumkin: “Men o‘z tashkilotimga juda kam yoki umuman ta’sir qilmasdan xavfsiz bo‘lishni xohlayman”. Ular ushbu ko‘rsatmani xavfsizlik bo‘yicha

mutaxassislarga, xuddi shunday qilib, balans boshqaruvini buxgalteriya xodimlariga topshirib, “Men raqamlar aniq bo‘lishini xohlayman” deb berishadi. Huquqiy va me’yoriy hujjatlarga rioya qilish zarurati bilan bog‘liq ikkita kasbdagi o‘xshashliklarni chetga surib qo‘ysak, delegatsiya ijrochi delegatlar topshirilgan masalalarni tushunadigan va biznesdagi barcha odamlar bilan yaqindan hamkorlik qila olishiga ishonishadi. Ijro hokimiyati-maqsadiga erishish uchun topshirilgan funktsiyalardan manfaatdor tomonlar hisoblanadi.

Biroq, buxgalterlik kasbi bir necha ming yillik tarixga ega bo‘lib, uning ishonchni vaziyatlar va sanktsiyalar kombinatsiyasini o‘z ichiga olgan munosabatlar nuqtai nazaridan aniqlash qobiliyatini qo‘llab-quvvatlaydi.

Aksincha, kiberxavfsizlik kasbi atigi yarim asr yoki birinchi sanoat yoki milliy xavfsizlik standartlari paydo bo‘lganidan beri, xalqaro xavfsizlik standartlari paydo bo‘lganidan beri ancha kamroqdir. Bundan tashqari, har qanday kelishilgan sanoat standartidan ko‘ra, masalan, buxgalteriya hisobining umumiy kelishilgan buxgalteriya hisobi tamoyillari, kiberxavfsizlikda juda ko‘p raqobatdosh standartlar mavjudki, ularni kataloglash va taqqoslash uchun biznes tashkil etilgan. Mahsulot elektron jadval yoki boshqa tuzilgan ma’lumotlar formatida yetkazib beriladi. U xavfsizlik ma’lumotlarini boshqarish (SIM) tizimiga import qilinishi uchun mo‘ljallangan va u xavfsizlik menejeriga ularning barchasini o‘qib chiqmasdan turib bir nechta standartlarga muvofiqligini ko‘rsatish imkonini beradi. Normativ-huquqiy hujjatlarga muvofiqlik asosida ishlab chiqilgan xavfsizlik dasturlari xavfsizlik bo‘yicha tashkiliy maqsadlarga erishish uchun maxsus ishlab chiqilmagan, balki xavfsizlikni boshqarish standartlariga muvofiqligini namoyish qilish uchun mo‘ljallangan. Shunday qilib, standartlarning o‘zi tashkilot chegaralarini kesib o‘tuvchi de-fakto xavfsizlik ko‘rsatkichlari taksonomiyalariga aylandi.

Amaliyotchilarga ko‘pincha o‘z ko‘rsatkichlarini xavfsizlikni boshqarish standartlaridagi talablar atrofida tartibga solish tavsiya etiladi, ular tekshirilishi mumkin. Xavfsizlik ko‘rsatkichlarini yaratish uchun xavfsizlikni boshqarish standartlaridan foydalanishning xalqaro standarti ham mavjud.

Xavfsizlikni boshqarishga yondashuvning bunday turining kamchiliklari shundaki, standartlarga muvofiqlik tafsilotlari xavfsizlik bo‘yicha korporativ maqsadlarni aks ettirish uchun mo‘ljallangan ko‘rsatkich kartasidan farqli o‘laroq, oldindan o‘rnatilgan ko‘rsatkichlar

kartasiga solishtiriladigan izolyatsiya qilingan texnologiya konfiguratsiyasi sifatida ko‘riladi.

Ushbu standartlarning hech biri tahdidlarni bartaraf etishda erishish nuqtai nazaridan xavfsizlikni bevosita o‘lchashning umumiy qabul qilingan usulini o‘z ichiga olmaydi. Ular odatda xavfsizlikni ta’minlashi kerak bo‘lgan faoliyatni o‘rnatishda rahbariyatning tegishli sinchkovlik bilan harakat qilganligini ta’minlash uchun ishlatiladi, bu faoliyat samarali bo‘lganligini o‘lchash uchun emas. Buni oddiy odamlarning xavfsizlikka nisbatan qarashlari bilan taqqoslang. Masalan, ish joyini o‘zgartirgan shaxslar ba’zan eski va yangi firmalardagi xavfsizlikni muhim ma’lumotlar va ma’lumotlarga mahalliy va masofadan kirish qiyinligi darajasiga qarab o‘lchaydilar. Misol uchun, ular ofisdagi mijozlar ma’lumotlariga kirish uchun uyda ish stollaridan foydalanishlari kerak bo‘lgan parollar sonini aniqlashlari va ularni ko‘proq autentifikatsiya qilish omillaridan foydalanishga majbur qiladigan firma xavfsizroq ekanligiga qaror qilishlari mumkin. 1.8-rasmda tizim xavfsizligining ushbu turdagi qatlamli mudofaa tasviri ko‘rsatilgan. Bunday qatlam ko‘pincha *chuqurlikdagi mudofaa deb ataladi*. Bu atama xavfsizlik boshqaruvlari qatlamli va ortiqcha bo‘lgan arxitekturani anglatadi va tizimning bir qismidagi zaiflik boshqasi tomonidan qoplanadi.

Ya’ni, hech bir boshqaruv elementi bitta nosozlik nuqtasini ko‘rsatmasligi kerak, chunki buzg‘unchi kirishi uchun kamida ikkita boshqaruv elementi sinishi kerak. Diagrammaning markaziy pastki qismida tasvirlanganidek, u bir nechta xavfsizlik “qatlamlariga” ega. Diagrammaning yuqori qismida “Masofadan foydalanish” foydalanuvchisi korxona tomonidan boshqarilishi yoki bo‘lmasligi mumkin bo‘lgan ish stantsiyasini autentifikatsiya qilish uchun zarur bo‘lganligi tasvirlangan.

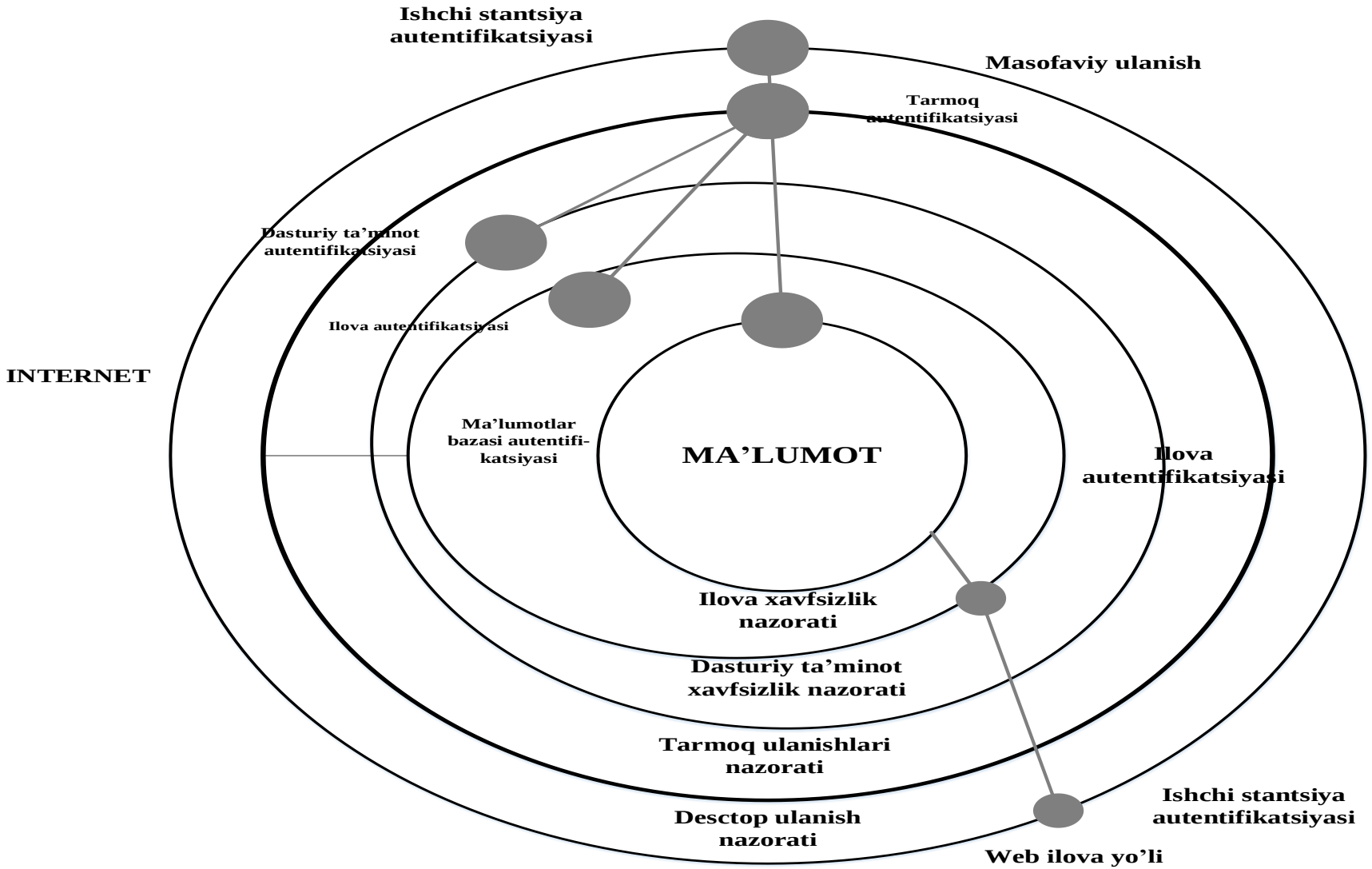
Keyin foydalanuvchi Internet orqali korporativ tarmoqqa autentifikatsiya qiladi. Tarmoqqa kirish nuqtasidan masofaviy foydalanuvchi ichki tarmoqdagi boshqa qatlamlarning istalganiga to‘g‘ridan-to‘g‘ri autentifikatsiya qilishi mumkin. Shuning uchun masofaviy kirish odatda yuqori darajadagi xavfsizlikni talab qiladi, chunki ichki tarmoqqa kirgandan so‘ng platformaga kirish uchun turli xil variantlar mavjud.

Ushbu masofaviy kirish yo‘li 1.8-rasmda veb-ilovaga kirish yo‘liga qarama-qarshidir. Veb-ilovaga kelsak, qatlamlarning mavjudligi aslida chuqur himoyani tashkil etmaydi. Buning sababi shundaki, Internetga

kirish mumkin bo‘lgan bunday ilovalar odatda bitta tizimga kirish orqali mavjud.

Veb-ilova yo‘li shuni ko‘rsatadiki, Internet foydalanuvchilari odatda korxona tomonidan boshqarilmaydigan o‘zlarining ish stantsiyalariga autentifikatsiya qiladilar. Keyin foydalanuvchi tarmoqqa autentifikatsiya qilmasdan dasturga kirishi mumkin, chunki xavfsizlik devori Internetdagi har bir kishiga veb-serverdagi ilovaning kirish ekraniga to‘g‘ridan-to‘g‘ri kirish imkonini beradi.

Shuningdek, serverning operatsion tizimida autentifikatsiya qilishning hojati yo‘q. Ilova ichida bir marta ma’lumotlar autentifikatsiya qatlami foydalanuvchiga ko‘rsatilmaydi; ilova avtomatik ravishda foydalanuvchi nomidan unga ulanadi. Ushbu qulayliklar rasmda masofaviy foydalanuvchi o‘tish uchun autentifikatsiya qilishi kerak bo‘lgan qatlamlar orqali ko‘priklar sifatida tasvirlangan, ammo dastur foydalanuvchisi buni qilmaydi. Demak, bu ishda mudofaa atamasini chuqur qo‘llash noto‘g‘ri bo‘ladi. Zarur bo‘lgan texnologiyani har bir qatlamdagi har bir qulf kaliti bo‘lmagani uchun aslida yopiq bo‘lishini ta’minlash uchun bir nechta qurilmalar muvofiqlashtirilgan holda sozlanishi kerakligi aniq. Shunday qilib, xavfsizlik ko‘rsatkichlari bo‘yicha ko‘plab adabiyotlarda maqsad ushbu qatlamlarning barchasini to‘g‘ri konfiguratsiya qilish deb taxmin qilinadi. Biroq, bu taxminga qaramay, xavfsizlik ko‘rsatkichlari uchun standart taksonomiya mavjud emas. Bunday tasniflashda foydalaniladigan tamoyillar turli tadqiqotchilar tomonidan tadqiq qilingan va bu izlanishlar turli natijalar bergan.



1.8-rasm. Veb ilovaga kirish yo‘lli

Nazorat savollari.

1. Qanday texnologiyalar kibermakondagi axborotning yaxlitligini himoya qilishga yordam beradi?
2. Kiberxavfsizlik nima va u ma’lumotlarning maxfiyligi, yaxlitligi va foydalanuvchanligi bilan qanday bog'liq?
3. Kiberxavfsizlikning qanday muqobil yondashuvlari mavjud va ularning afzalliklari va kamchiliklari qanday?
4. Kiberxavfsizlik bo'yicha chora-tadbirlar samaradorligi qanday o'lchanadi va kiberxavfsizlik ko'rsatkichlarini qanday yaxshilash mumkin?
5. Kiberxavfsizlik kontekstida jinoyat, tahdid, ekspluatatsiya va zaiflikni qanday aniqlash mumkin?
6. Kompyuter xavfsizligi sohasida jinoyatchilarning qanday turlari mavjud va ular tahdidlarni amalga oshirish uchun qanday zaifliklardan foydalanadilar?
7. Tahdidlar zararini oldini olish yoki kamaytirish uchun qanday xavfsizlik choralari texnologiyalari mavjud?
8. Xavfsizlikni boshqarishning maqsadi nima va u tashkilot rahbarlari uchun nima uchun muhim?
9. Agar rahbarlar yetarlicha tushuncha va hamkorlik qilmasdan xavfsizlikni boshqarishni mutaxassislarga topshirsalar qanday muammolar yuzaga kelishi mumkin?
10. Buxgalteriya hisobi va kiberxavfsizlik kasblarining tarix, standartlar va ishonch nuqtai nazaridan qanday farqlari bor?
11. UCF nima va u xavfsizlik menejerlariga turli xil xavfsizlik standartlariga muvofiqligini ko‘rsatishda qanday yordam berishi mumkin?
12. Xavfsizlik ma’lumotlarini import qilish va tahlil qilish uchun xavfsizlik ma'lumotlarini boshqarish (SIM) tizimidan foydalanishning afzalliklari va kamchiliklari qanday?
13. Kiberxavfsizlik siyosati va kiberxavfsizlik qonunlari va qoidalari o'rtasidagi farq nima?
14. Har bir davlatning kiberxavfsizlik siyosatini shakllantirishga qanday omillar ta’sir ko‘rsatadi?
15. Kiberxavfsizlik bo'yicha global shartnomalar, qonunlar va me'yoriy hujjatlardan qanday misollar keltira olasiz?
16. Xitoyning kiberxavfsizlik siyosati qanday va u qonun va qoidalarda qanday aks ettirilgan?
17. Kiberxavfsizlik bo'yicha qonunlar va me'yoriy hujjatlarni yaratish

va amalga oshirishda davlat organlari va sohani tartibga soluvchi organlar uchun qanday cheklovlar mavjud?

II BOB. KIBERXAVFSIZLIK SIYOSATI KATALOGI

2.1-§ Qaror qabul qiluvchilarga qo‘llanma.

Birlashgan Qirollik hukumati hozirda kiberxavfsizlikka katta sarmoya kiritmoqda, departamentlar endi kiberxavfsizlikning minimal standartini taqdim etishlari kerak. Departamentlarning yetukligi turlicha bo‘lib, bo‘limlar ushbu standart va undan yuqoriroq standartlardan xabardor va ularga erishishga intilishadi.

Bu bo‘lim Cyberthreat Intelligence (CTI) ni o‘rganmoqda va hozirgi eng yaxshi amaliyot “tahdidga asoslangan” yondashuvni qo‘llab-quvvatlamoqda. Bu bo‘limning tahdid qiluvchi aktyorlari kim bo‘lishi mumkinligini, ularning motivatsiyasi va qobiliyatini tushunishni va keyinchalik ular bo‘yicha amaliy ma’lumotlarni tarqatishni o‘z ichiga oladi. CTIning keng qamrovi sotuvchilardan ko‘plab mahsulotlar va xizmatlarni yaratishga turtki bo‘ldi. Biroq, bo‘limlar cheklangan CTI bilim va tajribasiga ega bo‘lishi mumkin, bu ularning tegishli asboblarni sotib olish qobiliyatiga va eng yaxshi amaliyotga mos keladigan muhitni yaratishga to‘sqinlik qiladi.

CTI qobiliyatiga ega bo‘limlar bir qator doiralar, byudjetlar va xususiyatlarga ega va ularning eng yaxshi amaliyotga muvofiq yetkazib berish qobiliyati har xil.

Maqsadli auditoriya. Ushbu qo‘llanma tahdidlarni razvedka qilish qobiliyatini nazorat qiluvchi yoki bo‘limga yetkazib beradigan shaxslarga qaratilgan. Ushbu hujjat CTI qobiliyatini taqdim etish bo‘yicha yo‘l xaritasini va zarur harakatlar, natijalar va texnologiyalar haqida umumiy ma’lumot beradi. Agar kerak bo‘lsa, texnik tafsilotlar kiritiladi.

Siz qaror qabul qiluvchi, guruh rahbari yoki tahlilchi bo‘lasizmi va har bir sohani o‘rganimiz. CTI haqida batafsil ma’lumot berilganda, bu tahdid razvedkasining hayot aylanishiga ko‘ra quyidagi bo‘limlarga bo‘linadi:

— Yo‘nalish;
— To‘plam;
— Qayta ishlash;
— Tahlil;
— Tarqatish.

Doimiy takomillashtirish va tashkil etish bo‘yicha qo‘shimcha bo‘limlar (shu jumladan resurslar bilan ta’minlash):

— Doimiy takomillashtirish;

— Tashkilot.

Kiber tahdidlar bo‘yicha razvedka. Cyberthreat Intelligence - kiberxavfsizlikni yumshatish bo‘yicha chora-tadbirlar to‘g‘risida ma’lumot berish uchun dushmanlarning motivlari, qobiliyati va ishlash usullarini tushunish orqali ta’sir ko‘rsatadigan tahdidlar haqida ma’lumotni tarqatish uchun kibermakondagi raqiblarga tegishli ma’lumotlarni to‘plash, qayta ishlash va tahlil qilish jarayoni hisoblanadi.

Tahdidlarni ovlash. Tahdid ovlash - bu IT tarmog‘iga ichki bo‘lgan va mavjud xavfsizlik nazoratidan qochgan kiber tahdidni proaktiv, iterativ va insonga yo‘naltirilganligini aniqlashdir.

Raqamli xavf va razvedka. Tashkilotning raqamli izini nazorat qilish orqali jamoat mulki ichidagi tahdidlarni kuzatish, aniqlash va bartaraf etish jarayonidir. Ushbu bob davlat idoralari raqamli xavf va razvedka qobiliyatlarini rivojlantirish va yetuklash orqali o‘zlarining raqamli izlarini qanday yaxshiroq tushunishlari va nazorat qilishlari bo‘yicha tavsiyalar beradi.

Ushbu bobda tavsiyalar uch darajaga bo‘lingan:

— *Tahdid razvedkasi jamoasi* - tez, osonroq amalga oshiriladigan, qisqa muddatli tavsiyalar;
— *Hukumat departamenti* - tahdid qobiliyatini kuchaytiradigan o‘rta muddatli tavsiyalar razvedka guruhlari;
— *Hukumatlararo funktsiyalar* - davlat idoralariga kelajak uchun raqamli izlarini yaxshiroq himoya qilish imkonini beradigan uzoq muddatli tavsiyalar.

Agar uchta imkoniyatni o‘zlashtirsak, quyidagi fikrlarga e’tibor berishni tavsiya qilamiz:

1. Har uchala qobiliyat minimal kiberxavfsizlik standartida ko‘rsatilgan imkoniyatlarning har biriga bo‘ysunadi. Agar minimal standart bajarilmasa, ushbu sohalarga investitsiyalar ushbu imkoniyatlardan ko‘ra foydaliroq bo‘lishi ehtimoli katta deb hisoblashadi.
2. Uchala sohada ham yetuk qobiliyatni yaratish biznes uchun katta sarmoyani anglatadi. Ayniqsa, davlat sektorida ushbu investitsiyani tekshirish yuqori darajada bo‘ladi va biz har bir sohada pul uchun haqiqiy qiymat mavjudligini ta’minlashni tavsiya qilamiz. Biz hamkorlik qilgan barcha tashkilotlarda ularning hech biri uchala qobiliyatni yangi tug‘ilgan davlatdan tashqarida rivojlantirish majburiyatini olmagan edi.

Ma’lumotlarga kirish va ma’lumotlarning ko‘rinishi *ichki* va *tashqi*

barcha funktsiyalar uchun juda muhimdir. Tashkilotingizdagi ma’lumotlarga kirishning o‘ziga xos shartlarini sarmoya kiritishdan oldin tushunishni tavsiya qilamiz. Maslahatlashgan boshqa tashkilotlar katta miqdorda sarmoya kiritgan va keyinchalik ma’lumotlarga kirish imkoni yo‘qligi sababli foydadan foydalana olmagan.

Yangi paydo bo‘lgan CTI va Threat Hunting qobiliyati, agar ular qo‘shimcha talablarga ega bo‘lsa, birgalikda rivojlanishi kerak. Razvedka bilan ta’minlash uchun CTI qobiliyatiga ega bo‘lmagan yetuk tahdidni ovlash qobiliyati cheklangan bo‘ladi va xuddi shunday tahdid ovchilari bo‘lmagan CSOCga ma’lumot beradigan CTI qobiliyati ham qiymat jihatidan cheklangan.

CTI funksiyasini yaratish. Bo‘limlar (hozirda) o‘z tarmoqlari yoki ma’lumotlarini to‘plash, integratsiya qilish yoki tahlil qilish uchun majburiy emas. NCSC minimal kiberxavfsizlik standarti minimal chora-tadbirlar majmuini taqdim etadi, jumladan: “Hech bo‘lmaganda, departamentlar ma’lum tahdidlarni aniqlash uchun umumiy tahdid razvedkasi manbalari, masalan, Cyber Security Information Sharing Partnership (CiSP) bilan birlashtirilishi mumkin bo‘lgan voqealarni yozib olishlari kerak”.

Bu shuni bildiradiki, bo‘limlar ma’lumotlarni (o‘z infratuzilmasi va qurilmalaridan) to‘plashi kerak, ammo CTI bilan integratsiya majburiy emas. Biroq, standart shuningdek, bo‘limlar iloji boricha standartlardan oshib ketishga harakat qilishlari kerakligini aytadi, shuning uchun hozirda tashkilotlar tahdid razvedkasi tarkibini iste’mol qilishlari shart emas, ularga buni qilish tavsiya etiladi.

Minimal standartlardan qat'i nazar, tahdidlar haqida ma’lumot allaqachon yetuk kiberxavfsizlik pozitsiyasiga ega bo‘lgan bo‘limlar uchun qimmatli bo‘lishi mumkin. CTI qiymatini taqdim etish qobiliyatiga tegishli zarur shartlar bo‘limdan bo‘limga farq qilishi mumkin bo‘lsa-da, biz diqqatga sazovor bayonot sifatida tashkilotlar CTIga sezilarli (ya’ni xavfsizlik byudjetining 5% dan ko‘prog‘i) investitsiyalarni faqat ular bajarilgandan keyin hisobga olishlarini tavsiya qilamiz yoki minimal kiberxavfsizlik standartining 10 ta bo‘limining barchasiga erishish uchun real yo‘l xaritasiga murojat qilamiz. CTI investitsiyalariga ajratilgan byudjet asoslanishi kerak.

CTI foydalanish holatlari. CTI bir necha usulda qo‘llanilishi mumkin. Bo‘lim o‘zining CTI qobiliyatini qanday yaxshilash bo‘yicha nisbatan qimmat va uzoq muddatli qaror qabul qilishdan oldin, u CTIdan foydalanish holatlarini tushunishi kerak. Quyida yettita asosiy

foydalanish holatlari aniqlangan:

2.1 jadval

CTIdan foydalanish

Foydalanish holati	**Maqsad**	**Intellekt talab qilinadi**
Tasdiqlash Signallar/hodisalar	Signallarni/hodisalarni tasdiqlang va qaysidur bir hodisaga javob berish guruhiga yetkazish va tuzatish uchun tanlang.	Tahdid ma'lumotlari: ma'lumotlar ulanishi individual ko'rsatkichlar, tahdid aktyorlar, texnikalar va boshqalar.
Yaxshilash Avtomatlashtirilgan Javob berish	Triaj jarayonini avtomatlashtirish Xavfsizlikka yordam berish orqali tekshiruvlar Axborot va tadbirlarni boshqarish (SIEM) va tahlil vositalarini to'g'ri taqdim etilgan signallar va hodisalarga ustuvor ahamiyat bering CTI yetakchisi/tahlilchisi.	Tahdid ma'lumotlari: tahdid ko'rsatkichlari va jiddiylik reytinglari bog'langan maxsus maqsadli hujumlar sanoat, ilovalar va boshqalar.
Xabar berish idoraviy Risk kasbi	Xavfsizlik kafolati va xavf darajasini oshiring kontekstli boshqaruv jarayoni, razvedka ma'lumotlarini mazmuni yig'ish	Tahdid ma'lumotlari: tahdid ko'rsatkichlari va jiddiylik reytinglari bog'langan maxsus maqsadli hujumlar sanoat, ilovalar va boshqalar.
Zaifliklarga ustuvorlik berish	Mavjud vaqt va resurslarni hisobga olgan holda, tuzatilishi mumkin bo'lgan muammolar va eng ko'p ta'sir ko'rsatadigan muammolar o'rtasidagi o'xshashlikni o'lchash orqali zaifliklarni baholash uchun ko'rsatkich yarating.	Zaiflik ma'lumotlari: ma'lum tarmoqlarga qarshi hujumlar bilan bog'liq CVE'lar, ma'lum tahdidlar bilan bog'liq CVE'lar va boshqalar.
ThreatHunting-	Joriy hodisalar yoki	Tahdid ma'lumotlari:

ni qo'llab-quvvatlash	bo'limga qaratilgan tahdidlar bilan bog'liq bo'lim tarmog'iga yashirin hujumlarni faol ravishda oching.	kampaniyalar, tahdid aktyorlari, texnikalar, tarix va maqsadlarga oid kontekstga bog'langan ko'rsatkichlar.
Tarkibida va Tuzatish Hujumlar	Tajovuzkor aloqalarini/buyruq va boshqaruvini buzing, zararli dasturlarni olib tashlang.	Tahdid ma'lumotlari: razvedka ma'lumotlari bazasi, shu jumladan turli xil tahdid guruhlari usullari, tarixi va maqsadlari haqidagi ma'lumotlar.
Fishingga qarshi	Aniqlash ma'lumotlar to'plamini ko'rsatkichlar bilan boyitish orqali mavjud pochtani himoya qilish imkoniyatlarini yaxshilang.	Tahdid ma'lumotlari: kampaniyalar, tahdid aktyorlari, texnikalar, tarix va maqsadlarga oid kontekstga bog'langan ko'rsatkichlar.

Ushbu indikativ foydalanish holatlari CTI funktsiyasi amalga oshirishi mumkin bo‘lgan faoliyat turlari haqida umumiy ma’lumot beradi. Agar sizning bo‘limingizda ushbu foydalanish holatlarining birortasini yetkazib berishga ishtaha bo‘lmasa, CTI sizning bo‘limingiz ehtiyojlarini qondiradimi yoki yo‘qligini o‘ylab ko‘rishingiz kerak. Ushbu bo‘limning qolgan qismi ushbu foydalanish holatlarini va kengroq CTI qobiliyatini bo‘limga yetkazish uchun yo‘l xaritasini taqdim etadi.

Yo‘l xaritasi. Yangi CTI qobiliyatini rivojlantirish uchun mavjud yoki minimal yangi kiberxavfsizlik resurslaridan foydalangan holda bir necha qadamlar qo‘yilishi mumkin.

Tahdidlarni baholash sizning tahdid profilingiz haqida ma’lumot beradi va CTI funktsiyalari maqsadlariga erishish uchun qancha odam talab qilinishi haqida ko‘rsatma beradi. CTI jamoasi quyidagi **uchta** roldan boshlashi mumkin (uchta shaxs emas) yoki ular boshqa rollarning funktsiyalari sifatida bajarilishi mumkin:

1. Funktsiyani boshqaradigan va boshqaradigan CTI rahbari strategiyani yetkazib berish uchun mas'uldir va kerak bo‘lganda boshqaruv kengashi, yuqori boshqaruv va tizim egalariga razvedka ma’lumotlarini yetkazib beradi.

2. Avtomatlashtirilmagan manbalardan (masalan, sanoat hujjatlari)

ma’lumotlarni to‘playdigan, tahlil qiladigan va qayta ishlovchi CTI tahlilchisi va tahdidlarni baholashda aniqlangan tahdid subyektlari faoliyatini profillash uchun mas’uliyatni o‘z zimmasiga oladi.

3. Texnik razvedka ma’lumotlarini to‘playdigan, qayta ishlovchi va tahlil qiluvchi va CSOC bilan maxsus aloqa nuqtasini ta’minlovchi CTI tahlilchisi.

Ushbu tahlilchi tahdid ishtirokchilarining profilini aniqlashni qo‘llab-quvvatlaydi, ammo ularning asosiy mas’uliyati CSOC va boshqa himoyachilarga texnik razvedka ko‘rsatkichlarini saqlash va yetkazib berish bo‘ladi.

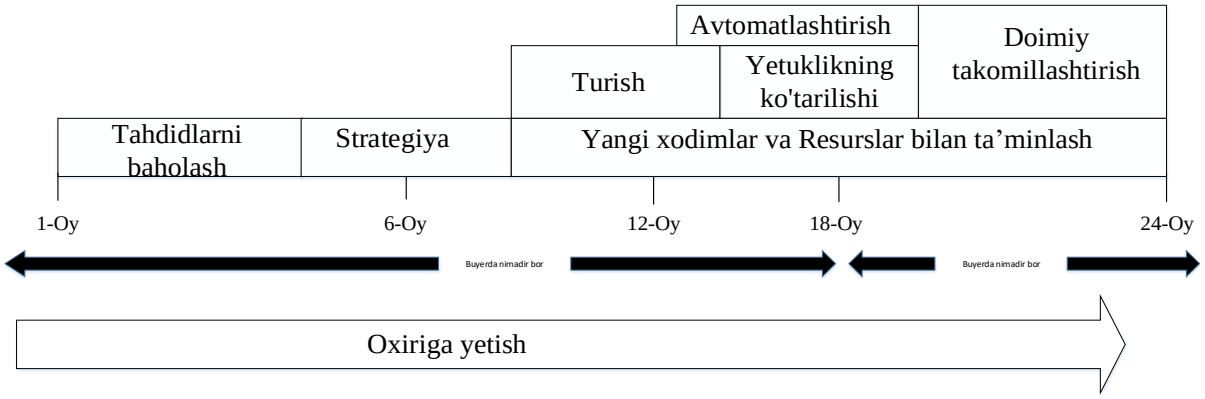
Yetkazib beriladigan narsalaringizni yetuklashtirish. CTI funktsiyasining maqsadi uning bo‘limiga tegishli razvedka ma’lumotlarini taqdim etishdir. Bu (ayniqsa, yangi paydo bo‘lgan qobiliyatda) CTI funksiyasining ilg‘or doimiy tahdidlardan (APT) nol kunlik hujumlarini tahlil qiluvchi razvedka tekshiruvining eng yuqori bosqichida bo‘lishini talab qilmaydi.

Avtomatlashtirish. Hisobotlar va brifinglarga qo‘shimcha ravishda, kiber tahdidlar bo‘yicha razvedkaning asosiy qismi CSOCga texnik razvedka ma’lumotlarini yetkazib berishdir. Asosiy masala shundaki, bu makonda qayta ishlash uchun juda ko‘p ma’lumotlar mavjud va bir qator bo‘limlar kontentning “o‘t o‘chiruvchisi” bilan samarali kurasha olmaydi.

Bizning tavsiyamiz ikki xil usuldan iborat:

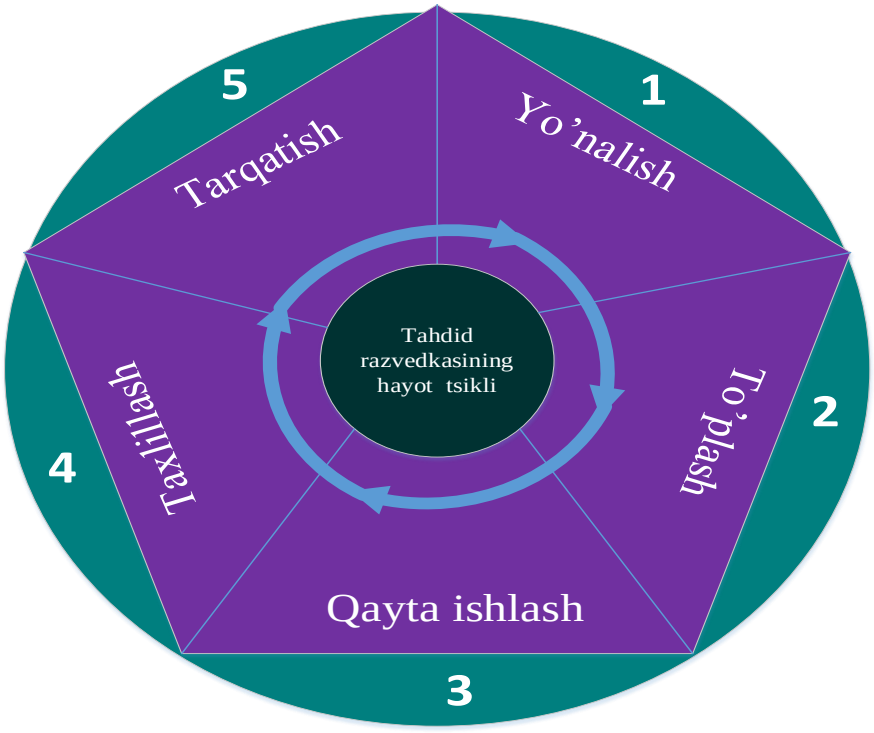
— Ochiq manbali texnologiyalardan foydalangan holda texnik razvedkaning foydaliligini o‘rganish,(masalan zararli dasturiy ta’minot haqida ma’lumot almashish loyihasi (MISP) va SIEM vositangizning mavjud imkoniyatlari. Bu sizning bo‘limingizga texnik ma’lumotlarni qayta ishlashga qo‘yiladigan talablarni va tizimning integratsiya talablari va ma’lumotlar hajmi kabi funktsional bo‘lmagan jihatlarini samarali aniqlash imkonini beradi.

— CiSP kabi platformalar yoki ishonchli provayderlarning tasmasi orqali markazlashtirilgan ma’lumotlardan imkon qadar ko‘proq foydalaning. Rivojlanayotgan tahdid landshafti haqida vaziyatdan xabardor bo‘lish uchun mavjud tahdidlar tasmasi ishlatilishi kerak.



2.1-rasm. CTIni rivojlantirish bo'yicha yo'l xaritasi

Narxi. Cyberthreat Intelligence - bu maxsus qobiliyat bo‘lib, u kiber va an’anaviy xavfsizlik rollarida mavjud xavfsizlik qobiliyati bilan bir qatorda o‘rnatiladi. Yuqorida aytib o‘tilganidek, CTI ushbu funktsiyalarni bo‘limni yaxshiroq himoya qilish imkonini beradi va ular allaqachon yetuk operatsion holatda bo‘lmagan holda cheklangan qiymatga ega. Binobarin, ushbu funktsiyalarga ajratilgan byudjetni CTI qobiliyatini moliyalashtirish uchun qayta yo‘naltirish tavsiya etilmaydi. CTIni mustaqil ravishda moliyalashtirilishi kerak.



2.2-rasm. Tahdid razvedkasining hayot sikli

Ta’riflar, qo‘llanilish doirasi va tuzilishi. Kiber tahdidlar bo‘yicha razvedka.

Cyberthreat Intelligence bir nechta ta’riflarga ega, ammo ushbu qo‘llanma maqsadlari uchun quyidagi ta’rifdan foydalaniladi:

“Kibertahdid razvedkasi bu kiberxavfsizlikni yumshatish chora-tadbirlari to‘g‘risida ma’lumot berish uchun dushmanlarning motivlari, qobiliyati va operandisini tushunish orqali ta’sir etuvchi tahdidlar haqida ma’lumotni tarqatish maqsadida kibermakondagi dushmanlar haqidagi ma’lumotlarni yig‘ish, qayta ishlash va tahlil qilish jarayonidir”.

Bir qator o‘zgarishlar mavjud bo‘lsa-da, ushbu kitobda 5 bosqichdan iborat hayot tsiklidan foydalanadi:

— Yo‘nalish;
— To‘plash;
— Qayta ishlash;
— Tahlil qilish;
— Tarqatish.

Tashkiliy yetkazib berish darajalari. Tashkiliy /bo‘lim faoliyati odatda uch darajaga bo‘linadi:

— Strategik;
— Operativ;
— Taktik.

CTI kontekstida to‘rtinchi daraja - texnik - odatda qo‘llaniladi.

Strategik CTI yuqori darajadagi va biznesga yo‘naltirilgan bo‘lib, odatda nasr shaklida, masalan, bo‘limdagi yuqori boshqaruv guruhlariga (SMT) qaratilgan hisobotlar yoki taqdimotlar shaklida bo‘ladi.

Strategik CTIning maqsadi SMTga bo‘limga tahdidlar to‘g‘risida tushuncha berish orqali ongli biznes qarorlarini qabul qilishda yordam berishdan iborat bo‘lib, ular keyinchalik o‘rnatilgan strategik risklarni boshqarish va resurslarni boshqarish jarayonlariga kiradi.

Strategik CTIning umumiy manbalariga geosiyosiy ishlar, sanoat oq qog‘ozlari va ishonchli tarmoqlar kiradi.

Operatsion CTIning umumiy manbalariga tahdidlar haqida hisobotlar, hodisalar haqida hisobotlar, zararli dasturlarni tahlil qilish va vaqti-vaqti bilan ijtimoiy media va suhbat xonalari kiradi.

Yo‘nalish. Ushbu bo‘lim tahdid razvedkasi hayotiy tsiklining birinchi bosqichi - yo‘nalishning umumiy ko‘rinishini taqdim etadi. Yo‘nalish bo‘yicha berilishi mumkin bo‘lgan bo‘lim ichidagi turli mijozlardan strategik, operatsion va taktik daraja talab qiladi.

Yo‘nalish foydali CTI funktsiyasini taqdim etishning eng muhim bosqichidir, chunki u keyingi barcha bosqichlarni boshqaradi. Keyingi bosqichda o‘zgarishlarning ta’sirini minimallashtirish uchun talablarni boshidanoq to‘g‘ri yig‘ish uchun harakat qilish kerak.

Kibertahdidni baholash. CTI jamoasining maqsadlarini tushunish uchun bo‘lim birinchi navbatda o‘zining tahdid profilining asosiy ko‘rinishiga ega bo‘lishi kerak. Tahdidlarni o‘rganish strategiyasini ko‘rib chiqishda, yetuk kibertahdidlarni baholash (TA) bo‘limlar uchun asosiy yo‘l-yo‘riq bo‘lishi kerak.

Tahdidlarni baholashning oldingi usullari va yetuk kibertahdidlarni baholash o‘rtasidagi asosiy farqlar quyidagi jadvalda ko‘rsatilgan:

2.2-jadval

O‘tgan TA va yetuk Cyber TA

O'tgan Tahdidni baholash	**Yetuk kiber tahdidlarni baholash**
Funktsional ahamiyatidan qat'i nazar, tahdid qiluvchilarning keng doirasi ko'rib chiqiladi (masalan, radio ixlosmandlari).	Faqat bo'limga hujum qilish qobiliyati va motivatsiyasi bo'lgan tahdid qiluvchi shaxslar batafsil baholanadi.
Tahdid qiluvchilar qo'pol tarzda guruhlangan (masalan, “Xorijiy razvedka xizmatlari (FIS)” yoki “Uyushgan jinoyatchilik guruhlari (OCG)”).	Har qanday rasmiy belgidan qat'i nazar, qobiliyat va motivatsiyaga bog'liq holda alohida ko'rib chiqiladi.
Departament aktivlari biznesga ta'sir qilish darajasi nuqtai nazaridan qo'pol ko'rib chiqiladi.	Biznes haqida chuqur tushuncha mavjud va muhim biznes aktivlari alohida xavf omillari va hujum stsenariylari bilan alohida ko'rib chiqiladi.
FIS kabi tahdidlar ko'pincha “rasmiy doiradan tashqarida” deb hisoblanadi.	Ko'pgina tahdid guruhlari tijoratda mavjud bo'lgan, aniqlanishi mumkin bo'lgan hujumlardan foydalanayotgani va ularning imkoniyatlari to'g'risidagi razvedka muhim ahamiyatga ega ekanligi e'tirof etilgan.

Tahdidni baholash jarayoni. Birinchi mashq bu bo‘lim o‘zining muhim aktivlarini tushunishini ta’minlashdir. Ko‘pgina yirik bo‘limlar uchun bu aktivlar turli joylarda va muhitlarda yashashi mumkin bo‘lgan tizimlar, tarmoqlar, ma’lumotlar to‘plamlari va platformalarni o‘z ichiga olishi mumkin. Texnik nuqtai nazardan muhim aktivlar konfiguratsiyani

boshqarish, ma’lumotlar bazasida (CMDB) qayd etilishi mumkin bo‘lsa-da, ushbu aktivlarni ustuvorlashtirish mashqlari nomoddiy aktivlar vintellektual mulkni ham o‘z ichiga olishi kerak.

Departament aktivlarining ko‘rinishi olingandan so‘ng, aktivlar bo‘lim uchun ularning ahamiyati sifatida baholanishi mumkin, bu esa ushbu aktivlarning yo‘qolishi qiymatini ko‘rish imkonini beradi.

2.3- jadval

Kirish ichiga tahdidni baholash.

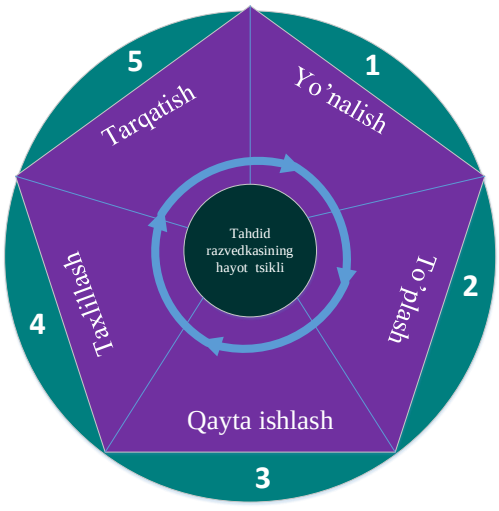
Kirish manbai	**Tavsif**
IncidentResponseReports	Ilgari muvaffaqiyatga erishgan hujumchilarni tushunish muhim, chunki bu raqiblar qaytib kelishlari mumkin. Oldingi hujumlarning vositalari, texnikasi va jarayonlari tahdid razvedkasini tahlil qilish va xavfni yanada yumshatish haqida ma'lumot berishi mumkin. IR hisobotlari, shuningdek, yaqin orada o'tkazib yuborilgan yoki tasdiqlanmagan murosa mazmunini o'z ichiga olishi mumkin.
Penetratsiya testi Hisobotlar	Penetratsion testlar (zaiflikni baholash yoki qizil jamoaviy faoliyat) hujumga moyil bo'lgan funksiyalar yoki tizimlarni aniqlashga qaratilgan. Ushbu ma'lumotni kengroq razvedka rasmiga qo'shish mumkin. Vaqt o'tishi bilan tahdidlar landshafti va bo'lim tizimlari o'zgaradi va bo'limlar bu baholashlar noto'g'ri bo'lib qolishidan ehtiyot bo'lishlari kerak, chunki har bir test tizimdagi zaifliklarni vaqt nuqtai nazaridan ko'rib chiqadi.
Mutaxassis maslahati	Yuqoridagi bo'limda muhokama qilinganidek, CTI mutaxassislari tahdidlar manzarasini xolis ko'rishlari va sizning bo'limingiz uchun asosiy tahdidlardan xalos bo'lishlari mumkin. KO'K ko'rsatkichlari va xulq-atvor namunalarini kuzatish uchun keng doiradagi bo'limlar va kontekstlardagi tajribadan foydalanishi mumkin.
Kafedra ekspertizasi	Bo'limni topshirishning “o'tkir oxirida” bo'lganlar, shuningdek, bo'lim duch keladigan tahdidlarni, hatto maxsus xavfsizlik rollaridan tashqarida bo'lganlarni ham ko'rishadi. Bunga ishlab chiquvchilar, ma'murlar, biznes menejerlari yoki yuridik a'zolar kirishi

	mumkin. C darajasi ham xuddi shunday ko'rinishga ega bo'ladi. Ushbu a'zolardan ma'lumot olish tahdidlarni tushunish uchun qimmatli bo'lishi mumkin. Ularning to'g'ri talqin qilinishi va ustuvorligini ta'minlash uchun ehtiyot bo'lish kerak.
Manfaatdor tomonlarning seminarlari	Bo'lim a'zolari, yetkazib beruvchilar va tashqi tomonlar (masalan, NCSC) o'rtasida tahdidlarni jamoaviy muhokama qilish tahdid modeliga foydali ma'lumotlarni taqdim etishi va bo'lim doirasini yaxshiroq tushunishi mumkin.

Mijozlarning CTI uchun maxsus so‘rovlari ham talablarni kuchaytiradi. Ushbu so‘rovlarni samarali boshqarish uchun barcha kerakli ma’lumotlarni olish uchun ishlab chiqarilgan shablon bilan RFI jarayoni aniqlanishi kerak.

Bu quyidagi kabi maydonlarni o‘z ichiga olishi mumkin:

— So‘rovchi tafsilotlari;
— Tomonidan talab qilingan sana;
— Talab uchun asos;
— Xulosa talablari;
— Batafsil talablar;
— Kechikishning ta’siri;
— Maqsadli tarqatish.



To‘plash. Threat Intelligence Lifecycle yo‘nalishi bosqichida belgilangan talablarni bajarish uchun ma’lumotlar to‘planishi kerak. To‘plam ulardan biri to‘g‘ri olish uchun CTIning eng qiyin bosqichlari tegishli ma’lumotlarning ko‘plab turli manbalardan tegishli miqdorda to‘planishini ta’minlash asosiy muammo hisoblanadi. Ushbu bo‘limda ma’lumotlarni yig‘ishning turli usullari va har birining foydaliligi o‘rganiladi. Ushbu bo‘lim *ikkita* asosiy sohaga bo‘lingan:

— odatda qo‘lda to‘planadigan ma’lumotlar;
— avtomatlashtirilgan vositalar yordamida to‘plangan ma’lumotlar.

CTI tarkibi amalda bo‘lishi kerak, bu esa o‘z navbatida tegishli, o‘z

vaqtida va to‘g‘ri bo‘lishi kerakligini anglatadi. CTI funktsiyasi millionlab IOClarni, katta hajmdagi ma’lumotlar va tasmalardan ma’lumotlarni nisbiy osonlik bilan qabul qilishi mumkin, ammo agar bu mijozlar tomonidan amalga oshirilmasa, bu funktsiya resurslariga yuk bo‘ladi. Shuning uchun to‘plangan tarkib CTI funktsiyasini tiklaganda diqqat qilish kerak bo‘lgan eng muhim sohalardan biridir.

Qo‘lda to‘plash. Ma’lumotni qo‘lda yig‘ishning turli mexanizmlari mavjud, ammo ko‘p qiymatga ega bo‘lishning kaliti yig‘ish jarayonlarining standartlashtirilganligini ta’minlashdir. Qo‘lda to‘plangan ma’lumotlarning asosiy elementlari qayd etilishi kerak:

- Sana va vaqt;
- Tegishli prognoz vaqtlari;
- Yig‘ilgan ma’lumotlarning tabiati;
- Maxsus texnik yozuvlar.

CTI almashish tarmoqlari. CTI almashish tarmoqlari amaliyotchilar o‘rtasida rasmiy yoki norasmiy tahdid haqida ma’lumot almashishni anglatadi.

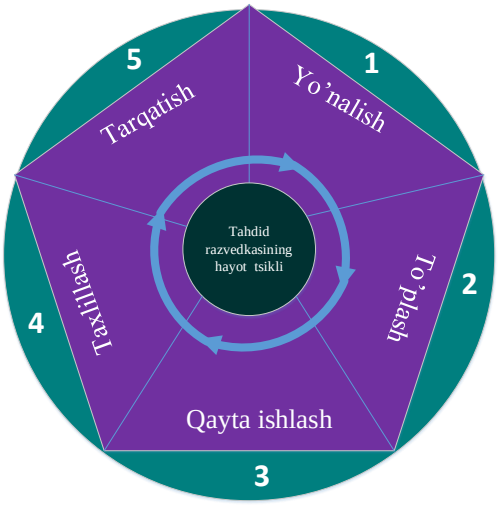
Bu davlat idoralarida keng tarqalgan amaliyot, masalan, ilgari harbiy yoki razvedka idoralarida ishlagan, hozir esa xususiy sektorda yoki davlat idoralarida ishlayotganlar o‘rtasida tarmoqlar mavjud.

Ochiq manbali razvedka. Open Source Intelligence (OSINT) Internetdagi yoki ommaviy axborot vositalaridagi ma’lumotlar kabi ochiq manbalardan ma’lumotlarni to‘plashni anglatadi. Ushbu ma’lumotlar tahlilchilar uchun ochiqdir;

OSINT quyidagilarni o‘z ichiga olishi mumkin (lekin ular bilan cheklanmaydi):

- Ijtimoiy media;
- Ijtimoiy media tomonidan nashr etilgan tahdid ma’lumotlarini kuzatish mumkin;
- Tadqiqotchilar ;
- Tijorat CTI provayderlari yoki hatto tahdid qiluvchi guruhlar uchun so‘zlovchilar.

Ijtimoiy tarmoqlardan to‘plangan razvedka ma’lumotlariga ishonch hosil qilish uchun tekshirish kerak.



Qayta ishlash. Barcha to‘plangan ma’lumotlar to‘plami faqat ularning mazmuni kabi yaxshi. Qayta ishlash to‘plangan ma’lumotlarning mazmuni tahlilchilar uchun eng foydali ma’lumotlar mavjudligini ta’minlash uchun tarkibni boyitadi. Kontentni qayta ishlashda uchta asosiy fikr mavjud:

— Obro‘: bu ma’lumot manbasi qanchalik ishonchli;
— Muvofiqlik: tarkib sizning bo‘limingizga tegishlimi;
— Sifat: foydali bo‘lishi uchun etarli sifatli tarkib bormi.

Ushbu bo‘lim tahlil uchun ma’lumotni yaxshiroq ta’minlash va mavjud ma’lumotlar hajmini boshqarish uchun tarkibni qanday qilib eng yaxshi boyitish kerakligini tasvirlaydi.

Obro‘. Barcha ma’lumotlar manbaning obro‘si kontekstida qayta ishlanishi kerak. Misol uchun, agar ma’lumot ishonchli kontaktdan olingan bo‘lsa, u tasdiqlanmagan Twitter akkauntidan olinganidan yuqoriroq bo‘lishi mumkin va bu tamoyil tahdidlar tasmasi uchun kengaytirilishi kerak. Shunday qilib, mazmunni farqlash uchun asosiy savol “Ushbu ma’lumotlarning manbasi qanchalik ishonchli?” Ushbu jarayonni standartlashtirish uchun kontentning obro‘si uchun ko‘rsatkich yaratilishi va birlashtirilishi mumkin.

CTI manbasi uning imkoniyatlari yoki tarixini texnik baholash asosida ishonchliligi uchun baholanadi. Ishonchlilik belgisi A dan F gacha bo‘lgan oltita belgidan birini ishlatadi:

A. To‘liq ishonchli: haqiqiylik, ishonchlilik yoki malakaga shubha yo‘q; to‘liq ishonchlilik tarixiga ega.

B. Odatda ishonchli: haqiqiylik, ishonchlilik yoki malakaga nisbatan kichik shubha; bor ko‘pincha haqiqiy ma’lumotlar tarixi.

C. Juda ishonchli: haqiqiyligi, ishonchliligi yoki malakasiga shubha, lekin o‘tmishda to‘g‘ri ma’lumot bergan.

D. Odatda ishonchli emas: haqiqiylik, ishonchlilik yoki malakaga nisbatan jiddiy shubha, lekin o‘tmishda to‘g‘ri ma’lumot bergan.

E. Ishonchsiz: haqiqiylik, ishonchlilik va malakaning etishmasligi; bekor qilish tarixi ma `lumot.

F. Ishonchlilikni baholash mumkin emas: manbaning ishonchliligini

baholash uchun hech qanday asos yo‘q. Ishonchlilik:

CTI manbasining ishonchliligi boshqa manbalar tomonidan tasdiqlash ehtimoli va darajalariga qarab baholanadi. Ishonchlilik belgisi 1 dan 6 gacha bo‘lgan oltita raqamdan birini ishlatadi:

1. Boshqa manbalar tomonidan tasdiqlangan: boshqa mustaqil manbalar tomonidan tasdiqlangan; o‘z-o‘zidan mantiqiy; Mavzu bo‘yicha boshqa ma’lumotlarga mos keladi.

2. Ehtimol, rost: tasdiqlanmagan; o‘z-o‘zidan mantiqiy; mavzu bo‘yicha boshqa ma’lumotlarga mos keladi.

3. Ehtimol rost: tasdiqlanmagan; o‘z-o‘zidan oqilona mantiqiy; mavzu bo‘yicha ba’zi boshqa ma’lumotlar bilan rozi.

4. Shubhali: tasdiqlanmagan; mumkin, lekin mantiqiy emas; mavzu bo‘yicha boshqa ma’lumotlar yo‘q.

5. Imkoniyatsiz: tasdiqlanmagan; o‘zi mantiqiy emas; mavzu bo‘yicha boshqa ma’lumotlarga zid.

6. Haqiqatni hukm qilib bo‘lmaydi: ma’lumotlarning to‘g‘riligini baholash uchun hech qanday asos yo‘q.

Muvofiqligi. Yig‘ilgan ma’lumotlar CTI funktsiyasi va uning talablariga mos kelishi kerak. Tegishli manbalar uchun ham (masalan, NCSC tahdid tasmasi), taqdim etilgan kontentning hammasi ham foydali bo‘lmasligi mumkin. Tahlilchilarga ozuqani boshqarish uchun ahamiyatliligini baholash uchun obro‘ga o‘xshash ko‘rsatkichlardan foydalanish tavsiya etiladi, ammo NATO tizimida tegishlilik uchun hech qanday ko‘rsatkich yo‘q. Tahdid tasmasi ko‘pincha turli xil tarkibni o‘z ichiga oladi – masalan, ko‘plab tahdidlar tasmalari korporativ emas, balki jismoniy shaxslarga mo‘ljallangan to‘lov dasturi bilan bog‘liq kontentni o‘z ichiga oladi

Sifat. CTIni qayta ishlashda e’tiborga olinadigan yakuniy e’tibor to‘plangan ma’lumotlarning sifati hisoblanadi. Ko‘rib chiqiladigan asosiy yo‘nalishlarga quyidagilar kiradi:

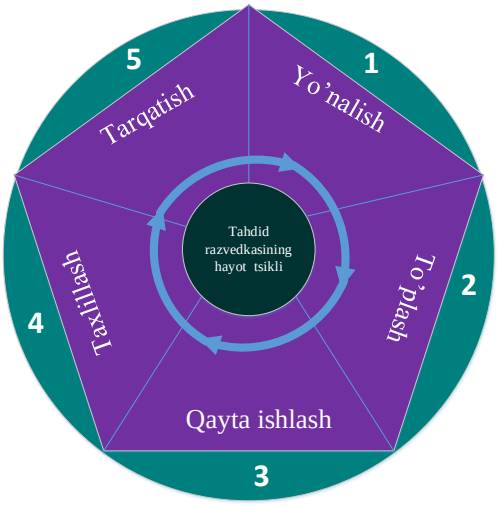
- Kontent formati, masalan, IPv4 manzillari XXX.XXX.XXX.XXX bo‘lishi kerak;
- Kontentning bog‘langan konteksti;
- Tarkibning yoshi;
- Tarkibning aniqligi, ya’ni noto‘g‘ri pozitivlardan farqli ravishda “haqiqiy” XOQ; Tasmadagi yangilanishlar chastotasi.

Ma’lumotlarning tegishli formatlarda to‘planishini ta’minlashni hisobga olish kerak. Noto‘g‘ri formatlangan ma’lumotlarni taqdim etuvchi manbalar doimiy ravishda mos keladigan (va shuning uchun

avtomatik ravishda qayta ishlanadigan) formatlarda kontent taqdim etadiganlarga nisbatan past sifat sifatida ko‘rilishi kerak. Masalan, ko‘rsatkichlar har doim maxsus formatlash qoidalariga ega bo‘ladi; IPv4 manzillari XXX.XXX.XXX.XXX formatida bo‘lishi kerak va domen nomlarida doimo @ bo‘ladi. Tasma tomonidan taqdim etilgan bog‘liq kontekst uning sifatiga hissa qo‘shishi kerak. Agar tasma faqat IP-manzil ko‘rsatkichlari haqida muntazam ravishda xabar bersa, bu IP ko‘rsatkichi bilan bog‘liq tahdidlar, kampaniya va domenlar kabi to‘liq kontekstli ma’lumotni taqdim etuvchi tasmaga qaraganda pastroq sifat sifatida ko‘rib chiqilishi kerak.

Kontentning yoshi ham muhim ahamiyatga ega va uni XOQ turi kontekstida qayta ishlash kerak, masalan, IP-lar qisqa umrga ega, xeshlar uzoqroq muddatga ega va hokazo. Foydalanish muddati o‘tgan kontentni muntazam ravishda ta’minlovchi tahdidlar tasmasi ustuvorlikdan chiqarilishi kerak. Bu tajovuzkorlar hujumkor infratuzilmani muntazam ravishda aylantirib turadigan bulut kontekstida aniq ko‘rinadi.

Tahlillash. CTI mahsulotlarini ishlab chiqarish uchun to‘plangan ma’lumotlarni tahlil qilish kerak. Razvedka mutlaq aniqlikni ta’minlay olmaydi. Shuning uchun har qanday xulosalar mavjudligini ta’minlash uchun sinchkovlik bilan tahlil qilish muhimdir. Tahlil bosqichining maqsadi qayta ishlangan tarkibni olish va uni CTI funktsiyasi mijozlari va hamkorlari tomonidan iste’mol qilish uchun amalda bo‘ladigan razvedka mahsulotlariga aylantirishdan iborat.



Tarqatish. Tarqatish mahsulotlarni tahlil bosqichidan oladi va ularni strategik, operatsion va taktik darajalarda CTI funktsiyasining tegishli mijozlariga tarqatadi. Ichki hisobotlardan alohida bo‘limlar, shuningdek, sanoat yoki jamoa ichidagi hujumlarning oldini olish uchun tegishli CTI (ayniqsa, operatsion va taktik CTI) ni tashqaridan baham ko‘rishning afzalliklarini hisobga olishlari kerak. Bir bo‘limga hujum haqida umumiy ma’lumot, masalan, ma’lum bir tahdid ishtirokchisi, ularning motivlari, infratuzilmasi , TTP va XOQga tegishliligi, boshqa bo‘limlarga mudofaa holatini yaxshilash va murosaga kelish xavfini kamaytirish imkonini beradi.

CTI mahsulotlarini taqsimlash. Tarqatish usuli va formati

mijozdan mijozga ularning moslashtirilgan CTI talablariga javob berishi uchun farq qiladi. Masalan, hukumatga hujumlar tendentsiyasi to‘g‘risida yuqori darajadagi nasr hisoboti SMTga elektron pochta orqali taqdim etilishi mumkin; Tegishli tahdid ishtirokchisining TTPlari bo‘yicha past darajadagi PDF nasriy hisoboti xavfsizlik boshqaruvi va voqealarga javob berish guruhiga elektron hujjatlar va yozuvlarni boshqarish tizimi (EDRMS, masalan, SharePoint) orqali taqdim etilishi mumkin; va tasdiqlangan XOQlar STIX/TAXII orqali CSOC va Network Operations Center (MOC) ga taqdim etilishi mumkin. CTI ning tajovuzkor ichki tarqalishi funktsiyadan olingan foydani optimallashtirish uchun kalit hisoblanadi. Muhokamalardan birida barcha xodimlarning taxminan 25% elektron pochta orqali CTI mahsulotining qandaydir shaklini olgan bo‘limni aniqladi. So‘ralgan barcha bo‘limlar bo‘ylab CTI ning taqsimlanishi uning foydaliligi uchun juda muhim ekanligi qayd etildi.

Ishonch munosabatlari. CTIni ulashish yuqorida aytib o‘tilganidek, ko‘plab afzalliklarga ega; ammo, bu, ehtimol, bo‘limlar o‘rtasida nozik ma’lumotlarni to‘g‘ridan-to‘g‘ri yoki bilvosita almashishni talab qiladi. Ushbu almashish bo‘limlar o‘rtasida ishonch darajasini o‘rnatishni talab qiladi, bunda baham ko‘rilgan ma’lumotlar tegishli tarzda qayta ishlanadi va faqat aniq ruxsat etilgan maqsadlarda foydalaniladi. Shuningdek, tahdid qiluvchi sub’ektlarning bilimlarini almashish bilan bog‘liq xavf elementi ham mavjud, masalan, agar tahdid ishtirokchisi TTP aniqlanganligi va unga qarshi choralar ko‘rilganligini aniqlasa, ular yangi va noma’lum TTPga o‘tishlari mumkin.

Ishonchni o‘rnatish usullaridan biri yopiq almashish forumlaridir. Misol uchun, CiSP qaysi nodavlat tashkilotlar a’zo bo‘lishi mumkinligini tanlaydi, MISP esa o‘zboshimchalik bilan ishonch guruhlarini yaratishga imkon beradi. Yuqoridagi mulohazalarni e’tiborga olish kerak bo‘lsa-da, asosan CTIning muvaffaqiyati barcha iste’molchilar undan foydalanishi mumkin bo‘lgan holda foydalanishi mumkinligini ta’minlash uchun kontentni tezda almashishdir. Bu odatda hamkorlik qilmaydigan kompaniyalar o‘rtasida munosabatlarni yaratishni talab qilishi mumkin, masalan, bir xil tarmoqlardagi to‘g‘ridan-to‘g‘ri raqobatchilardir.

Svetofor protokoli. Svetofor protokoli Buyuk Britaniyaning Milliy infratuzilma xavfsizligini muvofiqlashtirish markazi, Milliy infratuzilmani himoya qilish markazi (CPNI) ga asoslanib, maxfiy ma’lumotlarni almashishni rag‘batlantirish va ishonchni o‘rnatishga yordam berish uchun o‘rnatildi. Joriy standart endi Incidents Response and Security Teams Forum (FIRST) standartlari ta’riflari va foydalanish

bo‘yicha qo‘llanma tomonidan belgilangan. TLP almashish chegaralarini belgilash va nozik ma’lumotlarni qachon va qanday almashish mumkinligini ko‘rsatish uchun to‘rtta rangdan foydalanadi. U inson tomonidan o‘qiladigan ma’lumotlar uchun optimallashtirilgan, ammo STIX va MISP ham TLPni o‘z ichiga olgan. TLP ning muhim tamoyillari shundan iboratki, manba qabul qiluvchilarning TLP belgilarini tushunishi va ularga mos kelishini ta’minlash uchun mas'uldir va qabul qiluvchilar TLP belgilari ko‘rsatganidan ko‘ra kengroq bo‘lishishdan oldin manbadan aniq ruxsat so‘raydi.

To‘rtta TLP belgilari:

- TLP: QIZIL - oshkor qilish uchun emas, faqat ishtirokchilar uchun cheklangan;
- TLP: AMBER - cheklangan oshkor qilish, ishtirokchilarning bo‘limlari yoki tashkilotlari uchun cheklangan ;
- TLP: Yashil - cheklangan oshkor qilish, ma’lum bir ma’lumot almashish hamjamiyatiga cheklangan;
- TLP: OQ - oshkor qilish cheklanmagan.

Hukumat xavfsizligi tasnifining CTI uchun muvofiqligi. Hukumat xavfsizligi tasniflari Hukumatning Himoya Markalash Sxemasining (GPMS) o‘rnini bosadi. GSC ma’lumotlarning sezgirligini ko‘rsatadi va aktivlarni tegishli tarzda himoya qilish uchun zarur bo‘lgan asosiy xavfsizlik nazoratini (ma’muriy, jismoniy va mantiqiy) belgilaydi. GSC quyida tavsiflanganidek uchta tasnifga ega:

- RASMIY - Davlat sektori tomonidan yaratilgan yoki qayta ishlanadigan ma’lumotlarning aksariyati. Bu odatiy biznes operatsiyalari va xizmatlarini o‘z ichiga oladi, ularning ba’zilari yo‘qolsa, o‘g‘irlansa yoki ommaviy axborot vositalarida e’lon qilinsa, zararli oqibatlarga olib kelishi mumkin, ammo yuqori xavf profiliga tobe bo‘lmaydi. Ba’zi RASMIY ma’lumotlar ayniqsa sezgir bo‘lib, “bilish kerak” tamoyilini amalga oshirish uchun qo‘shimcha nazorat vositalarini talab qiladi - bu RASMIY SEZOR deb belgilanishi kerak;
- SECRET - o‘ta sezgir ma’lumot, bu aniq va yuqori qobiliyatli tahdid subyektlaridan himoya qilish uchun kuchaytirilgan himoya choralarini oqlaydi. Masalan, murosaga kelish harbiy imkoniyatlarga, xalqaro munosabatlarga yoki og‘ir uyushgan jinoyatchilikni tergov qilishga jiddiy zarar etkazishi mumkin bo‘lgan hollarda;

— TOP SECRET - Eng jiddiy tahdidlardan yuqori darajadagi himoyani talab qiladigan eng nozik ma’lumotlari.

Masalan, murosa keng ko‘lamli odamlarning yo‘qolishiga olib kelishi yoki mamlakat yoki do‘st davlatlar xavfsizligi yoki iqtisodiy farovonligiga tahdid solishi mumkin bo‘lgan hollarda.

GSC davlat ma’lumotlarining tegishli tarzda himoyalanishini ta’minlash uchun ishlab chiqilgan. Bu shuni anglatadiki, har bir tasnifga mutanosib ravishda majburiy nazorat talab qilinadi. Bu, dizaynga ko‘ra, ma’lumot almashishga to‘sqinlik qiladi va nazorat qilishda moslashuvchanlik talab qilinmaydi. Shuning uchun bo‘limlarga CTIni GSC bilan muntazam ravishda belgilamaslik tavsiya etiladi va buning o‘rniga, agar operatsion cheklovlar bilan majburiy bo‘lmasa, TLP dan foydalanish tavsiya etiladi. Qonuniy faoliyatni blokirovka qilishning oldini olish uchun ushbu infratuzilma uchun maxsus oq ro‘yxat qoidasi mavjud bo‘lishi kerak.

2.2-§. Katalog yondashuv.

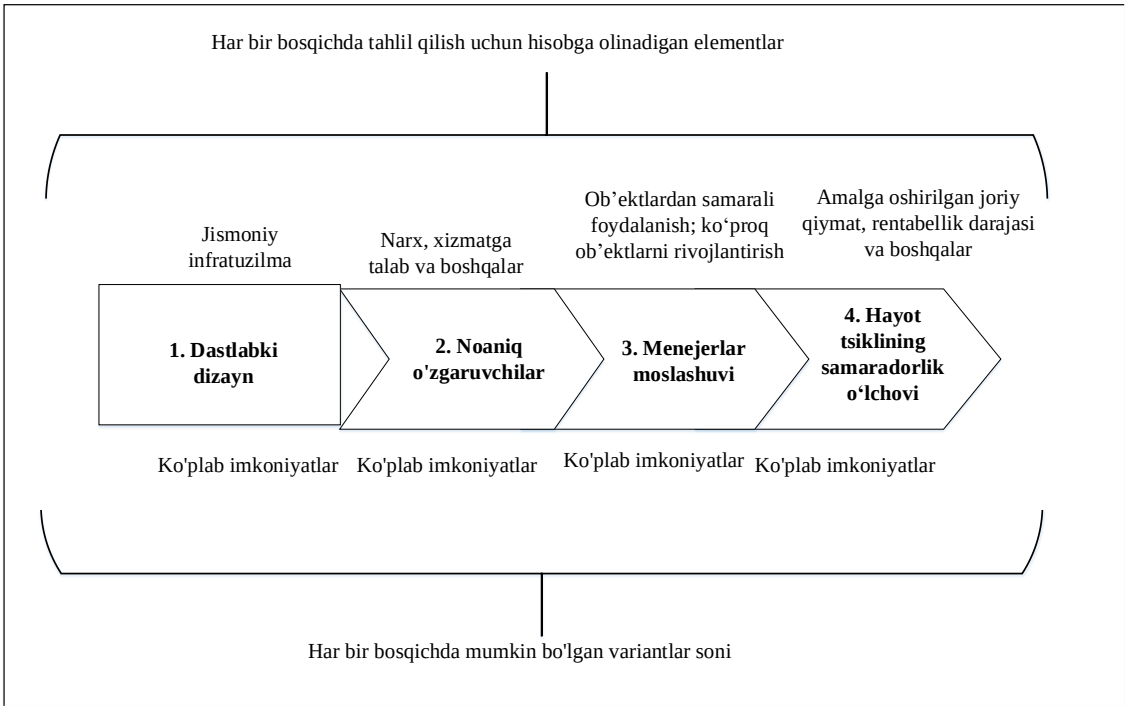
Muhandislik tizimlari yuqori darajadagi texnik murakkablik, ijtimoiy murakkablik va jamiyatdagi muhim funktsiyalarni bajarishga qaratilgan murakkab jarayonlar bilan tavsiflanadi. Ular uzoq umr ko‘rishlarini hisobga olsak, ular strategik, taktik va operatsion darajalarda juda ko‘p noaniqlikka duch kelishadi. Infratuzilma tizimlari - bu har qanday zamonaviy shaharda muhim rol o‘ynaydigan, favqulodda xizmatlarni (masalan, tez tibbiy yordam stantsiyalari, kasalxonalar), energiya ishlab chiqarish va tarqatish (masalan, elektr stantsiyalari va milliy tarmoq), telekommunikatsiya (masalan, uyali telefon tarmog‘i) ni qo‘llab-quvvatlovchi muhandislik tizimlarining alohida sinfidir. Transport (masalan, aeroportlar, yo‘llar, ko‘priklar, avtomobil yo‘llari) va uy-joy faoliyati (masalan, ko‘chmas mulk loyihalari).

Infratuzilma tizimlari ushbu uslubiy qo‘llanmaning diqqat markazida bo‘ladi. Muhandislik tizimlari uchun dizayn qarorlarini qabul qilishning dastlabki bosqichi juda qiyin vazifadir. 2.3-rasmda standart loyihalash va baholash jarayonining turli bosqichlari ko‘rsatilgan. Bular odatda tizimni ishlab chiqish bosqichida, tizim muhandisligida batafsilroq loyihalash bosqichidan oldin sodir bo‘lgan kontseptual dizayn va arxitektura tadbirlari hisoblanadi.

U dastlabki dizayndan boshlanadi, so‘ngra hayot aylanish jarayoniga ta’sir qiluvchi asosiy noaniqlik omillarini tan oladi, menejerlar o‘zgaruvchan sharoitlarga moslashish uchun vaqt o‘tishi bilan tizimni

moslashtirishini tan oladi va iqtisodiy baholash uchun turli ko‘rsatkichlarga tayanadi (masalan, sof joriy qiymat yoki NPV) va/yoki iqtisodiy bo‘lmagan ko‘rsatkichlar (masalan, favqulodda xizmatlar uchun javob vaqti). Bunday jarayon 1-bosqichda bir nechta mumkin bo‘lgan dizayn variantlarini hisobga olgan holda asosiy infratuzilma loyihalarini (masalan, zavodlar, tarmoqlar va boshqalar) modellashtirish va optimallashtirishni va 2-bosqichda uzoq muddatli ufqlarda noaniqlik stsenariylarini (masalan, bozor talabi, narx, qoidalar) hisobga olishni o‘z ichiga oladi. 3-bosqichda e’tirof etilganidek, ko‘plab arxitektura va ish rejimlari bo‘lishi mumkin (masalan, zavodlar soni va hajmi, yo‘l tarmog‘idagi transport vositalarining marshruti va boshqalar).

4-bosqichda ko‘rsatilgan daromad darajasi (IRR), NPV, investitsiyalar rentabelligi (ROI) va boshqalar).



2.3-rasm. Konseptual dizayn faoliyatining bir qismi sifatida muhandislik tizimlarini loyihalash uchun to'liq analitik muammosi

Tizimlarni loyihalash va tahlil qilishda odatiy yondashuv to‘liq tahliliy muammoni soddalashtirish, uni yanada qulayroq qilishdir.

Davriy ma’lumotlarning ko‘plab stsenariylarini ko‘rib chiqish o‘rniga, dizaynlar ko‘pincha asosiy noaniqlik drayverlarining eng katta prognozi uchun optimallashtiriladi. NPV kabi diskontlangan pul oqimi (DCF) tahliliga asoslangan loyihani baholashning odatiy yondashuvlari menejerlarning tizim ish faoliyatini yaxshilash uchun vaqti-vaqti bilan reaksiyaga kirishishini yaxshi hisoblamaydi.

Bundan tashqari, dizayn qarorlari ko‘pincha IRR, ROI yoki NPV

kabi bir baholash ko‘rsatkichiga asoslanadi. Bunday amaliyotlar eng maqbul dizayn tanloviga olib kelishi yoki hayot aylanishining yaxshi ishlashini ta’minlaydigan potentsial yechimlarni butunlay chetga surib qo‘yishi mumkin. So‘nggi yigirma yil ichida muhandislik tizimlarini loyihalashda noaniqlik va moslashuvchanlikni yanada aniqroq ko‘rib chiqish orqali standart dizayn va loyihalarni baholash amaliyotini takomillashtirish bo‘yicha katta sa’y-harakatlar amalga oshirildi. Moslashuvchanlik tizimni o‘zgaruvchan muhit, bozorlar, qoidalar va texnologiyalarga faol ravishda o‘zgartirish va moslashish imkonini beradi.

U mumkin bo‘lgan natijalar taqsimotiga ta’sir ko‘rsatish, salbiy sharoitlardan ta’sirni kamaytiradigan dizaynlarni tanlash (masalan, sug‘urta sotib olish) va tizimga qulay imkoniyatlardan foydalanishga imkon berish (ya’ni, aktsiyaga qo‘ng‘iroq optsionini sotib olish) orqali kutilgan hayot aylanishi samaradorligini yaxshilaydi.

Moslashuvchan tizimlarni loyihalash kontseptsiyasi quyidagilardan iborat:

a) noaniqlikni boshqarish strategiyasi (masalan, tizimdan doimiy yoki vaqtinchalik voz kechish, quvvatni kengaytirish, qo‘shimchalikni yaxshilash uchun dizayn konfiguratsiyasini o‘zgartirish va h.k.), tizimni haqiqiy “yoqish” variantiga o‘xshash;
b) tizimdagi haqiqiy variantga o‘xshash dizayn va boshqaruvni faollashtiruvchi vosita. Bir nechta tadqiqotlar an’anaviy ROA baholashga muvofiq standart dizayn va baholash amaliyoti natijalariga nisbatan 10-30% gacha yaxshilanishlarni ko‘rsatdi.

Muhandislik tizimlarining dizaynini noaniqlik va moslashuvchanlikni aniq hisobga olgan holda kengaytirilgan tahlil qilish imkonini beradigan, hayot aylanishining samaradorligini oshiradigan va standart dizayn va baholash yondashuvlari bilan taqqoslaganda analitik tarzda kuzatilishi mumkin bo‘lgan qanday tuzilgan jarayonni ishlab chiqish mumkin?” Ikkinchi darajali savol: “Taklif etilayotgan mexanizm misol muhandislik tizimini tahlil qilishda qo‘llanilganda hayot tsiklining samaradorligini oshirish nima va u boshqa raqobatdosh usullar bilan qanday taqqoslanadi?”

Taklif etilayotgan yechim *dizayn katalogi* kontseptsiyasiga tayanadi.

Katalog moslashuvchan dizayn arxitekturasini va dizaynerlar kutmoqchi bo‘lgan noaniqlik namunalariga mos keladigan boshqaruv javoblarini birlashtirgan *operatsion rejalar* to‘plamidan iborat.

Bu yerda taklif qilingan ushbu dizayn katalogi ma’lum bir noaniqlik

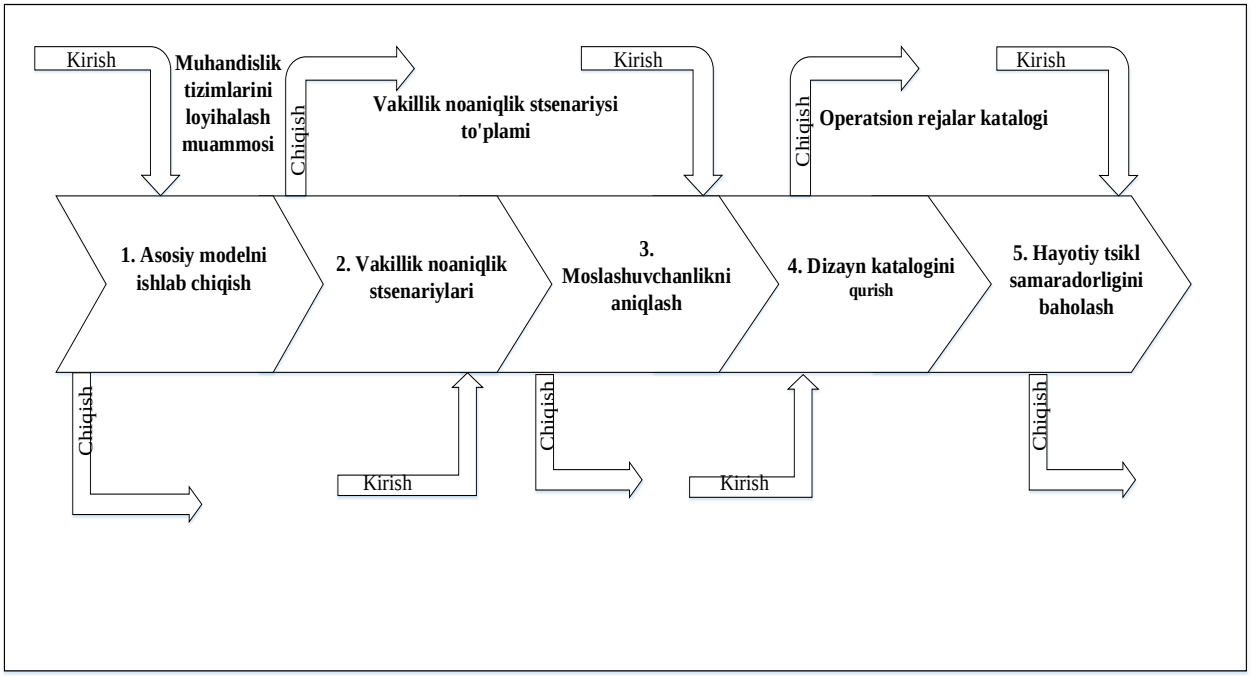
stsenariylarini birgalikda oqilona hal qiladigan operatsion rejalar yoki modellar to‘plamini tanlash orqali ishlab chiqilgan. Bu eng mos rejalar bo‘yicha tahlilni tezlashtiradi, tahlilchilarga ko‘proq dizayn muqobillarini ko‘rib chiqishga imkon beradi va stokastik dasturlash yoki simulyatsiyaga asoslangan optimallashtirishga asoslangan ilg‘or usullarga tayanmasdan, yaxshilangan umr ko‘rish ko‘rsatkichlari bilan yaxshiroq dizayn yechimlarini topishga imkon beradi. Taklif etilayotgan yechim odatda loyihalash va baholashda qilingan eng oddiy taxminlar to‘plami va 2.3-rasmda tasvirlangan to‘liq tahliliy muammo o‘rtasidagi o‘rta joyni taklif qiladi. U tizim dizaynerlariga ma’lum bo‘lgan va ehtimollik (masalan, bozor talabi) bilan tavsiflanishi mumkin bo‘lgan noaniqlik manbalariga qaratilgan.

U analitik tarzda boshqarish mumkin bo‘lgan darajada kichik, ammo yaxshi ma’lumotga ega bo‘lgan dizayn qarorlarini qabul qilish uchun yetarlicha keng bo‘lgan bir qator mumkin bo‘lgan stsenariylarga tayanadi. Maqsad, ilg‘or tahlil bilan bog‘liq bo‘lgan hisoblash qo‘shimcha xarajatlarini cheklash bilan birga, moslashuvchanlikni aniq hisobga olgan holda, tahlilchilarga hayot aylanish jarayonini tez yaxshilashga amaliy yondashuvni taqdim etishdir.

Katalogni loyihalash jarayoni. 2.4-rasmda taklif etilayotgan katalogga asoslangan jarayon umumlashtiriladi, u 2.3-rasmda tasvirlangan jarayonga asoslanadigan va kengaytiruvchi besh bosqichdan iborat:

1) hayot aylanishi samaradorligini o‘lchash tizimining asosiy modelini ishlab chiqish;
2) hayot aylanish jarayoniga eng ko‘p ta’sir qiluvchi noaniqlik stsenariylarini toping,
3) dizayn va boshqaruvda moslashuvchanlikning potentsial manbalarini aniqlash va yaratish;
4) har bir stsenariy uchun eng mos moslashuvchan operatsion rejani toping va dizayn katalogini tuzing;
5) hayot aylanish jarayonini baholash va noaniqlik sharoitida asosiy dizayn bilan solishtirish.

Quyidagi tavsifda sanoat va akademik doiralarda qo‘llaniladigan mashhur texnikalar taklif etiladi. Biroq, bu tanlov oxir -oqibat jarayonni amalga oshiruvchi tashkilotga bog‘liq.



2.4-rasm. Muhandislik tizimlarini loyihalash uchun dizayn katalogi yondashuvi

1-qadamning maqsadi turli stsenariylar ostida tizimning hayot aylanishi samaradorligini o‘lchash uchun asosiy modelni ishlab chiqishdir. Ushbu qadam muhandislik tizimlarini loyihalash muammosiga kirish sifatida qabul qilinadi va hayot aylanish jarayoniga ta’sir qilishi mumkin bo‘lgan aniqlangan noaniqlik drayverlari bilan bir qatorda ishlash modelini chiqaradi. Sanoatda DCF tahlili odatda kutilayotgan iqtisodiy samaradorlikni baholash uchun ishlatiladi, lekin agentga asoslangan modellashtirish, navbat, kompyuter yordamida dizayn, diskret hodisalar simulyatsiyasi va boshqalar kabi boshqa modellash usullaridan foydalanish mumkin.

2-bosqichning maqsadi hayot aylanish jarayoniga ta’sir qiluvchi noaniqlik drayverlari doirasini qamrab oluvchi vakillik stsenariylari to‘plamini topishdir.

Ushbu bosqichga kirish ishlash modelining bir qismi sifatida modellashtirilgan asosiy noaniqlik drayverlari bo‘lib, chiqish 3-bosqichda moslashuvchan tizimlar dizayni kontseptsiyasini yaratishni rag‘batlantirish uchun ishlatiladigan bunday stsenariylarning vakillik to‘plamidan iborat. Bunday vakillik to‘plamini topish sanoatda Shell stsenariysini rejalashtirish, ehtimollikni aniqlash yoki dizayn tashkilotidagi dizayn mutaxassislari va/yoki mijoz bilan munozaralar asosida vaziyatga asoslangan fikrlash kabi mashhur usullar yordamida amalga oshirilishi mumkin. Bu yerda stsenariyni rejalashtirishga

asoslangan tizimli jarayon taklif etiladi - tavsiya etilgan ma’lumotlar uchun Ilovaga qarang. Dastlab Shellda ishlab chiqilgan va ishlatilgan, bu o‘zgartirilgan jarayonni o‘z ichiga oladi.

a) muammo doirasini aniqlash;
b) asosiy manfaatdor tomonlarni aniqlash;
c) asosiy tendentsiyalarni aniqlash;
d) asosiy noaniqliklarni aniqlash;
e) dastlabki stsenariy mavzularini qurish,
f) miqdoriy modellarni ishlab chiqish va
h) qaror qabul qilish yo‘lida rivojlanish.

Eng yaxshi amaliyotni ifodalovchi maxsus usul mavjud bo‘lmasa-da, haqiqiy variantlarni tahlil qilish, taklif qilish, aqliy hujum va / yoki dizayn tuzilmalari matritsasi (DSM) ga asoslangan bir nechta texnikalar taklif qilingan va adabiyotda uchuvchisiz flot kabi murakkab tizimlarni o‘z ichiga olgan dastur sohalarida baholangan. aeromobillar, ko‘chmas mulkni rivojlantirish loyihalari va chiqindilardan energiyaga infratuzilma tizimlarida batafsil muhokama qilinadi, bu tizim va analitik kontekstga qarab tanlash uchun tegishli protseduralar bo‘yicha ko‘rsatmalar berishga yordam beradi.

4-bosqichning maqsadi dizayn katalogini yaratishdir. Kirish egiluvchan tizimlar loyihalash konsepsiyasilari qiziqish uyg‘otadi va kengaytirilgan samaradorlik modelidir, chiqish esa operatsion rejalar katalogidir. Noaniqlik yuzaga kelganda, menejerlarning operatsion rejani o‘zgartirish qobiliyatini modellashtirish uchun har bir vakillik stsenariysi uchun afzal moslashuvchan operatsion reja topiladi. Har bir reja, shuningdek, ma’lum bir stsenariyda foydalaniladigan mumkin bo‘lgan moslashuvchanlik strategiyasini modellashtiradi.

Shunday qilib, taklif qilingan doirada moslashuvchanlik ikki darajada qo‘llaniladi:

— operatsion rejalar o‘rtasida o‘zgarish qobiliyati;
— ma’lum bir operatsion reja doirasida moslashish qobiliyati.

Ushbu qadam kontseptual jihatdan stoxastik dasturlarni hal qilishda tez-tez bajariladigan diskretizatsiya bosqichiga o‘xshaydi. Katalogni yaratish uchun 4-bosqichda bir nechta mexanizmlardan foydalanish mumkin.

Turli xil algoritmlardan foydalanishning oqibatlari yechim sifatiga ta’sir qilishi mumkin va/yoki Shell-da qo‘llaniladigan ushbu o‘zgartirilgan jarayon quyidagilarni o‘z ichiga oladi.

a) muammo doirasini aniqlash;

b) asosiy manfaatdor tomonlarni aniqlash;
c) asosiy tendentsiyalarni aniqlash;
d) asosiy noaniqliklarni aniqlash;
e) dastlabki stsenariy mavzularini qurish,
f) miqdoriy modellarni ishlab chiqish va
h) qaror qabul qilish yo‘lida rivojlanish.

Variantlarning tabiatini va mumkin bo‘lgan natijalar spektrini qo‘lga kiritish uchun yetarlicha stsenariylar tanlanishi kerak. Simulyatsiyaga asoslangan va stokastik dasturlash texnikasi bilan bog‘liq bo‘lgan hisoblash yukini oldini olish uchun juda ko‘p stsenariylarni tanlamaslik kerak. Ushbu bosqich kontseptual ravishda stokastik dasturlashda qo‘llaniladigan namunaviy o‘rtacha yaqinlashish texnikasidan olingan. U optimallashtirish uchun ko‘rib chiqiladigan stsenariylar sonini va shuning uchun hisoblash yukini kamaytirishga qaratilgan.

Katalogni yaratish uchun 4-bosqichda bir nechta mexanizmlardan foydalanish mumkin. Algoritmni tanlash loyihalash masalasining tabiatiga bog‘liq (masalan, diskret va uzluksiz o‘zgaruvchilar, chiziqli va chiziqli bo‘lmagan maqsad funktsiyasi, deterministik va stokastik).

Turli xil algoritmlarni qo‘llash oqibatlari yechim sifatiga va/yoki zarur bo‘lgan 10 ta hisoblash darajasiga ta’sir qilishi mumkin. Murojaat qilingan matnlar vaqt, muammo turi va tahlilchi uchun mavjud resurslarga qarab foydalanish uchun eng yaxshi algoritm bo‘yicha ko‘rsatmalar beradi.

5-bosqichning maqsadi - katalog yordamida olingan natijalarni 1-bosqichda asosiy model uchun olingan natijalar bilan solishtirish, agar mavjud bo‘lsa, standart dizayn va baholash bilan taqqoslaganda, dizayn katalogi tomonidan olib kelingan yaxshilanishni o‘lchash. Ushbu qadam dizayn katalogiga kirish sifatida qabul qilinadi va tizim muhandisligi jarayonini batafsil tahlil qilish bosqichida hisobga olinadigan qiymatni oshiruvchi moslashuvchan dizaynlar va kataloglarning afzal qilingan to‘plamini chiqaradi. Bu keng doiradagi noaniqlik stsenariylarini simulyatsiya qilish, har bir stsenariyga bitta operatsion rejani belgilash va har bir reja/stsenariy bo‘yicha tizim ish faoliyatini o‘lchash orqali amalga oshiriladi. Ushbu bosqich stokastik dasturlashda o‘tkaziladigan namunadan tashqari sinovga o‘xshaydi, agar namunalar 2-bosqichda vakillik stsenariylarini yaratish uchun ishlatiladigan bir xil jarayon yoki modeldan yaratilgan bo‘lsa.

Katalogdan va moslashuvchan operatsion rejalardan foydalanishda

moslashuvchanlik qiymatini aniqlash uchun katalogli va katalogsiz tahlil o‘tkazilishi mumkin. Moslashuvchanlik taklif etilayotgan dizaynga qanday ta’sir qilishini aniqlash uchun natijalar taqsimotini solishtirish mumkin. Ko‘p mezonli baholash turli xil baholash ko‘rsatkichlari (masalan, o‘rtacha samaradorlik, 5 yoki 95 foiz va boshqalar) yordamida qaror qabul qilishda turli xil xavf profillarini hisobga olgan holda dizayn variantlarini yoki kataloglarini solishtirishga yordam beradi.

Ushbu haqiqiy infratuzilmani rivojlantirish loyihasi potentsial yangi mijozlar va savdo markaziga tashrif buyuruvchilarning to‘xtash joylariga bo‘lgan ehtiyojini qondirish uchun boshlangan. Potentsial mijozlar/tashrifchilar sonining o‘sishi noma’lum bo‘lganligi sababli, tizim dizaynerlari va arxitektorlari qo‘shimcha qavatlar va sig‘imlarni joylashtirish uchun tizimga moslashuvchanlikni o‘rnatdilar va shu bilan savdo markaziga dastlab rejalashtirilganidan ko‘proq mijozlar tashrif buyurgan taqdirda ko‘proq mashinalar joylarini taqdim etdilar. Ular moslashuvchan dizayn eng yaxshi yoki stokastik jihatdan optimal - belgilangan quvvat bilan ishlab chiqilgan tizimdan farqli o‘laroq, noaniq talab o‘sishi sharoitida qo‘shimcha iqtisodiy qiymat yaratishi mumkinligini ko‘rsatdi.

2.3-§. Kiberxavfsizlik siyosati katalogi

Kiberboshqaruv muammolari. Internet ilg'or tadqiqot loyihalari agentligi tarmog'i (ARPANET) sifatida boshlandi, bu yadroviy hujumdan omon qolish uchun mo'ljallangan AQSh harbiylari tomonidan moliyalashtiriladigan tarmoq edi. U tezda armiyadagi kompyuter fanlari tadqiqotchilari, uning pudratchilari va akademik hamkorlari o'rtasida ma'lumot almashish vositasiga aylandi. Aloqa protokoli g'oyasiga ega bo'lganlar uni Internet muhandislik bo'yicha ishchi guruhi (IETF) tomonidan boshqariladigan rasmiy jarayon deb qabul qilindi. Ular sharhlar uchun so'rovlar Nazarot savollari sifatida nashr etildi, bu boshqalarga yangi protokollarni tezda o'rganish, shuningdek ularni kengaytirish imkonini berdi.

Internet infratuzilmasi va funktsiyalarining katta qismi markazlashtirilmagan bo'lsada (Internetning dizayn maqsadi), ammo ma'lum markazlashtirilgan rejalashtirish va muvofiqlashtirish funktsiyalari talab qilinadi. Eng ko'zga ko'ringanlari domenlar (ya'ni, http://www.whitehouse.gov) va raqamlar (ya'ni, Internet Protocol yoki IP manzillar) taqsimotidir. Ushbu muvofiqlashtirish funktsiyalari dastlab AQSh Mudofaa vazirligi pudratchisi bo'lgan Stenford tadqiqot institutida

(SRI) amalga oshirildi. 1972-yilda bu funksiyalar Janubiy Kaliforniya universiteti qoshidagi Axborot fanlari institutida (ISI) Jon Postel nazorati ostida Internet Assigned Numbers Authority (IANA) ga o‘tkazildi. Bu ARPANET asta-sekin tarqatib yuborilishiga sabab bo’ldi. 1995 yilda Internet-trafigiga nisbatan oxirgi cheklovlar olib tashlandi.

1998 yilda AQSh Savdo Departamentining agentligi bo'lgan Milliy Telekommunikatsiya va Axborot Boshqarmasi (NTIA) IANA funktsiyalari uchun barqaror boshqaruv modelini yaratish jarayonini boshladi, bu jarayon 2000 yilda Tayinlangan nomlar va raqamlar uchun Internet korporatsiyasining (ICANN) yaratilishi bilan yakunlandi. 1998 yil 30 yanvarda ICANN sharh uchun “Yashil qog'oz” siyosatini chiqarildi: “Internet nomlarini texnik boshqarishni takomillashtirish bo'yicha taklif”. Natijada paydo bo'lgan ICANN modeli, Internetning markazlashtirilgan tarkibiy qismlari uchun noyob “ko'p manfaatdor” boshqaruv modeli bo'lib, unda hukumatlar,korporatsiyalar va individual Internet foydalanuvchilari bilan birgalikda Internetni pastdan yuqoriga qarab boshqaradigan siyosatlarni yaratishda ishtirok etadi. 2009 yilda ICANNni USG pudratchisidan USG va ICANN o'rtasidagi o'zaro anglashuv memorandumiga o'tgan 2009 yilda imzolangan Majburiyatlarni tasdiqlash to'g'risidagi shartnoma imzolanmaguncha ICANN texnik jihatdan AQSh hukumatini ko'p tomonli Internet boshqaruvi (USG) pudratchisi bo'lib qoldi.

Internet boshqaruvi va global telefon tizimi o'rtasidagi o'xshashlikni ko'rish oson. Sababi Xalqaro miqyosda to'g'ridan-to'g'ri qo'ng'iroq qilishingiz mumkin, va har bir mamlakatda o'z fuqarolarini dunyo bilan bog'lash bo'yicha o'zlarining shaxsiy missiyalarini bajarish uchun har joyda telefon aloqasi bo'yicha umumiy global maqsadi bo'lgan hamkorlik qiluvchi telekommunikatsiya kompaniyalari qo'mitasi mavjud. Bu kompaniyalar 1865 yilda Xalqaro elektraloqa ittifoqini tuzdi. 1947 yilda ITU o'sha paytdagi yangi Birlashgan Millatlar Tashkiloti (BMT) tarkibiga kirdi. Birlashgan Millatlar Tashkiloti/ITU yuqoridan pastga, hukumat tomonidan boshqariladigan boshqaruv modelidir. Bundan farqli o'laroq, ICANN/AoC modeli pastdan yuqoriga siyosat ishlab chiqishni qo'llab-quvvatlaydigan “xalqaro ko'p manfaatli boshqaruv modeli” dir. Jahon hukumatlari ICANN modelida Hukumat Maslahat Qo'mitasi (GAC) orqali ishtirok etadi, bu ICANN doirasida Internet siyosatini belgilovchi bir nechta maslahat qo'mitalaridan biri hisoblanadi. Ba'zilar ITU/UN modeli Internet boshqaruvi uchun to'g'ri model, deb da'vo qilsalar, boshqalari ICANN/AoC modeli optimal deb ta'kidlaydilar.

Kiberxavfsizlik siyosatining asosiy muammosi Internetni boshqarish modeli va xususan, jahon hukumatlarining ishtirok etish uslubidir. Internetning eng o'ziga xos xususiyatlaridan biri shundaki, u butun dunyo bo'ylab taqsimlanadi; har qanday Internet-mashina boshqa internetga ulangan mashina bilan gaplasha oladi va Kanzas, Singapur, Berlin va Moskvada http://www.cnn.com ni yozish sizni bir joyga olib boradi. Ushbu global hamkorlikning texnik sababi markaziy muvofiqlashtirish funktsiyalarining mavjudligidir. Agar hukumatlar markaziy muvofiqlashtirish funktsiyalari bo'yicha kelishmasa va turli standartlar/protseduralardan foydalanishni boshlasa, Internet bir nechta yoki qisman bog'langan qismlarga bo'linishi mumkin. Ba'zi hukumatlar senzura, milliy suverenitet va AQSh hukmronligiga qarshi turish bilan bog'liq sabablarga ko'ra bu yondashuvni afzal ko'radi.

Kiberfoydalanuvchi muammolari. Tarmoqqa ulanish - bu kibermakon foydalanuvchisi bo'lish. Dunyo aholisining taxminan 30% Internetga ulangan. Onlayn rejimga o'tgan an'anaviy biznes munosabatlariga qo'shimcha ravishda, so'nggi yigirma yil ichida Internet yangi elektron tijorat biznes modellarini yaratdi. Bularga an'anaviy biznes joylashuvi ya’ni internet do'konlaridan foydalanish kiradi. Elektron tijorat reklamasi dastlab Internetdan oldingi jamoatchilik bilan aloqalar va marketing faoliyatini aks ettirgan bo'lsada, Internet hamma joyda mavjud bo'lmagan bir qancha yangi marketing modellari ham paydo bo'ldi. Bular kibermakonning bir burchagidan ma'lumotlarni yig'ib, boshqasiga sotuvchi axborot xizmatlaridir. Ushbu ma'lumotlarning asosiy mijozi reklama sanoatidir.

Kiber foydalanuvchilar uchun xavfsizlik muammolari, asosan, elektron tijoratiga kutilmagan ulanishidan kelib chiqadi. Ushbu ulanishlarning barchasi dasturiy ta'minot yordamida yaratiladi va bu dasturiy ta'minot har qanday tajovuzkorga foydalanuvchining ma'lumotlari oqimini kuzatish yoki elektron tijorat tranzaksiyasini buzish imkonini beruvchi xato yoki zaiflikni aniqlab beradi. Ushbu ulanish nuqtalarining ko'pchiligida ma'lumotlar oqimini kuzatish keyingi hujumlar uchun ishlatilishi mumkin bo'lgan ma'lumotlarni taqdim etadi, masalan, shaxsni o'zgartirish va shaxsni o'g'irlash uchun foydalaniladigan foydalanuvchi nomlari va parollarini kuzatish.

2.4-jadval

Elektron pochta va xabar almashishga oid kiberxavfsizlik siyosati masalalari

Siyosat	Bayonoti	Qarama-qarshilik sabablari
Elektron tijoratda ishtirok etuvchi barcha sub'ektlar mijozlariga standart protokollar orqali elektron pochta serverlarini tekshirish imkoniyatini taklif qilishlari kerak.	Ushbu siyosat e-tijorat kompaniyalaridan o'zlarining elektron pochta serverlari uchun kalitlarni DNS-da nashr etishlarini talab qiladi.	Iste'molchilar xizmat ko'rsatuvchi provayderlar va boshqa sotuvchilardan kelgan xabarlar soxtalash tirilmaganligini tekshirish huquqiga ega. Iste'molchilar odatda elektron pochta serverini tekshirish dasturiga ega emaslar va shuning uchun tekshirish uchun ISP yoki hosting xizmati provayderlariga tayanishi kerak. Shunday qilib, bu talab elektron tijorat kuchlariga qoldirilishi yaxshiroqdir.
Tashkilot nomidan yoki unga tegishli barcha elektron pochta xabarlari, tashkilot tomonidan qo'llab-quvvatlanadigan elektron pochtasidan jo‘natilgan bo‘lishi kerak.	Bu tashkilot hodimlari tashkilotning biznesini yuritishda o'z tashkilotining elektron pochta tizimlaridan foydalanishi shart va ijtimoiy tarmoq saytlari, shaxsiy mobil telefonlar va boshqa davlat yoki xususiy tarmoqlar orqali tashkilot nomidan foydalanishni sheklash talabidir.	Ushbu siyosat barcha aloqalarni boshqaruv monitoringi doirasida saqlaydi. Bu ma'muriy javobgarlikka tortilish mumkin bo’lgan xodimlar sonini kamaytiradi. Ushbu siyosat sayohat yoki uzilishlar tufayli korporativ xizmatlarga erisha olmaydigan shaxslarning muloqot qilish qobiliyatini cheklaydi.
Elektron pochta orqali	Har xil shartnoma va	Yetkazib berishning

jo'natilganlik va o'qilganligi to'g'risidagi kvitansiya elektron ma'lumotlarning yetkazilganligini tasdiqlovchi hujjatni taqdim etishi kerak.	me'yoriy hujjatlar bildirishnomalarni taqdim etuvchi tashkilotlardan xabarnoma yuborilgan shaxs uni haqiqatda olganligini isbotlashni talab qiladi.	isboti sifatida elektron yetkazib berish va o‘qish kvitansiyasidan foydalanish imkoniyati turli sohalarda jismoniy shaxslarni xabardor qilish uchun qonuniy javobgar bo‘lgan tashkilotlar uchun xarajatlarni kamaytiradi, bank va Raqamli yozuvlarni autentifikatsiya qilishning joriy standartlari kalitlarni boshqarish, kriptografik algoritmlar va tashkiliy nazorat tartib-qoidalarini isbotlashning kombinatsiyasini talab qiladi. Bunga imkon beradigan infratuzilma yo'q
Jismoniy shaxslar o'zlarining elektron pochta manzillarini ro'yxatda joylashtirish imkoniyatiga ega bo'lishi kerak, bu esa sotuvchilarning ularga keraksiz elektron pochta xabarlarini yuborishini noqonuniy qiladi.	Bu elektron pochta so'rovi uchun milliy “qo'ng'iroq qilmang” reestrining ekvivalentidir. Ushbu turdagi ro'yxat hozirda telefon raqamlari uchun ishlatiladi. Marketing kompaniyalari qo'ng'iroq qilmaslik ro'yxatidagi telefon raqamlarini telefon marketing kampaniyalaridan olib tashlashlari kerak.	Elektron pochta manzillarini istalmagan so'rovlardan himoya qilish uchun “elektron pochta jo'natmang” siyosatini qo'llash mexanizmi hozirda elektron pochta orqali qabul qilinadigan kiruvchi reklamalar sonini sezilarli darajada kamaytiradi. Bu siyosat noqonuniy spamni aniqlashni osonlashtirishi kerak. Siyosatning bajarilishi o'tkazish qobiliyatini va

		saqlash resurslarini tejash imkonini beradi. Elektron pochta iste'molchilar bilan bog'lanishning samarali usuli bo'lib, turli xil onlayn tadbirlar orqali mahsulot va xizmatlarga bo'lgan afzalliklarini bildirgan iste'molchilar ushbu siyosat bo'yicha so'rashda davom etadilar. Qiziqish nimadan iborat bo'lganligi haqida chiziq chizish qiyin bo'lishi mumkin va shuning uchun siyosatni amalga oshirish qiyin bo'ladi. Ba'zi elektron tijorat korxonalari uchun asosiy daromad manbai Internet-trafikni kuzatishlari asosida yaratishi mumkin bo'lgan elektron pochta manzillari ro'yxatidir. Ushbu aktivlarning qiymati sezilarli darajada bo'ladi
Internet xabar almashish xizmatlari foydalanuvchilarga xabar almashish uchun hamjamiyatni tanlash va hamjamiyatdan tashqaridagi barcha aloqalarni istisno qilish imkonini berishi kerak.	Bu har bir potentsial elektron pochta qabul qiluvchisi uchun individual “oq ro'yxat” ning ekvivalenti. Faqat ro'yxatdagilar qabul qiluvchiga elektron pochta yoki xabar yuborishlari mumkin.	Ushbu siyosat Internet foydalanuvchilariga o'z resurslarini boshqarish va keraksiz xabarlar sonini kamaytirish imkonini beradi. Bu ham tarmoqli kengligi, ham saqlash resurslarini tejaydi.

		Elektron pochta yoki xabar almashish uchun umumiy qabul qilingan autentifikatsiya usuli mavjud emasligi sababli, har kim oq ro‘yxatdagi istalgan foydalanuvchi nomini o‘xshatib, bu siyosatni chetlab o‘tishi mumkin. Shuning uchun uni amalga oshirish mumkin emas.
Xabar almashish xizmatlaridan foydalanuvchi shaxslar faqat o'zlari ro'yxatdan o'tgan Internet domen nomlaridan foydalanishlari shart.	Bu elektron pochtadagi “Kimdan” manzillaridan foydalanishni jo'natuvchi ICANNda ro'yxatdan o'tgan manzillar bilan cheklaydi.	Manzillarni cheklash elektron tijorat marketingidagi innovatsiyalarni qo'shimcha xavfsizlikni ta'minlamasdan cheklaydi, chunki Imtiyozli davrni qo'shish (AGP) bu talabni vaqtincha qondirish uchun osongina ishlatilishi mumkin edi.
Fishing elektron pochta xabarlarini ma'lum jo'natuvchilar jinoiy zararlikka tortiladi va jazolar fishing oluvchilardan potentsial ma'lumot o'g'irlanishi natijasida hosil bo'lgan jinoyatlarga mutanosib bo'lishi kerak.	Ushbu siyosat fishing elektron pochta xabarlarini yuborganlarga shaxsni o'g'irlash jazosini qo'yadi.	Phish elektron pochta jo'natuvchilari uyushgan jinoyatchilikning katta jamoasining kichik bir qismidir. Garchi ularning jinoyati begunoh bo‘lib ko‘rinsa-da, bu shaxsga qasddan kattaroq hujum qilish uchun zaruriy shartdir va hujumning o'zi kabi jiddiy qabul qilinishi kerak.

		Fishing elektron pochta jo'natuvchisi, ehtimol, ommaviy elektron pochta xabarlarini yuboradigan biznesdir turli mijozlar uchun va qonuniy va noqonuniy mijozlarni ajrata olmaydi va Internet jinoyatchilarini aniqlash yukini ko'tarmasligi kerak. Bundan tashqari, oddiygina elektron pochta xabarini yuborish foydalanuvchining o'ziga jalb qilinishiga kafolat bermaydi.

Xavfsizlik nuqtai nazaridan e-tijorat muhitida foydalanuvchilarning to'rtta asosiy turi mavjud: mijoz, sotuvchi, ishlab chiqaruvchisi va buzg’unchi. Buzg’unchining maqsadi boshqa uchta turdagi foydalanuvchining bir yoki bir nechtasini noqonuniy usulda daromadini olish. Buzg’unchi dasturiy ta'minot, dastur konfiguratsiyasi, apparat va inson omili zaifliklardan foydalanishga intiladi. Elektron tijorat hujumlari doimiy ravishda sodir bo'ladi. Birinchi sahifaga faqat qurbonlar uchun eng og'ir oqibatlarga olib keladigan eng qiziqarli firibgarlik holatlari chiqadi. Shunga qaramay, axborot xavfsizligi bo'yicha kiberjinoyatlar tarmog'ida giyohvand moddalar aylanishida bo'lgani kabi kundalik faoliyat mavjud. “Zero Day Threat” kitobida USA Today’ning ikkita muxbiri bu hodisani uchta arxetekturaning mahsuli sifatida tasvirlaydi: ekspluatatorlar, faollashtiruvchilar va ekspeditorlar. Ekspluatatorlar ma'lumotlarni o'g'irlash va firibgarlikni amalga oshiradilar.

Ekspeditorlar - bu asosiy sababni texnik nuqtai nazardan aniqlaydigan texnologlar ammo ular buzg‘inchilar yoki himoyachilar bo'lishi ham mumkin. beixtiyor iste'molchilarning ma'lumotlarini muntazam ravishda o'g'irlashi mumkin. Ekspluatatorlar nafaqat shaxsiy ma'lumotlarni o'g'irlash qurboni bo'lgan iste'molchini, balki past darajadagi ijtimoiy noqulayliklardan ham foydalanadilar. Ular o'z-o'zidan iste'molchilarning naqd pullarini bankomatlardan olib qo'yish yoki o'z-

o'zidan bilmasdan iste'molchilarning kredit kartalarida hashamatli narsalarga buyurtma berish uchun ijtimoiy nosozliklarni qo'llashadi.Har bir qayg'uli voqeaning axloqiy jihati shundaki, yordamchi o'z nazorati ostidagi ma'lumotlarni etarli darajada himoya qilmagan, shu bilan birga, uyushgan jinoiy tuzilmaning uch yoki undan ortiq qatlamini ijtimoiy nosozliklar ustidan nazorat qiluvchi yovuz daho hech qachon qo'lga olinmaydi. Iste'molchi zararlangan kredit, shuningdek, vaqt va pul yo'qotilishi bilan qoladi, aktivlashtiruvchi esa korxonani himoya qilish uchun xavf choralari mavjudligini da'vo qiladi.

Ushbu bo'lim kiberfoydalanuvchi xavfsizligi masalalarini oltita kichik bo'limga ajratadi: noto'g'ri reklama, o'zini taqlid qilish, tegishli foydalanish, kiberjinoyat, geografik joylashuv (“geografik joylashuv”) va maxfiylik.

Noto'g'ri reklama - bu “zararli” va “reklama” so'zlarining anagrammasi.

O‘zini taqlid qilish internetdagi turli xil firibgarliklar bilan shug‘ullanadi, anonim e’lonlardan tortib hisobni o‘g‘irlashgacha.Ba'zilar g'ayriijtimoiy deb hisoblaydigan Internetdagi odatiy xatti-harakatlarga qaratilgan va ular qonun chiqaruvchilar tomonidan hali rasman ko'rib chiqilmaganligi sababli jinoiy bo'lmasligi mumkin. Kiberjinoyat elektron tijoratda keng tarqalgan uyushgan jinoiy faoliyatga qaratilgan. Internet foydalanuvchilarining, ham iste'molchilar, ham jinoyatchilarning geolokatsiyasini aniqlash juda qiyin va o'ziga xos siyosat masalalarini taqdim etadi. Maxfiylik kiberxavfsizlikning geolokatsiya siyosati bo'yicha munozaralarni kuchaytiradigan tashvishlardan biridir, ammo maxfiylik muammolarning ancha kengroq to'plamidir va shuning uchun uning o'ziga xos bo'limi mavjud.

Kibermojarolar muammolari. Kibermojarolar - bu dasturiy ta'minot, kompyuterlar va tarmoqlar vosita yoki maqsad bo'lgan kibermakondagi nizolar va majburlash uchun umumiy belgidir. U kiber urushdan ko'ra kengroq qamrovni o'z ichiga oladi va dasturiy ta'minot, kompyuterlar va tarmoqlar ham vosita, ham maqsad bo'lgan kibermakonda strategik maqsadlar uchun davlatlar va guruhlar o'rtasidagi barcha nizolar va majburlashni o'z ichiga oladi. Kibermojaro milliy xavfsizlik maqsadlarida kibermakonda bir-biri bilan faol kurashayotgan milliy davlatlarni o'z ichiga oladi. Hamma kibermojarolar qurolli kuchlar darajasiga ko'tarilmaydi, masalan, keng ko'lamli kiberjosuslik. Kibermojaro davlatlar va korxonalar bilan chegaralanib qolmaydi, balki har qanday individual, erkin bog'langan ijtimoiy tarmoq guruhlari va har

qanday shakl va o'lchamdagi tashkilotlar o'rtasida bo'lishi mumkin. Odamlar siyosiy maqsadlarda yoki axloqiy e'tiqodlarni himoya qilish uchun kibermojaroga kirishsa, bu aktivlik deb ataladi. Kibermojaroning har qanday muhokamasida eslash kerak bo'lgan asosiy nuqta shundaki, u kompyuterlar haqida emas, balki odamlar haqida gap boradi.

Kibermojaro ko'pincha strategik maqsadlarda amalga oshiriladi, chunki milliy davlatlar texnik ustunlik uchun kurashish uchun kibermakonda faol missiyalarni amalga oshiradilar. Ushbu mojarolar qurolli kuchlar darajasiga ko'tarilishi yoki ko'tarilishi mumkin, masalan, keng ko'lamli kiber josuslik yoki kiber urush. Kibermojaroning ushbu atamasi milliy davlatlar va yirik kiberkosmik operatsiyalarga ega bo'lgan boshqa uyushgan guruhlar kibermakonda qanday kurashayotgani haqida kengroq muhokama qilish imkonini beradi va “urush” atamasini faqat milliy davlatlar o'rtasidagi eng muhim hujumlar uchun saqlab qoladi. Bu atama urush, josuslik va boshqa hujumlar tushunchalarini soddalashtirishga yordam beradi, chunki u koʻplab boshqa dushmanlikka asoslangan harakatlarni oʻz ichiga oladi, lekin baribir oʻsish va kibermakonda amalga oshirilgan yoki ular yordamida amalga oshirilgan zoʻravonlik mohiyatini muhokama qilish uchun oʻziga xos xususiyatga ega. Kibermojaro uchun eski atama bu elektron urush bo'lib, u ko'proq cheklovchi edi, chunki u odatda faqat kibermakon hujum vositasi va nishoni bo'lgan holatlarga nisbatan ishlatilgan.

Ushbu bo'lim kibermojaroning asosiy omillaridan biri - kibermakondagi intellektual mulkka da'volarni qamrab oladi. Intellektual mulk bilan bog'liq nizolar ochiq yoki yashirin bo'lishi mumkin, bu holda ular kiber josuslik sifatida tasniflanadi. Kibermojaroning eng ekstremal shakli kiber urushdir.

2.5-jadval

Maxfiylikka oid kiberxavfsizlik siyosati masalalari

Siyosat bayonoti	Izoh	Qarama-qarshilik sabablari
Milliy hukumatlar kompaniyalarning mijozlar ma'lumotlaridan tranzaktsiyalarni amalga oshirish yoki xizmatlar ko'rsatish uchun zarur bo'lgan usullardan boshqa	Kompaniyalar o'zlarining mijozlar bazasi haqidagi ma'lumotlarni marketing kompaniyalariga sotishlari va/yoki shaxsiy atributlar	Bu turdagi Do-Not-Track opsiyasi iste'molchining maxfiylik huquqining muhim qismidir. Ushbu siyosat nafaqat maxfiylikni ta'minlash, balki tajovuzkorlar tomonidan buzilgan qo'shimcha ob'ektlarga ma'lumotlar

usullarda foydalanmasliklarini ta'minlash uchun qonunlar qabul qiladi, agar mijoz bunday almashishni tanlamagan bo'lsa.	bo'yicha to'plangan yoki sotib olingan ma'lumotlar asosida foydalanuvchi tajribasini moslashtirishlari odatiy holdir.	tarqalishining oldini olishga yordam beradi. Mijoz hech qachon buzilgan shaxs bilan ish qilmaganligi sababli, mijozning ma'lumotlari bunday xavfga duchor bo'lmasligi kerak. Ma'lumot almashish ko'plab mijozlarga foyda keltiradi, chunki u mijozning qiziqishi va moslashtirilgan maxsus maqsadli takliflarga imkon beradi.
Davlatlar kiberxavfsizlik bo'yicha barcha tashabbuslarida shaxsiy daxlsizlikning muhim himoyasini o'z ichiga olishi kerak.	Kiberxavfsizlik tashabbuslari ko'pincha faoliyatni aniqlash va kuzatishga qaratilgan. Ushbu siyosat ushbu tashabbuslardan maxfiylik siyosatiga rioya qilishni talab qiladi.	Yaxshi ishlab chiqilgan xavfsizlik tashabbuslari maxfiylikni ham oshirishi mumkin, chunki xakerlar va boshqa zararli shaxslar endi shaxsiy ma'lumotlarga kira olmaydi. Maxfiylik ba'zi odamlar uchun vaziyatga qarab xavfsizlikdan ko'ra dolzarbroq tashvishdir. Vaqti-vaqti bilan xavfsizlik va maxfiylik o'rtasida kelishmovchiliklar bo'ladi va jamiyatlar har bir alohida holatda ushbu ikki maqtovga sazovor maqsad o'rtasida eng yaxshi kelishuvni amalga oshirishlari kerak.
Xalqaro tashkilotlar davlatlar o'rtasidagi maxfiylik qonunlaridagi farqlarni yaxshiroq hal qilish uchun ma'lumotlarni	Turli mamlakatlar shaxsiy daxlsizlik qonunlarini boshqacha belgilaydi, chunki har bir xalqning o'z qonunlari,	Global standartlar maxfiylik talablarini yaxshiroq tushunishga, fuqarolar uchun maxfiylikni yaxshilashga va iqtisodlarga imkon berishi mumkin. Bunday uyg'unlashtirish

tasniflash bo'yicha harakatlarni uyg'unlashtirishga yordam beradi.	an'analari va muvozanatlari bor.	imkonsiz bo'lishi mumkin, chunki, aytaylik, Qo'shma Shtatlar, Xitoy va hatto ittifoqchilar o'rtasidagi tafovutlar ularning elektron tijorat bizneslariga iqtisodiy ta'sir ko'rsatadi, shuning uchun ham ittifoqchilar o'rtasidagi uyg'unlikni sezilarli harakatlarsiz bartaraf etib bo'lmaydi. Yagona, global maxfiylik standarti imkonsiz va istalmagan bo'lishi mumkin; ammo, xalqaro tashkilotlar asosiy tamoyillar bo'yicha kelishib olishga yordam berishi mumkin
Milliy hukumatlar mavjud qonunlarni ularning kiberxavfsizlikka qanday tatbiq etilishini aniqlash uchun ko'rib chiqishi va bo'shliqlar mavjudligini va ularni yangilash zarurligini aniqlashi kerak (masalan, texnologiyaga nisbatan neytralroq).	Bu kiberxavfsizlik bilan bog'liq qonunlarni milliy darajada ko'rib chiqishni talab qiladi. Ba'zi qonunlarni yangilash kerak bo'lishi mumkin; boshqalar kiberxavfsizlik muammolariga yangi yechimlarni taklif qilishlari mumkin.	Ushbu siyosat maxfiylikni himoya qilish uchun xavfsizlik qoidalarini o'rnatishga imkon beradi texnologlar emas, balki ijtimoiy olimlar. Kiberxavfsizlik kontekstida tanqidiy ko'rib chiqilishi kerak bo'lgan qonunning yaxshi namunasi 1934 yildagi AQShning Mudofaa ishlab chiqarishi va telekommunikatsiyalar to'g'risidagi qonunidir. Bunday ko'rib chiqish natijasida olingan xulosalar, xulosalar va tavsiyalar qonun chiqaruvchi xodimlarni yangi qonunlar yoki o'zgartirishlar kiritish haqida xabardor qilishi

		kerak. eskilar. Ko'pincha eski qonunlarni ko'rib chiqish shaxsiy hayot himoyachilari va xavfsizlik o'rtasida ziddiyatlarga olib keldi.
Veb-saytda e'lon qilingan Maxfiylik siyosati talab qilinishi va muvofiqligi isbotlanishi kerak.	Siyosat jarayon va protseduradan farq qilganligi sababli, maxfiylik siyosatini shunchaki ko'rsatish uni amalga oshirish uchun texnik kafolatlar mavjudligini anglatmaydi.	Maxfiylik siyosati bugungi kunning ilon moyidir. Ular iste'molchi baholash vositasi sifatida har qanday qiymatga ega bo'lishlari uchun ular tartibga solinishi kerak. Maxfiylik siyosati tabiatan shartnomaviy emas, balki kompaniyaning xavfsizlik pozitsiyasining bayonotidir. Dasturiy ta'minotdan foydalanish qoidalari va shartlari oxirgi foydalanuvchi litsenziya shartnomalari bilan tartibga solinadi.
Tegishli Internet-administrator jismoniy shaxslarga o'zlari haqidagi ma'lumotlarni sotish usulini taqdim etishi kerak va boshqa hech qanday shaxsni aniqlash mumkin bo'lgan ma'lumotlar bozori mavjud bo'lmasligi kerak.	Shaxsiy ma'lumotlarni yig'ish va sotish uchun ko'plab imkoniyatlar mavjud bo'lsa-da, ulardan foyda olish imkonini beradigan hech qanday vosita mavjud emas.	Internetda shaxslarning profilini aniqlashning turli xil usullari mavjud va hech kimga Elektron kabi maxfiylikni himoya qilish guruhi tavsiyalarini inobatga olmasdan ruxsat berilmasligi kerak. Internet saytidan foydalanish haqidagi ma'lumotlar elektron tijorat sotuvchilari tomonidan to'planadi va ularga haqli ravishda tegishli. Modomiki, ismlar yoki (elektron pochta) manzillari yordamida individual

		atributlar amalga oshirilmasa, bunday ma'lumotlar qimmatli hisoblanadi.
Foydalanuvchilar to'g'risida ma'lumot to'playdigan har bir veb-sayt to'plangan maydonlarni foydalanuvchi tanlashi uchun ochiq qilib qo'yishi yoki ularni rad etishga ruxsat berishi kerak.	Ushbu siyosat barcha Internet saytlarini Grahm-Leach-Bliley Act (GLBA) kabi moliyaviy maxfiylik qoidalariga bo'ysundiradi, bunda ma'lumotlar faqat mijozga bevosita xizmatlar ko'rsatish maqsadida ishlatilishi mumkin.	GLBA uchun amalga oshirilgan rad etish siyosatlari ko'pincha noqulay va talqin qilish qiyin bo'lgan. Sog'liqni saqlash sug'urtasi portativligi va javobgarligi to'g'risidagi qonun (HIPAA) tomonidan asoslantirilgan maxfiylik bildirishnomalari odatda e'tiborga olinmaydi, chunki ularni imzolashning alternativi muqobil tibbiy yordam ko'rsatuvchi provayderni izlashdir. Ushbu siyosatlarda sukut bo'yicha ma'lumot to'planishiga yo'l qo'ymaslik bo'lishi kerak, agar rasmiy ravishda tasdiqlanmasa, chora ko'rishni talab qilmaslik kerak. Internetda taklif qilinadigan har qanday xizmat foydalanuvchiga shaxsiy ma'lumotlarni to'plashdan voz kechish imkonini berishi kerak va agar kompaniyalar reklama daromadining etishmasligi ushbu siyosatni sotib olish imkonsiz deb da'vo qilsalar, ular buni amalga oshirishlari mumkin.
Iste'molchilar huquqlarini himoya	Ushbu siyosat shaxsiylashtirishni	Veb-saytga tashrif buyuruvchilar xizmat uchun

qilish agentliklari keraksiz shaxsiylashtirishni taqiqlashlari kerak.	shaxsni identifikatsiyalash mumkin bo'lgan ma'lumotlar sifatida ko'rib chiqishni talab qiladi, ular hozirda asosan moliyaviy masalalarga qaratilgan.	pul to'lamasliklari sababli, ular veb-sayt mijozlari emas va shuning uchun veb-sayt iste'molchilari hisoblanmaydi. Iste'molchilar huquqlarini himoya qilish agentliklari uchun shaxsiylashtirish bo'yicha maxfiylikka nisbatan ustuvorliklarni belgilash shaffoflikni, foydalanuvchi tomonidan o'rnatiladigan boshqaruvni, xavfsizlikni kuchaytirishni, ma'lumotlarni saqlashni cheklashni va foydalanuvchi roziligi va/yoki oshkor qilish usullari beriladi.
Iste'molchi qurilmalari uy telefonining xususiyatlari bilan sozlanmasligi kerak.	Uyali telefon, elektron o‘quvchi va o‘yinlar kabi mahsulotlar odatda ishlab chiqaruvchi yoki xizmat ko‘rsatuvchi provayderga foydalanuvchining qurilma bilan o‘zaro aloqasi yoki qurilmadagi ma’lumotlarni taqdim etish uchun ma’lumot to‘playdi.	Bu siyosat iste'molchilarga o'zlarining shaxsiy ma'lumotlari bir kun kelib o'zlariga zarar etkazishi mumkinligidan xavotirlanmasdan qurilmalardan foydalanishga imkon beradi, hatto ularning elektron pochtasiga reklama hujumining oldini olish uchun ham. Iste'molchi qurilmalarining ko'plab mijozlari o'zlarining xizmat ko'rsatuvchi provayderlariga yanada moslashtirilgan xizmatlar evaziga ularning xatti-harakatlarini kuzatishga ruxsat berishga tayyor.

		Dasturiy ta'minot ishlab chiqaruvchilardan mavjud ma'lumotlar maydonlarini oshkor qilishni talab qilish mantiqiyroq bo'lar edi.
Xavfsiz simsiz xizmatlarga o'z xohishi bilan ulangan foydalanuvchilar maxfiylikni kutmaydilar.	Simsiz xizmatlar ko'pincha ulangan foydalanuvchilar bir-birining trafigini ko'ra oladigan tarzda taqdim etiladi. Bu, shuningdek, ba'zi quruqlikdagi xizmat takliflarida ham mavjud, ammo foydalanuvchilar sanoat standarti usullari orqali simsiz tarmoqqa ulanganda bo'lgani kabi, bu imkoniyat haqida aniq ogohlantirilmaydi.	Tarmoq xizmatlarining tez o'zlashtirilishi tarmoqning o'tkazish qobiliyatiga bo'lgan talablarni qondirishni qiyinlashtirdi. Foydalanuvchilarning bir-birini tinglashiga yo'l qo'ymaydigan xavfsizlik xususiyatlaridan keng foydalanish sekinlashadi Tarmoqqa ulanish jadallik bilan shaxsiy hayot uchun talabga aylanib borayotganini inobatga olsak, foydalanuvchilardan tirikchilik va shaxsiy hayot o‘rtasida tanlov qilishni talab qiladigan xizmatlarni taqdim etish axloqiy emas.

Kiber boshqaruv muammolari. Harbiylar o'z missiyasi atrofida o'z resurslarini tartibga solishda cheksiz muvaffaqiyatga erishgan bo'lsa ham, harbiy kibermudofaani o'rnatish bo'yicha eng yaxshi rejalar uning fuqarolik infratuzilmasiga kutilmagan qaramligi tufayli past bo'lishi mumkin. Ham davlat, ham xususiy telekommunikatsiyalar uchun infratuzilmani ta'minlovchi nom maydonlari va raqamlash tizimlari xususiy sanoat tomonidan boshqariladi. Kasbiy intizom sohasi sifatida texnologiya amaliyoti boshqa sohalarga nisbatan ancha yosh. Dasturiy ta'minot me'morlarida jismoniy ob'ektlar me'morlari singari ustoz yoki shogirdlik tizimi yo'q. Texnologiya bo'yicha maslahatchilar tibbiy maslahatchilar singari bir qator imtihonlar orqali o'z kasblarini o'rganishlari shart emas. Xaridor ehtiyot bo'lish - kunning qoidasi. Shunday qilib, texnologiya amaliyoti sohasi, kutilmaganda, texnologik

noto'g'ri ishlash maydonini keltirib chiqardi. Texnologiyani noto'g'ri ishlatish bo'yicha tekshiruvlar xavfsizlik masalalariga rahbariyatning e'tiborsizligi shubhasi bilan asoslanadi. Masalan, ular AQSh Federal Savdo Komissiyasi tomonidan e'tiborsizlik bilan bog'liq qonuniy ishlar bo'yicha dalillarni taqdim etadilar.

Shunga qaramay, xavfsizlik bo'yicha mutaxassislarning yarim asrlik amaliyoti kiberxavfsizlik bo'yicha katta bilimlar to'planganini ko'rsatdi. Shunga o'xshash texnologiya arxitekturasi va operatsion jarayonlarining umumiy tajribasi eng yaxshi amaliyotlar va qoidalarni berdi, chunki ularni universal qabul qilish uchun ilmiy asos yo'qligi sababli ularni chetga surib qo'ymaslik kerak. Ushbu bo'lim kiberxavfsizlikni boshqarishda muntazam ravishda yuzaga keladigan ayrim siyosat muammolarini o'rganadi. Kiberxavfsizlik kompyuter tizimlari tomonidan kuzatilayotgan aktivlarni boshqarish uchun uzoq vaqtdan beri foydalanilgan va shuning uchun kiberxavfsizlik menejmenti aktivlarni boshqarish bo'yicha ishonchli javobgarlik bajarilishini ta'minlash uchun nazorat va muvozanatlarni qo'llashga odatlangan. Kiberxavfsizlikni boshqarish ko'pincha texnologiya imkoniyatlari va tizim talablarini o'rganish bilan boshlanadi. Bu tashkilotning texnologiya komponentlarini sotib olish, qurish yoki autsorsing qilish qobiliyatiga bog'liq va shuning uchun ta'minot zanjirini boshqarish texnologiya amaliyotida muvaffaqiyatga erishish uchun muhim talabdir. Ko'pincha kiberxavfsizlikni boshqarish xavfsizlik funktsiyalarini himoya qilinadigan aktivlar bilan chambarchas bog'liq bo'lgan kibermakonni boshqarish sohalariga topshirishga harakat qiladi. Biroq, bu delegatsiyaga urinishlar ba'zan vakolat berilgan hududda xavfsizlik ko'nikmalarining etishmasligi tufayli muvaffaqiyatsizlikka uchraydi. Ushbu muammoning tez-tez taklif qilinadigan yechimi xavfsizlik bo'yicha mutaxassislar uchun sertifikat yoki akkreditatsiyaning bir turidir. Ushbu talablar korporativ kibermakon infratuzilmasiga kiritilgan xizmatlar va uskunalar yetkazib beruvchilariga taalluqlidir. Kiberxavfsizlik xavfidan himoyalanish uchun tekshiruvlar va muvozanatlar talab qilinadi. Kiberxavfsizlik amaliyotlari bo'yicha katta hajmdagi tadqiqotlar muvaffaqiyatli xavfsizlik yechimlarini ta'minladi va bu mutaxassislarni xavfsizlikni loyihalash va ishlatish bo'yicha yo'l-yo'riq ko'rsatuvchi tamoyillarni qabul qilishga olib keldi. Biroq, 3-bobda muhokama qilinganidek, kiber-kosmosdan foydalanishning mavjud va paydo bo'lgan stsenariylarini qamrab olish uchun ko'proq tadqiqot va ishlanmalar talab etiladi.

2.6-jadval

Kiberxavfsizlik siyosatining kiber urushga oid masalalari

Siyosat bayonoti	Izoh	Qarama-qarshilik sabablari
Qurollarni nazorat qilish bo'yicha xalqaro harakatlar kiberxavfsizlik texnologiyasining tarqalishini cheklashga qaratilgan bo'lishi kerak.	Bu yadroviy qurol siyosatiga o'xshab kiberxavfsizlik siyosati bo'lib, uning tarqalishi to'xtatilishi kerak va shu bilan dunyo xavfsizroq joyga aylanadi.	Hujumkor kiber qobiliyatlarning tarqalishi juda qiyin bo'lar edi, agar uni to'xtatish imkonsiz bo'lmasa. Ularni aniqlash qiyin, nisbatan arzon va har qanday podvalda yoki kompyuter laboratoriyasida ishlab chiqilishi mumkin. Yaylov tarqalishini to'xtatish bo'yicha har qanday shartnomani tekshirish yoki amalga oshirish deyarli mumkin emas. Qurollarni nazorat qilish bo'yicha xalqaro sa'y-harakatlar qurolning o'ziga emas, balki ruxsat etilgan nishonlar va kiberhujumlardan foydalanish doirasini cheklashga qaratilgan bo'lishi kerak. Buni amalga oshirish uchun mumkin bo'lgan ramkalar qurolli to'qnashuv qonunlarining mavjud cheklovlarini yoki kiberdan foydalanishni cheklashga intilayotgan yangi tuzilmalarni o'z ichiga oladi. Kiberxavfsizlikda “o'q-dorilar” yoki “qurol” atamalarining ta'rifi ushbu siyosatni samarali qo'llash uchun etarlicha

		tushunilmagan. Ushbu turdagi siyosat 1900-yillarning oxirida kriptografik texnologiyalarning tarqalishini cheklashga urinishlarning asosi edi. Bu siyosat istalmagan oqibatlarga olib keldi
Harbiy rahbarlik xalqaro me'yorlarni belgilashga yordam beradigan va mudofaa istiqbollarini belgilashga yordam beradigan deklarativ siyosatni e'lon qilishi kerak.	Deklaratsion siyosat keng ijtimoiy maqsadlarga qarshi birinchi marta foydalanmaslik, viruslar yoki qurtlardan foydalanmaslik, hujumlar himoyalangan ob'ektlardan (kasalxonalar kabi) kelib chiqmasligi kabi elementlarni o'z ichiga olishi mumkin.	Deklaratsiya siyosati variantlarni cheklash uchun ishlatilishi mumkin. Deklarativ siyosat shaffoflikni yaxshilaydi va imkoniyatlar va doktrinani rivojlantirishga yordam beradi. Agar yaxshi so'z bo'lsa, ular olib qo'yish shart emas Aksincha, ular hech qachon e'tiborga olinmaydigan variantlarni haqli ravishda cheklaydi. Deklaratsion siyosat dushmanlarga harakatlarini oldindan ko'rishga imkon beradi.
Harbiy rahbarlik kibermakon va qo'llab-quvvatlash siyosati bo'yicha milliy xavfsizlik strategiyasini ishlab chiqishi va e'lon qilishi hamda ittifoqchilar bilan muvofiqlashtirishi kerak.	Kibermakon uchun milliy xavfsizlik strategiyasi asosiy qarorlar va ular kelishilgan maqsadlarni qanday qo'llab-quvvatlashini ta'kidlashi kerak. Huquqbuzarlik va	Strategiyalar yuqori rahbariyat uchun o'z niyatlariga shaffoflik berishning samarali usullaridir va ularning byurokratiyasiga rahbarlik qiladi. Kibermakon bo'yicha milliy strategiyalar ko'pincha haddan tashqari

	mudofaa o'rtasidagi muvozanat, asosiy tashkilotlarning roli, operatsiyalarni muvofiqlashtirish, fuqarolik hokimiyati va xususiy tuzilmalar bilan o'zaro hamkorlik masalalari hal qilinishi kerak.	tasniflanishi mumkin - bu begonalarning keraksiz tashvishlariga sabab bo'ladi - va kiber mojaroni haddan tashqari militarizatsiya qiladi, chunki uni harbiylar hal qilish uchun eng yaxshi jihozlangan muammo deb biladi.
Harbiy rahbarlik xususiy sektor tashkilotlari bilan operatsiyalarni muvofiqlashtirishi kerak.	Kibermakonda xususiy sektor ustunlik qiladi, chunki u boshqa sohalarda emas. Kosmosda, havoda va hatto ochiq okeanda ham bu sohalarda bo'shliq hukmronlik qiladi. Hatto quruqlikda ham odamlar imkoni bo'lsa, mojarodan qochib ketishadi. “Kosmos” ning o'zi yaratilgan va unga tegishli bo'lgan kibermakonda bunday imkoniyatlar mavjud emas	Milliy kibermudofaani ta'minlash uchun xususiy sektor tashkilotlari juda zarur. Agar ular harbiy strategiyalar yoki texnologiyalarga ishonmasalar, ular yoqmagan dasturlarni bekor qilish yoki to'sqinlik qilish uchun milliy rahbariyat bilan aralashishlari mumkin. Kelajakda kibermojarolar ularning tarmoqlari va tizimlarida olib borilishi mumkinligi sababli, ular bilan yaqin muvofiqlashtirish mudofaa uchun juda muhimdir. Harbiylar hamma narsani tasniflashga moyildir va xususiy sektor bilan ishlash bo'yicha har qanday mandat, daromadni himoya qilish uchun xususiy sektorning kiberxavfsizlik

		harakatlari bilan raqobatlashadigan tasniflash harakatlariga oid dalillar bilan yakunlanishi mumkin.
Harbiylar hujum va mudofaa kiberoperatsiyalari, kinetik va kiberoperatsiyalar, hujum va ekspluatatsiya o'rtasida hamda fuqarolik hamkasblari bilan keng ko'lamli muvofiqlashtirishlari kerak.	O'zining ta'minot zanjiri va maqsadli aktiv egalari bilan muvofiqlashtirish har qanday harbiy operatsiyalar uchun hal qiluvchi omil hisoblanadi. Bular kiber-buyruqlarning fuqarolik hamkasblari.	Ushbu harakatlarning har biri kibermakonning o'ziga xos xususiyati tufayli kerak. Bu nafaqat yangi va umuman sinovdan o'tmagan, balki effektlar kaskad bo'lishi va kutilmagan fuqarolik tizimlariga ta'sir qilishi mumkin. Har qanday qarshi hujumlar raqib tomonidan mutanosib bo'lishi mumkin, ammo to'g'ridan-to'g'ri mezbon mamlakatning tanqidiy tomoniga qaratilgan bo'lishi mumkin. Bir nechta tashkilotlardan potentsial ko'p shaxslar bilan muvofiqlashtirish kiberoperatsiyalar sur'atini albatta sekinlashtiradi. Harbiylarning kiber sohasidagi missiyalari fuqarolik infratuzilmasiga, oddiygina harbiy kiberkosmosga tegmasligi kerak. Kiberqo'mondonlik o'z missiyasini bajarishi uchun xususiy sektor bilan muvofiqlashtirishning hojati yo'q, chunki uning vazifasi faqat harbiy tizimlarni kiber tahdidlardan himoya

		qilishdir. Hukumatning boshqa sohalarida kiberxavfsizlikka yordam ko'rsatish uchun katta nizom mavjud Ko'pgina malakali kiber-mudofaa operatsiyalari markazlari xususiy sektorga tegishli va boshqariladi. Agar harbiylar ular bilan muvofiqlashmasa, ular yutqazadi Faol mudofaa jamoatchilik va ayniqsa, maxfiylik guruhlarini katta tashvishga solmoqda. Agar noto'g'ri va ehtiyotkorlik bilan bajarilgan bo'lsa, vaqtinchalik foyda bo'lmaydi Ba'zi hukumat infratuzilmalari fuqarolik va harbiy foydalanuvchilarni qo'llab-quvvatlovchi ikki tomonlama foydalanishi mumkin. Ularning harbiy faoliyati maqsad yoki jahon rahbariyati tomonidan nomutanosib deb qaralishi mumkin. Bundan tashqari, agar maqsadlar kaskadi bo'lsa, faoliyat aslida nomutanosib va/yoki noqonuniy bo'lishi mumkin. Qanday bo'lmasin, bu mojaroni yanada kuchaytirishi mumkin.
Harbiylar o'zlarining kibermudofaa	Stol usti - bu ishtirokchilarga	Mashqlarni yaxshi bajarish uchun oldindan keng

rejalarini, shu jumladan davlat sektori va boshqa davlatlarni real tarzda mashq qilishlari kerak.	oddiy stsenariylar bo'ylab o'tishga imkon beradigan mashqlar bo'lib, ular ishtirokchilarga qaror qabul qilishda mashq qilish, ularni berilgan javob standarti bo'yicha sinab ko'rish yoki ishtirokchilarni javob rejalari bilan tanishtirish imkonini beradi. Stol usti, shuningdek, qanday javoblar bo'lishi mumkinligini aniqlash uchun yangi tushunchalarni o'rganish uchun ishlatiladi.	qamrovli rejalashtirish talab qilinishi mumkin. Umuman olganda, mashg'ulotlar va darslarning sifati yuqoriroq rejalashtirish va resurslarni talab qiladi. Demak, mashqlarning xarajati-foydasi muqobildan, ya'ni hozirgi kiber-josuslik holatlarini o'rganishdan ustun bo'lmasligi mumkin. Ushbu mashg'ulotlar natijalari milliy strategiya, ko'rsatkichlar, hodisalarga javob berish rejalari va harbiy doktrinaga qayta aloqa sifatida zarur. Ushbu mashqlar keng ko'lamli milliy urush o'yinlarigacha bo'lgan javob rejalarining o'ziga xos jihatlarini o'rganish uchun kichik maqsadli stol usti o'yinlarini o'z ichiga olishi kerak. Mashqlar ishtirokchilarga tinchlik davrida javob berish, qaror qabul qilish va muvofiqlashtirishni mashq qilish imkonini beradi, ularga xato qilish, o'z rollarini o'rganish va oqibatlari kamroq ahamiyatga ega bo'lganida “mushak xotirasini” yaratish imkoniyatini beradi. Ushbu darslarni nisbatan arzon narxlarda o'rganish mumkin Stol usti mashqlari ideal

		o'quv vositalari sifatida e'lon qilinadi, lekin o'z ishini tushunadigan hech bir qo'mondon kibermakonni himoya qilish uchun nima qilish kerakligini tushunish uchun o'yin o'ynash uchun turli xil qimmatli inson resurslarini to'plashi shart emas. Bundan tashqari, eng muhim qaror qabul qiluvchilar odatda mashqlarda qatnashmaydilar va ular ma'lumotlarni ishlab chiqarish usullariga qisqartiriladi.
Harbiylar nafaqat axborot texnologiyalari bo‘yicha mutaxassislarning an’anaviy kiber ishchi kuchini, balki “bahs ostidagi soha” bilan bog‘liq missiyalar uchun zarur bo‘lgan xodimlarni ham o‘z ichiga olgan holda, o‘z kiber ishchi kuchining malakasini oshirishi kerak. kibermakon.	Ko'pincha “kiber ishchi kuchi” “IT ishchi kuchi” bilan birlashtiriladi. Harbiylar missiya operatsiyalarida operatorlar, himoyachilar, harbiy rejalashtiruvchilar, sudyalar advokatlari va razvedka yordami kabi odatiy axborot texnologiyalarini qo'llab-quvvatlash bilan bog'liq bo'lmagan kiber ko'nikmalarni talab qiladi.	Harbiylarning axborot texnologiyalarini qo'llab-quvvatlashi va kiberkosmik missiyalarni amalga oshirish uchun zarur bo'lgan xodimlar o'rtasida hech qanday bo'linish bo'lmasligi kerak. Harbiy texnologiyani ishga tushirish boshqa mudofaa missiyalari bilan teng darajada missiya deb hisoblanishi kerak. Boshqa har qanday yondashuv axborot texnologiyalari xodimlarini tark etadi Kiberkosmosda harbiy missiyalarni bajarishdan ko'ra texnologik infratuzilmani boshqarish uchun turli ko'nikmalar to'plami talab qilinadi. Ushbu siyosat harbiylarga

		ishchi kuchining chuqurligi va kengligini va tegishli ravishda to'liq tushunish imkonini beradi IT bo'lmagan xodimlarga topshirilgan kiber topshiriqlarga e'tibor hujumlarni amalga oshiruvchilarning ahamiyatini oshirib yuborishi mumkin, ular odatda umumiy kiber ishchi kuchining kichik foizini tashkil qiladi. Bu ularning xizmatlari kibermudofaa topshiriqlaridan ko'ra muhimroq degan noto'g'ri taassurot qoldirishi mumkin.
Harbiylar “dushmanga eng ko'p duch kelgan” ishchi kuchining qo'shimcha jangovar tayyorgarlikdan o'tishini ta'minlashi kerak.	Raqibga qarshi hujum qilish yoki himoya qilishda asosiy rolga ega bo'lganlarning barchasi kinetik tengdoshlariga o'xshash jangovar fikrga ega bo'lishi kerak.	Ichkaridan kelib chiqadigan kiberhujumlar keng tarqalganligi sababli, harbiy kiber ishchi kuchining qaysi qismi ko'proq dushmanga duch kelishini aniqlash mumkin emas. Barcha kiberxodimlar raqib kibertahdidlarni tan olish va ularga qarshi kurashishda teng qobiliyatga ega bo'lishi kerak. Chunki har doim uni ta'minlash uchun resurslardan ko'ra ko'proq treninglar talab qilinadi. mashg'ulotlar darhol foydali bo'lishi mumkin bo'lgan joyga taqsimlanishi kerak.
Harbiy rahbarlik	Boshqa domenlar	Kibermakonni domen

kibermakonni xuddi havo, quruqlik, fazo va an'anaviy domenlar kabi urush sodir bo'lishi mumkin bo'lgan yangi soha sifatida ko'rib chiqishi kerak.	singari, u xalqaro, shaxsiy va tijorat manfaatlariga ega, o'z geografiyasiga ega joy. Kosmos va havodan farqli o'laroq, u kirish uchun juda kam to'siqlarga ega.	sifatida ko'rib chiqish nafaqat uning ahamiyatini oshirishga yordam beradi kibermakon, lekin mutaxassis bo'lmaganlar uchun tushunishni osonlashtiradi. Kibermakonni harbiy domen sifatida tasniflashning kutilmagan natijasi shundan iboratki, harbiy amaliyotlar uni urushga qarshi domen sifatida ko‘rib chiqishi mumkin, lekin buni unutib qo‘yadi. Artilleriya domen bo'lgani kabi kibermakon ham domen emas. Bu havo, dengiz va quruqlikni zabt etishda ishlatiladigan asbobdir.
Harbiy rahbarlik kibermudofaani huquqbuzarlikdan ustun qo'yishi kerak.	Kibermudofaa - bu dushmanlarning kiberhujum imkoniyatlaridan samarali foydalanishini to'xtatish qobiliyati. Kiberhuquq (kiber fazoda dushmanlarga hujum qilish uchun kinetik bo'lmagan kiber imkoniyatlardan foydalanish) ham muhim harbiy	Faol kibermakon bo'lmasa, davlatlar o'z iqtisodiyotini boshqara olmasligi, mojaro paytida siyosiy qarorlar qabul qila olmasligi yoki harbiy kuch ishlab chiqara olmasligi mumkin. Agar mudofaa deb hisoblanmasa, ularning har biri yoki barchasi raqib tomonidan buzilishi mumkin Bu siyosat faqat kibermakondan foydalangan holda muhim infratuzilmani boshqaradigan davlatlar uchun mantiqiy. Dunyodagi

	qobiliyat hisoblanadi.	ba'zi ittifoqdosh davlatlar kibermakonga shunchalik kam bog'liqki, ularning hamjamiyatlari kontekstida ularning marjinal dollarlari sodiqlik eng yaxshi hujumga sarflanadi. Mudofaa murakkab va qimmat bo'lishi mumkin, huquqbuzarliklar esa to'xtatuvchi bo'lishi mumkin va shu bilan ham mudofaaga hissa qo'shishi mumkin. Nazariy jihatdan, ba'zi dushmanlarni to'xtatib qo'yish mumkin
Kiber huquqbuzarlik haqiqiy, ba'zan hatto afzal qilingan harbiy qobiliyat sifatida qaralishi kerak.	Bu siyosat barcha harbiy amaliyotlar uchun birinchi navbatda kiberhujumlarni an'anaviy jismoniy hujumlardan ustun qo'yadi.	Kiberhuquq yadroviy qurolga teng, chunki undan foydalanish tinch aholiga nomutanosib ravishda ta'sir qilishi mumkin. Keng miqyosdagi tanqidiy kiberhujumlar infratuzilma, albatta, nomutanosib ta'sirga ega bo'lishi mumkin. Kiberhujumlar kutilmagan oqibatlarga olib kelishi mumkin bo'lsa-da, kiberhujumlar ko'proq kinetik bo'lmagan hujumlar sifatida qo'llanilishi mumkin, ular na o'ldiradi, na o'ldiradi. Kinetik temir bomba bilan nishonga olingan sayt o'rniga havo hujumidan mudofaa saytini o'chirib qo'yadigan kiberhujum sayt

		operatorlarining hayotini saqlab qolishi mumkin. Xuddi shunday, elektr energetika tizimiga kiberhujum ham kinetik hujum natijasida yuzaga keladigan shunga o'xshash ta'sirga qaraganda ancha vaqtinchalik va qaytariladigan zararga olib kelishi uchun tuzilgan bo'lishi mumkin. Komandirlar kirish huquqiga ega bo'lgan joyga kinetik bo'lmagan va halokatli bo'lmagan qobiliyatlar, bu hujumlardan foydalanish insoniyroqdir.
Harbiy rahbarlik vaqt o'tishi bilan kibermojaro uchun o'z qobiliyati va kuchlarini an'anaviy urush doktrinalari va tuzilmalariga birlashtirishi kerak.	Tarixan harbiy kiber qobiliyatlar razvedka, maxsus hujum dasturlari yoki axborot texnologiyalarini mustahkamlash dasturlari bilan bog'langan. Bu kiberxavfsizlikni harbiy tashkilotlar tomonidan boshqariladigan missiyalarni normal tushunishdan tashqariga qo'yadi. Bu siyosat reintegratsiya maqsadini	Hujum va mudofaa (va razvedka) operatsiyalarini birlashtirish jang maydonida integratsiyalashgan effektlarni beradi, kiberkosmik operatsiyalar bundan mustasno bo'lmasligi kerak. Ixtisoslashgan kibertashkilotlar muhim maqsadlarga xizmat qiladi, ammo ularning imkoniyatlari rasmiy boshqaruv va boshqaruv tizimiga birlashtirilishi kerak. Turli xil kiberxavfsizlik operatsiyalari bo'lishi qiyin bo'lishi mumkin

	belgilaydi.	Harbiy tashkilot kiber qobiliyatlarni integratsiyalashda nisbatan etuk bo'lmagan joyda, kuchlarni birlashtirish kichik kibermojaro bo'linmalari dastlab ishlab chiqilgan missiyalar va mudofaa dasturlarini buzadi va bu dasturlarni kiberxavfsizlikni qo'llab-quvvatlashning jiddiy etishmasligi bilan qoldiradi.
Harbiy rahbarlik kibermakon uchun boshqa domenlarni aks ettiruvchi, lekin kibermakon voqeliklariga taalluqli bo'lgan ishtirok etish qoidalarini ishlab chiqishga ustuvor ahamiyat berishi kerak.	Jang qoidalari do'stona kuchlar boshqalarga nisbatan qachon va qanday kuch ishlatishi mumkinligini belgilaydi. Kinetik urushda ular nisbatan sodda yoki (masalan, tartibsiz urush paytida) juda qiyin bo'lishi mumkin. Kibermojarolarda ular nafaqat urushning yangi sohasi bo'lgani uchun, balki texnik jihatdan ham qiyin bo'ladi. kiberkosmosning tabiati.	Bu siyosat qatnashish qoidalari o'ta cheklovchi bo'lib boshlanishini anglatishi mumkin, chunki ular vaqt o'tishi bilan siyosiy rahbarlar, qo'mondonlar, operatorlar va advokatlar yanada tanish va bilimdon bo'lib qolguncha shunday bo'lishi kerak. Jang qilish qoidalari mavjud bo'lmaganda, harbiylar nazoratsiz yoki bilmasdan dushmanlik va zararli kiberkosmik operatsiyalarni amalga oshirishi mumkin. Jang qoidalari harbiylarni xalqaro huquqiy tomonda ushlab turadigan narsadir
Harbiy rahbarlik muayyan maqsadlar va imkoniyatlardan	Faol mudofaa odatda hujumlarda ishtirok etgan	Ushbu hududlarning har birida, odatda, harbiylar buni ta'qib qilishlari mutlaqo

ehtiyot bo'lishi kerak: faol mudofaa, atrof-muhitni kiberoperativ tayyorlash va chet elliklarni nishonga olish kabi.	tizimlarni “qaytarib olish” qobiliyatini anglatadi. Kiberelementlar tajovuzkor hujumdan oldin xorijiy tizimlarga bostirib kiradi. Xorijiy infratuzilmalar chet el harbiylariga bog'liq bo'ladi va bu odatda qonuniy maqsadlardir.	qonuniydir maqsadlar va imkoniyatlar; ammo, buni juda ehtiyotkorlik bilan qilish kerak. Kiber-operativ rejalashtirish elementlari hujumkor harakatlarga tayyorgarlik ko'rish uchun zarur bo'lgan qobiliyatdir, ammo keskinlashuvchi bo'lishi mumkin, chunki dushmanlar kiberni ko'rishlari mumkin.
Kiberhujumlar “tahdid yoki kuch ishlatish” yoki “qurolli hujum” (BMT Nizomiga muvofiq) hujumning ko‘lami, davomiyligi va intensivligiga qarab hisoblanadi.	Ushbu chegaralar xalqaro harakatlar kuch, mojaro yoki urush darajasiga ko'tariladimi va maqsadli davlat yoki xalqaro hamjamiyat bunga javoban qanday harakatlar qilishi mumkinligini aniqlash uchun kalit hisoblanadi.	Bu siyosat faqat o‘sha hujumlarga teng ta’sir ko‘rsatishini ta’minlaydi kinetik qurollardan harbiy kuch ishlatishning yuqori nuqtasida qurolli hujumlar hisoblanadi, kuch ishlatish tahdidi yoki undan foydalanish esa pastki qismida. Agar kiberhujumlar katta ziyon keltirishga mo'ljallangan bo'lsa-da, lekin o'z maqsadiga erisha olmasa, bu hujumlar urush harakatlari sifatida qabul qilinishi kerak. Ularga ahamiyatsiz munosabatda bo'lish dushmanga o'z ahvolini yaxshilash uchun to'siqsiz imkoniyat beradi

Davlatlar o'z chegaralarida joylashgan kibermakon elementlari uchun javobgar hisoblanadi.	Kibermakon odatda chegarasiz deb hisoblansa-da, u jismoniy dunyoga asoslangan va davlatlar suveren chegaralarida joylashgan jismoniy infratuzilma va tashkilotlarda ishlaydi.	Shunga ko'ra, davlatlar o'z chegaralaridan boshlangan kiber urush hujumlari uchun javobgar bo'lishlari va agar imkoni bo'lsa, hujumni to'xtatishlari shart. Bu mas'uliyat hujumning ko'lami, davomiyligi va intensivligiga qarab o'zgarishi kerak. Agar davlatlar ushbu majburiyatni bajara olmasalar, maqsadli davlatlar qarshi choralar ko'rishga haqlidirlar (BMT Nizomi va qurolli mojaro qonunlariga muvofiq). Agar xususiy guruhlar davlat nomidan hujumlar uyushtirsa, davlat guruh ustidan umumiy nazoratni ushlab tursa, javobgarlikka tortilishi mumkin. (masalan, manbalar yoki nishonlar va qurollar bo'yicha ko'rsatmalar berish) Davlatlarni javobgarlikka tortish repressiv mamlakatlarni yanada ko'proq himoya qilishi mumkinshaxsiy daxlsizlik va so'z erkinligini cheklash. Bundan tashqari, Qo'shma Shtatlarda juda ko'p Internet infratuzilmasi (va ko'plab xavfsiz bo'lmagan kompyuterlar) mavjud bo'lib, u ko'plab hujumlarni to'xtatish uchun

		katta kuch sarflashi kerak.
“Kiberterrorizm”ni kibermakon orqali amalga oshiriladigan terroristik hujumlar deb hisoblash kerak.	Ishga olish yoki tarqatish kabi harakatlartarg'ibot terroristik hujum emas va ular kibermakonda sodir bo'lgani uchun “kiber terrorizm” deb hisoblanmasligi kerak. Faqat kiber tizimlar yoki ma'lumotlarni o'chirib qo'yadigan, yo'q qiladigan yoki buzadigan va terrorizmga qaratilgan kiber hujumlar kiber terrorizm deb hisoblanishi kerak.	Kiberterrorizmga shunday munosabatda bo'lish terrorizmga hech qanday aloqasi bo'lmagan, lekin tez-tez sodir bo'ladigan ko'plab hujumlarni istisno qilish orqali tushunchani sezilarli darajada soddalashtiradi. bu belgi beriladi “terrorizm” deb atash orqali ba'zi tashkilotlar foyda olishga muvaffaq bo'ldi

Kiberinfratuzilma muammolari. Ushbu bo'limda xususiy sektor tarmoqlari duch keladigan kiberinfratuzilma muammolarining yorqin misollari mavjud. AQSh Ichki xavfsizlik departamentining Milliy infratuzilmani himoya qilish rejasi (NIPP) xususiy sektor tomonidan boshqariladigan muhim infratuzilma va mamlakatning asosiy resurslari (CIKR) kabi 18 ta misolni tan oladi. Ba'zilari boshqalardan ko'ra faolroq bo'lishiga qaramay, ushbu sektorlarning har biri rejaga ko'ra milliy infratuzilmani ta'minlash uchun davlat-xususiy sektor hamkorligi sa'y-harakatlarida ishtirok etishni talab qiladi. Tarmoqlar ro‘yxatiga oziq-ovqat va suv tizimlari, qishloq xo‘jaligi, sog‘liqni saqlash tizimlari,

favqulodda xizmatlar, axborot texnologiyalari, aloqa, bank va moliya, energetika (elektr, atom, gaz va neft, to‘g‘onlar), transport (havo, avtomobil yo‘llari, temir yo‘l) kiradi,kimyo va mudofaa sanoati, pochta va yuk tashish korxonalari, milliy yodgorliklar va piktogrammalar.
Bo'limda moliyaviy xizmatlar, sog'liqni saqlash va sanoat nazorati tizimlarining illyustrativ sohalarida axborotni ta'minlash siyosatining muhokamalari va misollari keltirilgan. E'tibor bering, sanoat boshqaruv tizimlari o'zi sanoat sektori emas, balki sanoatning turli sohalarida qo'llaniladigan avtomatlashtirilgan uskunalar turi uchun umumiy belgidir.

2.7-jadval

Tadqiqot va ishlanmalarga oid kiberxavfsizlik siyosati masalalari

Siyosat bayonoti	Tushuntirish	Qarama-qarshilik sabablari
Millat ijroiya hokimiyati kiberxavfsizlik siyosati bo'yicha maslahat berish va kiberxavfsizlik dasturlarini baholash uchun turli sohalardan kiberxavfsizlik bo'yicha ekspertlar qo'mitasini yig'adi.	Bu Millat ijroiya hokimiyati (masalan, AQSh Prezidenti) o'zining kichik maslahatchilari doirasidan tashqariga chiqish va kiberxavfsizlik strategiyasi masalalari bo'yicha yordam so'rash uchun talabdir.	Kiberxavfsizlik muammolarining kengligi va chuqurligi har qanday shaxsning tajribasidan tashqarida. Milliy liderlar eng ma'rifiy qarashlarga ega bo'lishi kerak. Bunday yuqori darajada siyosat o'rnatishga hojat yo'q. Milliy liderlar muhim masalalar bo'yicha maslahat so'rash va olishning bir qancha yo'llari va jarayonlari allaqachon mavjud. Kiberxavfsizlik muammolari bunga kiradi
Milliy hukumat milliy strategiyada belgilangan ustuvorliklarga muvofiq kiberxavfsizlik xavfi, tizimlar va dasturiy ta'minot	Ushbu siyosat dasturiy ta'minot, test, kompyuter va tarmoq domenlarida kiberxavfsizlik tadqiqotlarini moliyalashtirishni	Tadqiqot va ishlanmalarni moliyalashtirish nafaqat bugungi tahdidlarga nisbatan qo'llanilishi mumkin bo'lgan yangi xavfsizlik texnologiyasini ishlab chiqaradi, balki aspirantlarni

bo'yicha fundamental va amaliy tadqiqotlarni moliyalashtirishga yordam beradi. Iloji boricha, bunday tadqiqotlar hamkorlikda, ko'p tarmoqli va tasniflanmagan bo'lishi kerak.	ta'minlaydi. Shuningdek, u milliy xavfsizlikka ta'sir ko'rsatadigan ko'p tarmoqli tadqiqotlarni (xavfsizlik bo'yicha tadqiqotlar, yuridik va xalqaro aloqalar bo'limlari bilan) o'z ichiga olishi kerak.	kiberxavfsizlik muammolarini o'rganishga undaydi va shu bilan kelajakdagi kiberxavfsizlik tahdidlarini bartaraf etadi. Hukumatning ilmiy-tadqiqot va ishlanmalarni moliyalashtirishi ba'zan xususiy sektor uchun yanada dolzarb deb hisoblangan muammolarni bartaraf qilishi mumkin. Bundan tashqari, agar tadqiqotchilar boshqa tadqiqotlardan bexabar bo'lsalar (masalan, u tasniflangan loyihaning bir qismi sifatida amalga oshirilgan bo'lsa), moliyalashtirish takroriy va behuda bo'lishi mumkin.
Hukumat har yili kiberxavfsizlik bilan bog'liq barcha tadqiqot va ishlanma investitsiyalarini ko'rib chiqadi.	Ushbu siyosat kiberxavfsizlik uchun ajratilgan milliy tadqiqot va ishlanmalar mablag'lari qanday sarflanishini tavsiflovchi yillik hisobot ishlab chiqarishni talab qiladi.	Kiberxavfsizlik bo'yicha aniq tadqiqot kun tartibi bo'lmasa, bunday baholash informatsion hisobotdan farqli ravishda sub'ektiv mashq bo'ladi. Eng yaxshi holatda, bu boshqa joyda osongina topiladigan ma'lumotlarning oddiy ro'yxati bo'lar edi, Milliy hukumat uchun strategik ahamiyatga ega bo'lgan tadqiqotning boshqa yo'nalishlari universitetga tegishli tadqiqot dasturlari bilan qo'llab-quvvatlanadi.
Xususiy sektor	Xususiy sektor	Ushbu siyosat

kompaniyalariga kiberxavfsizlik bo'yicha tadqiqotlar olib borish uchun soliq imtiyozlari beriladi.	kompaniyalari odatda xavfsizlik standartlariga rioya qilishadi va o'zlarining innovatsion echimlarini ishlab chiqish o'rniga mavjud mahsulotlardan foydalanadilar. Ushbu siyosat innovatsiyalarni rag'batlantirishga qaratilgan.	kiberxavfsizlik tadqiqotlarining umumiy miqdorini ishtirokchilarni bozorga jalb qilish orqali. oshiradi Hozirda kiberxavfsizlik bilan shug'ullanmaydigan kompaniyalar soliq imtiyozlari bilan jalb qilinishi mumkin emas, ammo bunday soliq imtiyozlari kompaniyalarning tegishli sohadagi mavjud tadqiqot harakatlarini, masalan, mijozlarni kuzatishni kiberxavfsizlikni identifikatsiya qilish mexanizmlari sifatida qayta tasniflashiga olib kelishi mumkin. Bu xavfsizlik imtiyozlarisiz soliq tushumlarining umumiy qisqarishiga olib keladi. Bu siyosat xususiy kompaniyalarni kiberxavfsizlik bo'yicha tadqiqotlarga pul sarflashga undashi mumkin, ammo ular kabi millat foyda olishiga kafolat yo'q
Aktsiyadorlik jamiyatlari aktsiyadorlariga kiberxavfsizlik bo'yicha tadqiqotlar olib borish uchun	Ushbu siyosat xavfsizlik maqsadlariga intiladigan kompaniyalarda aktsiyalarning	Kiberxavfsizlikni o'rganishga investitsiyalar haqiqiy xavfsizlik foyda keltirmasligi mumkin bo'lgan sarf-xarajatlar emas, balki bozor

soliq imtiyozlari beriladi.	maqbulligini oshirishga qaratilgan.	natijalariga ko'ra baholanishi kerak. Bu siyosat xususiy sektorni kiberxavfsizlik sohasidagi tadqiqotlarni moliyalashtirishga undaydi. Bu ularning bozor qiymatini oshirishi va rag'batlantirishi mumkin
Talabalarning kiberxavfsizlik sohasidagi iqtidori va innovatsiyalarini taqdirlash uchun milliy tanlovlar tashkil etiladi. Boshqa musobaqalar ham taniqli universitetlarni mukofotlashi mumkin va tadqiqot muassasalari.	Pul mukofotlari bilan o‘tkaziladigan tanlovlar iqtidorli talabalarni kiberxavfsizlik masalalarini o‘rganishga jalb etishga qaratilgan.	Ushbu siyosatni amalga oshirish talabalar hamjamiyatini yaratishi kerak Ushbu dastur talabalarni mudofaadan ko'ra zararli xakerlikdan foydalanish usullarini o'rganish uchun mukofotlashi mumkin.
Davlatlar boshlang'ich yoki o'rta maktab o'quvchilaridan boshlab kibermudofaa bo'yicha xabardorlikni, ta'limni va o'qitishni va kiberhimoyachilar uchun maxsus texnik tayyorgarlikni	Kiberxavfsizlik, kiberxavfsizlik va kiberaxloq hozirda boshlang'ich va o'rta maktabda pilot dasturlarning predmeti bo'lib, bu siyosat ularni asosiy o'quv dasturiga ko'chiradi.	Ushbu siyosat erta yoshda kiberxavfsizlik haqida tanqidiy fikrlashni rivojlantirishga yordam beradi va shu orqali bo'lajak qaror qabul qiluvchilarga axloqiy tamoyillarni kelajak tizimlariga kiritishga ta'sir qiladi. Ushbu siyosat butun mamlakat bo'ylab kiberxavfsizlik darajasini oshiradi. Umumiy aholi

davom ettirishni rag'batlantirishlari kerak.		kibermakonda o'zini qanday himoya qilishni yaxshiroq tushunadi, axborot xavfsizligi bo'yicha mutaxassislar esa ularning tizimlari va dasturiy ta'minotini qanday himoya qilishni yanada intuitiv tushunishga olib keladi. Ta'lim keng ko'lamli sa'y-harakatlardir, chunki ko'pchilik kibermakon bilan shug'ullanadi va turli darajadagi tushunishga muhtoj. Bu potentsial qimmat va uzoq muddatli harakatni anglatadi. Bundan tashqari, agar texnologiyaga xos bo'lgan xabardorlik dasturlari (“bolalar uchun xavfsiz faks bilan shug'ullaning!”), ular tezda rivojlanadi.
Milliy hukumatlar kiberxavfsizlik bo'yicha o'qishni istagan talabalarga davlat xizmatida bo'lish evaziga universitet stipendiyalarini taqdim etishlari kerak.	Ushbu siyosat talabalarni kollej darajasida kiberxavfsizlikni o'rganishga undash uchun mo'ljallangan. Bakalavr kolleji o‘quv dasturlari odatda kiberxavfsizlik bo‘yicha mutaxassislikni o‘z ichiga olmaydi.	Mamlakatda milliy manfaatlarni himoya qilish uchun talab qilinadigan ishlarni to'ldirish uchun kiberxavfsizlik bo'yicha bilimli mutaxassislar etarli emas. Milliy stipendiya dasturi malakali mutaxassislarni ta'minlaydi. Bakalavr dasturlari bitiruvchilari kiberxavfsizlik bo'yicha katta tajribaga ega bo'lmaydilar.

		Kiberxavfsizlik yo'nalishi odatda magistratura darajasida boshlanadi, chunki har qanday sohada kiberxavfsizlikni qo'llash uchun zarur bo'lgan asosiy bilimlar miqdori bakalavriatda konsentratsiyani talab qiladi. Ushbu siyosat kiberxavfsizlik bo'yicha o'quv dasturini yaratishga turtki bo'ladi va talabalarni hukumatda kiberxavfsizlik bo'yicha ish olib borishga undaydi. Shuningdek, u universitetlarni dasturlarni ishlab chiqishga undashi mumkin
Akademik hamjamiyatlar kiberxavfsizlik sohasi assotsiatsiyalarining talabalar bo'limlarini olib borishlari kerak.	Ko'pgina sanoat birlashmalari talabalar bo'limlarini o'stiradi, ammo kiberxavfsizlik professional uyushmalari hozirda bu yo'nalishda unchalik katta tezlikka ega emas.	Bugungi kunda talabalar ijtimoiy tashkilotlar bilan shug'ullanishadi. Kiberxavfsizlikdan muhimlik ijtimoiy tarmoqlardan voz kechishga sababdir. Kiberxavsizlik professional tashkilotlari talabalar inilishlari kerak bo'lganf tajriba ega va ular veb-saytlarda bepul mavjud.
Kiberxavfsizlik tizimlari, texnologiyalari va operatsiyalari bo'yicha tadqiqotlar va ishlanmalar	Ko'pincha menejment kiber muhitni nazorat qilishni xohlaydi, lekin nazoratni amalga oshirish	Ushbu siyosat aktivlarni nazorat qilish uchun mas'ul bo'lgan menejerlarga, hatto hozirgi bo'lsa ham, uzoq muddatda buni amalga oshirish uchun vositalarni

kibermakon va joriy xavfsizlikni ta'minlash uchun boshqaruv maqsadlari o'rtasidagi bo'shliqlarni to'ldirish uchun zarur bo'lgan darajada amalga oshirilishi kerak.	uchun usullar, vositalar va protseduralar yo'q. Bu holat ularni shunday holatga keltiradi vakolatsiz javobgarlik	beradi. Bu kabi siyosatlar tashkilot uchun oldindan ko'rinadigan foydasiz kiberxavfsizlik bilan bog'liq barcha turdagi tadqiqotlar uchun ochiq chek kitobi sifatida ko'rib chiqilishi mumkin.
Barcha dasturiy ta'minotni ishlab chiqishda dasturiy ta'minotni ishlab chiqishning hayot aylanishini ta'minlash uchun eng yaxshi amaliyotlar qabul qilinishi kerak.	Bu siyosat xavfsiz dasturiy ta'minotni kodlash amaliyotiga, shuningdek, xavfsizlik testlariga rioya qilishni talab qiladi.	Ma'lumki, xavfsiz kodlash amaliyotlari o'rnatilganda zaifliklarni kamaytiradi Innovatsiyalar tashkiliy strategiya va jarayonni doimiy ravishda o'zgartirishni talab qiladi. Xavfsiz kodlash amaliyotlari texnologiya tezligiga moslashish uchun juda statikdir.
Barcha tizimlarni ishlab chiqishda tizimni ishlab chiqish hayotiy siklini ta'minlash uchun eng yaxshi amaliyotlar qabul qilinishi kerak.	Ushbu siyosat yuqoridagiga o'xshaydi, lekin bitta dasturiy ta'minot komponentining xavfsizligini emas, balki butun tizim yondashuvini qabul qiladi.	Tizim xavfsizlik talablari bo'lgan eng yaxshi xavfsizlik amaliyotlari talablari ishlab chiqish jarayonining boshida ko'rib chiqiladi va mahsulot xususiyatlariga birlashtiriladi. Xavfsizlik talablari boshqalardan ustun bo'lmasligi kerak

Nazorat savollari.

1. Diskontlangan pul oqimi tahlili (DCF) nima va uning cheklovlari qanday?

2. Muhandislik tizimlarini loyihalash kontekstida moslashuvchanlik

nima?

3. Loyihalarni baholashda ROA usulidan foydalanishning an’anaviy ko‘rsatkichlarga nisbatan qanday afzalliklari bor?

4. Strukturaviy tezkor tizimni loyihalash jarayoni qanday asosiy elementlarni o'z ichiga olishi kerak?

5. Buyuk Britaniya hukumat idoralari tomonidan talab qilinadigan minimal kiberxavfsizlik standartining nomi nima?

6. CTI nima va uning maqsadi nima?

7. Kibermakondagi raqibning tahdid profilini belgilovchi asosiy omillar nima?

8. Tahdidlarni tahlil qilish hayotiy siklini tashkil etuvchi sohalar qaysilar?

9. CTIni doimiy ravishda takomillashtirish va tashkil etish uchun qanday qo'shimcha yo'nalishlar kerak?

10. Ishonch belgisi nima va u CTI manbasining ishonchliligini baholashda qanday ma'nolarga ega bo'lishi mumkin?

11. Boshqa manbalar tomonidan tasdiqlangan ma'lumotlarning ishonchliligini aniqlash uchun qanday mezonlar qo'llaniladi?

12. Axborotning CTI funksiyasi va uning talablari bilan mosligi nimani anglatadi?

13. Nima uchun NCSC tahdid tasmalaridagi barcha ma'lumotlar CTI tahlilchilari uchun foydali emas?

14. Yig'ilgan ma'lumotlar sifatini baholashda qaysi asosiy yo'nalishlarga e'tibor berish kerak?

15. Nima uchun CTI to'plashda to'g'ri ma'lumotlar formatini ta'minlash muhim?

III bob. KIBERXAVFSIZLIK SIYOSAT YONDASHUVLARI. GEOPOLITIKA VA KIBERXAVFSIZLIK

3.1-§. Kiberxavfsizlik siyosati: AQSH yondashuvi

Ushbu bobda AQSh federal hukumati tomonidan qabul qilingan kiberxavfsizlik siyosati strategik nuqtai nazardan ko'rib chiqiladi. 1990-yillarning boshlariga qadar AQShning kiberxavfsizlik siyosati elektron yozuvlarning tarqalishiga to'g'ridan-to'g'ri javob bo'lib, 2-bobda tasvirlangan. Bu erda biz strategiya va tegishli siyosatni belgilab bergan federal darajadagi kiberxavfsizlik muammolarining so'nggi tarixini keltiramiz. Ushbu bobda hukumatning tarixiy voqealarga javoban qilgan harakatlari tushuntiriladi va hukumat kelajakdagi chora-tadbirlarni ko'rib chiqishi mumkin bo'lgan sohalar taklif etiladi. Bu Vashingtondagi bugungi siyosiy munozaralarni shakllantirgan so'nggi yigirma yillikdagi eng muhim voqealarni qisqacha tarixiy ko'rib chiqish bilan boshlanadi. Aksariyat tadbirlar aniq kiberfazoga qaratilgan bo'lsa-da, ba'zilari kiberxavfsizlik siyosatiga qo'shgan hissalari nuqtai nazaridan darhol e'tiborga olinmaydi. Biz ushbu tarixiy sharhni 1990-yillarning boshlarida qo'shma Shtatlarga qilingan terroristik hujumlar bilan boshlaymiz va keyingi ma'muriyatlar tomonidan amalga oshirilgan harakatlarga o'tamiz. Bob tarix tomonidan tasvirlangan strategiya va siyosat haqidagi umumiy fikrlar bilan yakunlanadi.

AQSh federal hukumatining kiberxavfsizlikka bo'lgan siyosiy munosabati milliy standartlar va texnologiyalar instituti (MSTI) va Milliy xavfsizlik agentligi (MXA) tomonidan ishlab chiqilgan qat'iy standartlarga rioya qilishdan tortib, vaziyatning jiddiyligini to'liq bilmaslikgacha bo'lgan. Xardoim AQSh Senati va AQSh vakillar palatasida, kiberxavfsizlik bilan bog'liq bir necha o'nlab qonun loyihalari rivojlanishning turli bosqichlarida bo’ladi. Ushbu qonun loyihalarining aksariyati avvalgi Kongress tomonidan boshlangan sa'y-harakatlarning qayta yozilgan versiyalari bo'lib, ularning ba'zilari butunlay yangi harakatlardir. Ishlab chiqilayotgan qonun hujjatlarining hech biri o'z-o'zidan mamlakatimiz duch keladigan kiberxavfsizlik muammolarini “hal qilmaydi”. Darhaqiqat, har qanday kiberxavfsizlik siyosati bo'yicha mutaxassis, ehtimol, Kongress akti kiber makon xavfsizligini ta'minlashda katta qiymatga ega ekanligiga ishonish o'rinli emas.

Albatta, Kongress harakatlari yoki to'g'ridan-to'g'ri davlat idoralari orqali kiberxavfsizlik siyosatini shakllantirishga ko'p urinishlar bo'lgan. Shuningdek, siyosat va strategiyaning bir-biriga mos kelishi haqida

ko'plab taxminlar va tushunmovchiliklar mavjud. Sof strategiya-bu qaror qabul qiluvchining hamma narsa qanday ishlashini xohlashining sxemasi. Strategiyani amalga oshirish uchun siyosat jarayon, protsessual munosabat, standartlar va ijro bilan birlashtiriladi. Strategiyaga qarab, uni yaratish uchun zarur bo'lgan narsalar ro'yxati to'liq bo'lmasligi mumkin. Bundan tashqari, strategiyani amalga oshirish uchun yaxshi rejalashtirilgan va bajarilgan urinishlar ham ba'zida strategik maqsadlarga olib kelmasligi mumkin. Bu, ayniqsa, strategiya amalga oshirilayotganda rivojlanadigan muhitda, masalan, tez o'zgaruvchan kiber-kosmik dunyoda to'g'ri keladi.

Masalan, 2006 yilda shaxsiy ma`lumotlarni o'g'irlash muammosi davlat siyosatining mavzusi bo'lishi aniq bo'ldi. O'sha paytda, har qanday potentsial qonunchilikning maqsadi bo'lishi mumkin bo'lgan eng yirik kredit karta kompaniyalari to'lov kartalari sanoatining xavfsizlik standartlari Kengashini tuzdilar, bu esa o'z navbatida to'lov kartalari sanoatining ma'lumotlar xavfsizligi standartini ishlab chiqdi. Standartlar mavjud moliyaviy maxfiylikni himoya qilish siyosatiga muvofiqligini namoyish etish uchun qabul qilingan va bizning oramizdagi axloqsizlar taxmin qilganidek, har qanday qo'shimcha Qonunchilik zarurligi haqidagi fikrni rad etish uchun qabul qilingan. Biroq, standartlar qabul qilingandan keyin ham, sanoat tomonidan yaratilgan standartlarga javob beradigan yirik to'lov tizimlari shaxsiy ma'lumotlarning o'g'irlanishiga olib keladigan ommaviy ma'lumotlarning buzilishi manbai bo'lgan. Iste'molchilarning harakatlarini kuzatishni taqiqlovchi maxfiylik standartlarini ixtiyoriy ravishda qabul qilish orqali o'z-o'zini tartibga solishga o'xshash urinish onlayn reklama sohasida amalga oshirilmoqda. Ushbu misollar standartlar va siyosatlar juda boshqacha narsalar ekanligini va siyosatga muvofiqligini ta'minlash uchun mo'ljallangan standartlar buni amalga oshirishi shart emasligini ko'rsatadi.

Kiberjinoyatlarning o'sishi. Har qanday madaniyatda omadsizroq, ishonuvchan va shaxsiy xavfsizligiga e'tibor bermaydiganlarning afzalliklaridan foydalanadigan jinoyatchilar bo'ladi. Internet madaniyati bundan farq qilmaydi, bundan tashqari ko'plab jinoyatchilar o'zlarining hunarmandchiligini deyarli noma'lum va aksariyat huquqni muhofaza qilish organlari qo'li etmaydigan joyda qilishlari mumkin. Umuman olganda, Internet jinoyati kredit kartalarini o'g'irlash, firibgarlik, onlayn qimor o'yinlari va pornografiyaga, shuningdek, foydalanuvchilarni soxta elektron pochta va soxta veb-saytlar bilan aldashga qaratilgan. Boshqa jinoyatlar orasida intellektual mulkni o'g'irlash, shu jumladan peer-to-peer

fayllarni almashish va buzilgan yoki ko'chirilgan dasturlarni sotish yoki tarqatish kiradi.

1990-yillarda ko'plab xavfsizlik bo'yicha mutaxassislar biz internetdagi ba'zi bir jiddiy nosozliklar-“kiber Pearl Harbor” bilan to'qnashuv yo'lida ekanligimizga ishonishdi. Biroq, 2003 yil oxiri va 2004 yil boshlarida yana bir tahdid paydo bo'ldi va shu vaqtdan beri sahnada hukmronlik qilmoqda. Uyushgan jinoyatchilik Internetda qimmatli narsa ko’pligini va bularni e'tiborsiz qoldira olmasligini angladi. Bu barcha onlayn foydalanuvchilarni yangi jinoyat qurboniga aylantiradi va ko'pincha ular o'g'irlangan yoki aldanganligini bilishmaydi.

Eng yomoni, “veb 2.0” texnologiyasining jadal rivojlanishi (wiki, peer-to-peer, ijtimoiy media va o'zini ifoda etishning boshqa shakllari) jinoyatchilarga bexabar qurbonlardan foydalanishni yanada osonlashtirdi. Sanoat korxonalarida vaziyat bundan ham yomonroq — bu yangi texnologiyalarning aksariyati modernizatsiya qilinayotganda eski tizimlarni almashtirmoqda. ICS/SCADA tizimlarini kuzatish va ishga tushirish uchun Web 2.0 texnologiyalarini joriy qilish orqali biz ichki nazorat tarmoqlarimizni tashqi jinoiy hamjamiyat uchun ochishimiz mumkin. Muhim infratuzilmani boshqarish tizimi juda katta ahamiyatga ega va butun dunyo bo'ylab jinoiy guruhlar sizning har qanday kichik xatolaringizdan foydalanishga atigi millisekund vaqt yetarli bo’ladi.

2008 yildan beri har yili Verizon nashr etadi ma'lumotlar buzilishini tekshirish to'g'risidagi hisobot (DBIR- Data Breach Investigation Report) nomli hisobotni, katta ma'lumotlar bazalariga oqib chiqadigan voqealar ketma-ketligi bo'yicha tergov tahlilini o'z ichiga oladi. Yildan-yilga Verizon jamoasi barcha yirik ma'lumotlar buzilishlarining aksariyati jinoiy niyatlar tufayli yuzaga kelganini aytdi. 2010 yilda tekshirilgan (qavs ichidagi raqam 2009 yilga nisbatan foiz o'zgarishi) va 2011 yilda nashr etilgan 800 ga yaqin qonunbuzarliklarga asoslangan so'nggi statistik ma'lumotlar shuni ko'rsatadiki:

- 92% tashqi omillarga bog'liq (+22%);
- Ishtirok etgan insayderlarning 17% (-31%);
- 9% da bir nechta tomonlar ishtirok etdi (-18%);
- 50% xakerlikning u yoki bu shaklidan foydalangan (+10%);
- O'rnatilgan zararli dasturlarning 49% (+11%);
- 29% jismoniy hujumlar bilan bog'liq (+14%);
- 17% - imtiyozlardan noto'g'ri foydalanish natijasi (-31%);
- 11% ijtimoiy taktikadan foydalangan (-17%);

— Qurbonlarning 83% imkoniyat qurbonlari bo'lgan;
— * 92% hujumlar juda murakkab emas edi (+7%);
— Barcha ma'lumotlarning 76% serverlardan buzilgan (-22%);
— 86% uchinchi tomon tomonidan aniqlangan (+25%);
— 96% qoidabuzarliklarning oldini olish oddiy yoki oraliq nazorat yordamida amalga oshirildi;
— PCI-DSS qurbonlarining 89% talablarga javob bermadi (+10%).

Jinoyatchilarga qarshi kurashchilar kiberhujumda jinoyatchilarni aniqlash va ularni ta'qib qilishni tezda o'rganadilar, ammo bu jangda g'alaba qozonish oson emas. Bugungi kunda aniq ustunlik jinoyatchilar tomonida. Umid qilamizki, bir necha yil ichida afzallik yaxshi qo’llarga o'tadi, ammo hozircha Internet 150 yil oldingi yovvoyi G'arb bilan bir xil.

So'nggi bir necha yil ichida yanada dahshatli jinoiy usul — Janubi-Sharqiy Osiyoda ishlab chiqarilgan va Amerika bozorlariga mo'ljallangan soxta kompyuter va tarmoq uskunalari paydo bo'ldi. Federal qidiruv byurosi va boshqa huquqni muhofaza qilish organlari tomonidan olib borilgan tekshiruvlar shuni ko'rsatdiki, Qo'shma Shtatlarga keladigan barcha elektronikaning taxminan 10% soxta yoki juda ko'p miqdordagi soxta qismlarni o'z ichiga oladi. Bundan ham yomoni, xorijiy hukumatlar o'z mamlakatlarida ishlab chiqarilgan va ochiq jahon bozorida sotiladigan mahsulotlarga ataylab orqa eshiklar va boshqa yashirin kirish imkoniyatlarini o'rnatayotgani haqidagi nazariyani qo'llab-quvvatlovchi dalillar ortib bormoqda. Mudofaa vazirligi, Milliy xavfsizlik va boshqalar bu muhim infratuzilma tizimlari va tarmoqlari uchun uzoq muddatda nimani anglatishi mumkinligidan jiddiy xavotirda.

Josuslik va milliy davlatlarning harakatlari. Sovuq urush davrida va undan oldingi asrlarda mamlakatlar chet elda ishlash uchun josuslarni yollash va o'qitish bilan katta xavf ostida edilar. Bugungi kunda Internet josuslikni veb-brauzerni ochish va keyinchalik qidiruv tizimiga kirish kabi osonlashtirdi va o'lim xavfini deyarli nolga tushirdi. Albatta, bu nazariya faqat yaxshi aloqalarga ega bo'lgan mamlakatlarni kuzatish uchun yaxshi.

Hukumatlardan tashqari, ko'plab kompaniyalar “raqobatbardosh razvedka” deb nomlanuvchi faoliyat bilan shug'ullanadilar, korporativ josuslik uchun evfemizm. Bu shunchalik mashhur bo'ldiki, hatto barcha korporativ strategik va raqobatbardosh razvedka josuslari yoki SCIP

1990-yillarning oxirida AQShning bir nechta hukumat tizimlarida yashirin hisoblar va ko'plab ruxsatsiz faoliyat mavjudligi aniqlandi. Tergov davom etar ekan, federal hukumatdan tashqarida ko'proq

kompyuterlar va tizimlar ruxsatsiz hisoblarga ega ekanligi aniqlandi. “Ma'lumotlarni filtrlash” “bosqin” yoki “ruxsatsiz kirish” emas, balki yangi shov-shuvli so'zga aylandi. Maqsadlar atmosfera ma'lumotlari, batimetrik ma'lumotlar va o'nlab yillar davomida to'plangan boshqa ma'lumotlarni o'z ichiga olgan katta ma'lumotlar bazalari edi. Hujumlarning kelib chiqishi noaniq edi-tajovuzkorlar hujumlarni bir nechta buzilgan kompyuterlar orqali yo'naltirish uchun murakkab usullardan foydalanganlar va o'g'irlangan ma'lumotlarni yig'ish punktlari sifatida “qayta tiklash saytlari” dan foydalanganlar. Hech qanday holatda buzilish belgilari kuzatilmagan. Bularning barchasi elektron josuslikka o'xshardi, intellektual mulkni o'g'irlashning klassik holati, faqat Internet orqali, Jeyms Bond kabi mikrofilmlar va josuslik kamerasi bilan emas.

Sovuq urush davrida josuslik hamjamiyati AQShning SSSRga qarshi josusligiga aniq e'tibor qaratgan. Ammo so'nggi yillarda e'tibor sobiq sovet mamlakatlaridan Xitoyga o'tdi. Xitoyda madaniyat akademik yutuqlarni qo'llab-quvvatlaydi. Ko'pgina talabalar va o'qituvchilar internetga tajriba sifatida qarashadi va doimiy ravishda masofaviy tizimlarga kirishadi yoki zaif dasturiy ta'minotdagi xatolarni faqat akademik maqsadlarda aniqlaydilar. Ularning topilmalari ilmiy maqolalarda chop etiladi va tadqiqotchilar keyingi loyihaga o'tadilar. Biroq, ba'zilar ushbu tadqiqotning aql bovar qilmaydigan qiymatini topdilar va o'z natijalarini hukumatlarga, jinoiy guruhlarga va hatto terrorchilarga sotish orqali undan biznes qilishni boshladilar.

2003 yilda xitoylik deb taxmin qilingan bir qator kiberhujumlar Amerika kompyuter tizimlariga qaratilganligi aniqlandi. Mudofaa vazirligi tomonidan “Titanik yomg'ir” deb nomlangan bosqinchilik bo'yicha tergov ushbu voqea matbuotga tarqalguncha maxfiy bo'lib qoldi. Matbuotga sizib chiqqandan so'ng, tajovuzkorlar ko'plab kompyuter tarmoqlariga, jumladan Lockheed Martin, Sandia National Laboratories, Redstone Arsenal va NASAga kirish huquqiga ega ekanligi ma'lum bo'ldi. Tergov nomlari yillar davomida o'zgargan bo'lsa-da, josuslik bugungi kungacha davom etmoqda.

Xitoy kiber-josusligi 2006 yilning bahorida, xususiy sektor tizim ma'muri uning ko'plab foydalanuvchilari Xitoy tilini o'z ichiga olgan Microsoft Word qo'shimchalari bilan elektron pochta xabarlarini olishlarini payqaganida ommaga ma'lum bo'ldi. Word ochilganda ishlamay qoldi va foydalanuvchi Microsoft bilan ma'lumotlarni baham ko'rishni xohlaydimi yoki yo'qligini so'rab dialog oynasi paydo bo'ldi. Tizim ma'muri SANS Internet Storm Center bilan bog'landi, u o'z

navbatida muammo haqida kundalik nashr etdi. Bir necha kundan so'ng, muammo Word-da nol kunlik zaiflik bilan bog'liq edi. Hujumchilar Microsoft Office mahsulotlaridagi ob'ekt havolasi kengaytmalari (OLE) yordamida ma'lum bir xotira joyiga ma'lumotlarni yozish uchun zaiflikdan foydalanib, Word hujjatlarini o'zgartirish usulini topdilar. Ushbu usul tajovuzkorlarga o'zlari tanlagan zararli kodni o'rnatish yo'lini taqdim etdi, bu oddiy kalitlarni ro'yxatdan o'tkazish dasturidan tortib, tajovuzkorga olingan kompyuterni to'liq boshqarish imkoniyatini beradigan to'liq “rootkit” paketlariga qadar bo'lishi mumkin.

Ammo Xitoy josuslik yoki kiber urush uchun o'zgartirilgan axborot texnologiyalari mahsulotlariga nisbatan yagona gumondor emas. Ehtimol, ushbu tendentsiyaning eng yaxshi (va eng qo'rqinchli) misoli 2010 yil o'rtalarida Stuxnet qurtini aniqlash edi. Bir yoki bir nechta G'arb davlatlari tomonidan yozilgan deb taxmin qilingan dasturiy ta'minot Eronda o'rnatilgan yadro yoqilg'isini qayta ishlash zavodlarining ayrim qismlariga jismoniy zarar yetkazish uchun ishlab chiqilgan. Internetga o'xshash tarmoq orqali tarqatish o'rniga, Stuxnet an'anaviy universal serial bus (USB) xotira drayverlarini yuqtirish orqali tarmoqdagi “havo bo'shliqlarini” engib o'tish uchun ishlab chiqilgan. Stuxnet-ning kelib chiqishi sir bo'lib qolmoqda, ammo manba kodi har qanday foydalanuvchi uchun yangi maqsadlar uchun o'zgartirish va qayta joylashtirish uchun mavjud.

Josuslik tahdidlarining kuchayishiga siyosiy javob: AQSh kiber qo'mondonligi. 2009 yilda Mudofaa kiber qo'mondonligi (USCYBERCOM) 1998 yilda xorijiy mamlakatlardan kelayotgan kiberhujumlarning tobora ortib borayotgan tahdidiga qarshi kurashish uchun tashkil etilgan “vaqtinchalik” tashkilot JTF-GNO vazifalarini o'z zimmasiga oldi. 2000-yillarning oxiridagi o'ta murakkab hujumlar oq uyni o'sib borayotgan tahdidga qanday qarshi turish kerakligini qayta ko'rib chiqishga va urush rejalari va operatsiyalarida kiberxavfsizlikni doimiy ravishda institutsionalizatsiya qilishga majbur qildi. Bugungi kunda USCYBERCOM mudofaa vazirligining ko'pgina tarmoqlarining operatsiyalari va himoyasini boshqaradi va prezidentning ko'rsatmasi bilan kiber kosmosda “to'liq spektrli” harbiy operatsiyalarni ham amalga oshirishi mumkin. Biroq, USCYBERCOM Internet yoki umumiy telefon tizimi kabi xususiy sektor tarmoqlarining ishlashini nazorat qilish vakolatiga ega emas.

Mudofaa vazirligi ma'lumotlariga ko'ra, USCYBERCOM Vazirlikning kiber kosmosdagi barcha operatsiyalarini birlashtiradi va

quyidagilarni o'z ichiga olgan tadbirlarni rejalashtiradi, muvofiqlashtiradi, birlashtiradi, sinxronlashtiradi va amalga oshiradi: Mudofaa vazirligining axborot tarmoqlarining kundalik mudofaasini boshqarish; mudofaa vazirligining harbiy missiyalarni qo'llab-quvvatlovchi operatsiyalarini muvofiqlashtirish; Mudofaa vazirligining ayrim axborot tarmoqlarining operatsiyalari va himoyasini boshqarish va; kiber kosmosda va rahbariyatning ko'rsatmasi bilan harbiy operatsiyalarning to'liq spektrini amalga oshirish. Qo'mondonlikka mavjud kiber-kosmik resurslarni birlashtirish, hozirda mavjud bo'lmagan sinergiyani yaratish va axborot xavfsizligi muhitini himoya qilish uchun jangovar harakatlarni sinxronlashtirish vazifasi yuklatilgan.

USCYBERCOM kiberhujumdagi operatsiyalar qo'mondonligini markazlashtiradi, mudofaa vazirligining kiberhujumdagi imkoniyatlarini mustahkamlaydi va mudofaa vazirligining kiberxavfsizlik bo'yicha ekspert bilimlarini birlashtiradi va mustahkamlaydi. Shunday qilib, USCYBERCOM mudofaa vazirligining axborot-kommunikatsiya tarmoqlarining barqarorligi, ishonchliligi, kiberhujum tahdidlariga qarshi turish va kiberhujumga kirishni ta'minlash imkoniyatlarini yaxshilaydi. USCYBERCOM sa'y-harakatlari, shuningdek, Qurolli kuchlarning tezkor va samarali operatsiyalarni ishonchli tarzda amalga oshirish qobiliyatini qo'llab-quvvatlaydi, shuningdek, qurol tizimlari platformalarini qo'llab-quvvatlovchi qo'mondonlik va nazorat tizimlari va kiberhujum infratuzilmasini nosozliklar, bosqinlar va hujumlardan himoya qiladi.

USCYBERCOM-qo'shma Shtatlar strategik qo'mondonligiga (USSTRATCOM) bo'ysunuvchi qo'shma qo'mondonlik bo'limi. Xizmat elementlariga quruqlik kuchlari kiber qo'mondonligi (MARFORCYBER); AQSh qurolli kuchlarining 24-korpusi; flot kiber qo'mondonligi (FLTCYBERCOM); va dengiz piyodalari kiber qo'mondonligi (MARFORCYBER).

USCYBERCOM mamlakatning eng sezgir tarmoqlari xavfsizligini yaxshilashda qanchalik samarali bo'lishini aniqlash kerak. Eng jiddiy muammolardan biri harbiy tashkilotlarning uzoq vaqtdan beri mavjud bo'lgan “pechka trubkasi” mentaliteti bo'ladi - menga tegishli bo'lgan narsa meniki va boshqa hech qanday guruh yoki qo'mondonlik mening plastinkamdagi narsalar ustidan hech qanday kuchga ega bo'lmasligi kerak. Kiber makonning millisekundlik tabiati va bir guruh tomonidan yuzaga keladigan xatarlar boshqa guruhlarga tezda ta'sir qilishi mumkinligini anglaganligi sababli, uscybercom muvaffaqiyatli bo'lishi uchun bu munosabat o'zgarishi kerak.

Afsuski, hamkorlik qilishdan bosh tortgan yoki himoya vositalarini birlashtirgan tashkilotlar uchun ular ushbu chegaralar bo'ylab zaif tomonlardan foydalanishni o'rgangan dushman guruhlarga nisbatan zaifroq.

Kongress harakatlari. Ushbu kitobni yozish paytida AQSh Senati va vakillar palatasida rivojlanishning turli bosqichlarida bir nechta qonun loyihalari mavjud edi. Ushbu qonun loyihalarining aksariyati avvalgi Kongress tomonidan boshlangan sa'y-harakatlarning qayta yozilgan versiyalari bo'lib, ularning ba'zilari butunlay yangi harakatlardir. Ishlab chiqilayotgan qonun hujjatlarining hech biri o'z-o'zidan mamlakatimiz duch keladigan kiberxavfsizlik muammolarini "hal qilmaydi". Darhaqiqat, har qanday kiberxavfsizlik siyosati bo'yicha mutaxassis, ehtimol, Kongress akti kiber makon xavfsizligini ta'minlashda uzoq yo'lni bosib o'tishiga ishonish o'rinli emas.

111-Kongress (2009-2010) kiberxavfsizlik muammolarini qonuniy ravishda hal qilishga uringan 50 dan ortiq alohida "kiber qonun loyihalarini" tayyorladi. Senatda muhokamaning katta qismini ikkita qonun loyihasi — Liberman/Snow Bill (Milliy xavfsizlik qo'mitasi) va Rokfeller/Kollinz Bill (savdo qo'mitasi) egallagan. Oldingi qonun loyihasi ommaviy axborot vositalarida va Vashington bo'ylab keng masxara qilingan "to'sar" kontseptsiyasini kiritdi. Bu oxir-oqibat qonun loyihasining so'zlaridan chiqarib tashlandi, ammo kontseptsiya Kongress o'zining Qonunchilik kun tartibiga nisbatan qanchalik uzoqqa borishni rejalashtirganini eslatdi. O'sib borayotgan milliy tahdidga qarshi kurashni ikki tomonlama qo'llab-quvvatlashni namoyish etish uchun 2010 yilgi oraliq saylovlardan oldin kiberxavfsizlik bo'yicha keng qamrovli qonunchilikni qabul qilish istagi kuchli edi, ammo Senat ham, vakillar palatasi ham o'z palatalarida ovoz berish uchun qonun loyihasini tayyorlay olmadilar.

Ushbu yozuv paytida 112-Kongress (2011-2012) Senatga ham, vakillar palatasiga ham kamida o'nlab kiberxavfsizlik to'g'risidagi qonun loyihalarini kiritdi. Ushbu qonun loyihalarining aksariyati 111-Kongressda kiritilgan qonun loyihalarining takrorlanishi, ammo ba'zilari yangi boshlanishdir. Biroq, Kongressning diqqat markazida byudjetlar va iqtisodiy masalalar bo'lganligi sababli, kiberxavfsizlik to'g'risidagi keng qamrovli qonun loyihasi tez orada qabul qilinishi dargumon. Vakillar palatasidagi ko'pchilik muayyan muammolarni hal qilishga qaratilgan kichik qonun hujjatlarini ishlab chiqish va qabul qilish tarafdori bo'lgan yondashuv bo'lishi mumkin.

Kiberxavfsizlik bilan bog'liq ba'zi qonun loyihalari allaqachon rad etilgan. Masalan, onlayn qaroqchilikni to'xtatish to'g'risidagi qonun va iqtisodiy ijodga va intellektual mulkni O'g'irlashga Real onlayn tahdidlarning oldini olish to'g'risidagi qonun Kongressning AQSh huquqni muhofaza qilish organlarining intellektual mulk bilan himoyalangan onlayn savdosiga qarshi kurashish imkoniyatlarini kengaytirishga qaratilgan qonun loyihalari edi. mualliflik huquqi. mulk va qalbaki tovarlar. Ushbu ikkala qonun loyihasi texnologiya hamjamiyatida keng tanqid qilindi va oxir-oqibat Vikipediya kabi nufuzli Internet saytlari norozilik sifatida bir kunga yopilganidan keyin Kongress tomonidan rad etildi.

Ushbu kitobni yozish paytida AQSh Senati va vakillar palatasida rivojlanishning turli bosqichlarida bir nechta qonun loyihalari mavjud edi. Ushbu qonun loyihalarining aksariyati avvalgi Kongress tomonidan boshlangan sa'y-harakatlarning qayta yozilgan versiyalari bo'lib, ularning ba'zilari butunlay yangi harakatlardir. Ishlab chiqilayotgan qonun hujjatlarining hech biri o'z-o'zidan mamlakatimiz duch keladigan kiberxavfsizlik muammolarini “hal qilmaydi”. Darhaqiqat, har qanday kiberxavfsizlik siyosati bo'yicha mutaxassis, ehtimol, Kongress akti kiber makon xavfsizligini ta'minlashda uzoq yo'lni bosib o'tishiga ishonish o'rinli emas.

Vakillar palatasining ikkita qonun loyihasi, H. R. 3523 (kongressmen Mayk Rojers va kongressmen golland Ruppersberger tomonidan kiritilgan kiberhujumlarni almashtirish va himoya qilish to'g'risidagi qonun 2011) va H. R. 3647 (kongressmen Daniel Lungren tomonidan kiritilgan kiberxavfsizlik va axborot almashinuvini targ'ib qilish va takomillashtirish to'g'risidagi qonun). kamroq tortishuvlar. Birinchi qonun loyihasida xususiy sektor va hukumatning kiberxavfsizlik bo'yicha muhim va vaqtga sezgir ma'lumotlarni almashishiga to'sqinlik qiladigan aniq huquqiy cheklovlar ko'rib chiqiladi. Oxirgi qonun loyihasi ancha keng qamrovli bo'lib, yangi axborot almashish tashkiloti to'g'risidagi qoidalarni o'z ichiga oladi, DHSDA kiberxavfsizlik bo'yicha yetakchi xodimni tayinlaydi, texnik kiberxavfsizlik muammolariga yangi yechimlarni topish uchun DHSDAGI tadqiqotlarni rag'batlantiradi va DHSGA kiberxavfsizlik hodisalariga javob berish bo'yicha milliy rejani ishlab chiqishni buyuradi.xususiy sektorning muhim infratuzilma aktivlari bilan birgalikda. egalari.

Vakillar palatasi va Senatning kiberxavfsizlik to'g'risidagi qonunchiligining muhim jihati bu “yopiq muhim infratuzilma”

tushunchasi — yoki xususiy sektorning qaysi qismlariga Qonunchilik qo'llaniladi. Vakillar palatasining bir qonun loyihasida ta'rif kiber himoya tufayli buzilgan yoki yo'q qilingan taqdirda, odamlarning sezilarli darajada nobud bo'lishiga, jiddiy iqtisodiy tanazzulga, yirik aholi punktlarini ommaviy evakuatsiya qilishga yoki milliy xavfsizlik imkoniyatlarining jiddiy yomonlashishiga olib kelishi mumkin bo'lgan ob'ektlar yoki funktsiyalarni o'z ichiga oladi. Bir nechta sanoat tarmoqlari ushbu ta'rifdan aniq “istisnolarni” izlaydilar, shunda ular har qanday yangi davlat nazorati yoki tartibga solishdan tashqarida qoladilar. Ularning argumenti shundaki, ularning sektorlariga tashqi kuchlar ta'sir qiladi va har qanday cheklovchi Qonunchilik texnik o'sishga to'sqinlik qiladi yoki aktiv egalarini infratuzilma tizimlaridan foydali foydalanish imkoniyatidan mahrum qiladi.

Bir nechta senatorlarning fikriga ko'ra, harakatlarning asosiy motivatori Amerika qo'shma Shtatlarining muhim infratuzilmasiga Internet orqali hujum qilish nafaqat mumkin, balki yaqin kelajakda ham bo'lishi mumkin degan xavotirdir. Kongress bo'sh qolishni istamaydi, ular inqirozdan oldin harakat qilganliklarini ko'rsatishni afzal ko'radi va bu masalaga e'tibor bermaslikda ayblanmaydi. Boshqa tomondan, xususiy sektor hukumat har qanday tartibga soluvchi yoki jazolanadigan biznes doirasini joriy etishdan oldin birinchi navbatda o'z uyini ta'mirlashni afzal ko'radi. Sanoat hukumatdan xavfsizlikni yaxshilash uchun imtiyozlar berishni afzal ko'radi, masalan, tartibga solish yukini kamaytirish, biznes soliqlarini kamaytirish va xarajatlarni qoplash uchun kreditlar yoki grantlar. Biroq, byudjetga yo'naltirilgan zamonaviy dunyoda Kongress soliq to'lovchilarga pul sarflaydigan kiberxavfsizlik to'g'risidagi qonunchilikni qabul qilishi ehtimoldan yiroq emas. Xarajatlarni neytral rag'batlantirish - bu sohalarni aniqlash kerak bo'lgan narsa, keyin esa yoqimli joyni topish mumkin.

Qisqacha tavsif. AQSh federal hukumatining kiberxavfsizlikka bo'lgan siyosiy munosabati NIST va NSA tomonidan ishlab chiqilgan qat'iy standartlarga rioya qilishdan tortib, vaziyatning jiddiyligini to'liq bilmaslikgacha bo'lgan. Ushbu bob so'nggi yigirma yil ichida federal hukumat siyosati o'zgaruvchan tahdidlarga va kiber makonga qaramlikning kuchayishiga javoban qanday o'zgarganligini ko'rsatishga harakat qildi. Internet va kiberhujum rivojlanib borgan sari, so'nggi 20 yil ichida hukumatning kiberxavfsizlik siyosati bo'yicha sa'y-harakatlari ham rivojlandi. Afsuski, kiberhujum tahdidlari va zaifliklari davlat siyosatiga qaraganda tezroq rivojlanmoqda. Maksimal harakatlar faqat hujumlarni

sekinlashtirgan yoki etkazilgan zarar miqdorini cheklagan bo'lishi mumkin.

Kiberxavfsizlik siyosati statik emas va u himoya qilish va boshqarish uchun mo'ljallangan kiberhujum kabi moslashuvchan bo'lishi kerak. Ko'pincha hukumatlar tez o'zgarishlarga moslasha olmaydi va davlat siyosati nuqtai nazaridan tezda orqada qoladi, strategiyalar, qarshi tizimlar, shuningdek, odamlarning ta'limi va xabardorligi rivojlanishda davom etmoqda. Ehtimol, federal hukumatning o'z tashkiloti juda ierarxik va chiziqli bo'lib, kompyuterlar va kompyuter tarmoqlari xavfsizligini ta'minlashda uning eng yomon dushmani bo'lishi mumkin. Aksincha, dushman tarmoqlarini juda erkin bog'langan ma'muriy rahbariyat va strategik muvofiqlashtirilgan hujumlarga qodir bo'lgan turli xil operatsion tuzilmalar boshqarishini kutish mumkin. Kiber makon murakkab va o'zaro bog'liq bo'lib, unda yagona kuch yoki nazorat nuqtasi yo'q. Tarmoqlarni himoya qilish, shuningdek, tashkilotni boshqarishda markazlashtirilmagan va ierarxik bo'lmagan yondashuvni talab qilishi mumkin. Ba'zi xususiy sektor kompaniyalari tekis, markazlashtirilmagan tashkiliy tuzilishga o'tdilar va shu bilan tashqi kuchlarga qarshi turishda muvaffaqiyat qozonishdi. Hukumat tashkilotlari modellarini kiberhujumga o'xshash qilish uchun ularni qayta ko'rib chiqish vaqti ham bo'lishi mumkin.

3.2-§. Kiberxavfsizlik siyosati: Rossiya yondashuvi

Xalqaro axborot xavfsizligini ta'minlash to'g'risidagi konventsiya

Ekaterinburgda (**2011-yil 21-22-sentyabr**) xavfsizlik masalalari bo‘yicha yuqori vakillarning ikkinchi xalqaro uchrashuvi doirasida Rossiya tomoni Xalqaro axborot xavfsizligini ta’minlash to‘g‘risidagi konvensiya konsepsiyasini taqdim etdi.

Konventsiyaning tartibga solish predmeti davlatlarning xalqaro axborot xavfsizligini ta'minlash bo'yicha faoliyati hisoblanadi.

Ushbu Konventsiyaning maqsadi *xalqaro tinchlik va xavfsizlikni buzish maqsadida axborot-kommunikatsiya texnologiyalaridan foydalanishga qarshi kurashish, shuningdek davlatlarning axborot makonidagi faoliyatini ta’minlash bo‘yicha chora-tadbirlarni belgilash:*

1) umumiy ijtimoiy-iqtisodiy rivojlanishga hissa qo'shgan;

2) xalqaro tinchlik va xavfsizlikni saqlash maqsadlariga mos keladigan tarzda amalga oshiriladi;

3) xalqaro huquqning umume’tirof etilgan tamoyillari va

normalariga, shu jumladan nizo va nizolarni tinch yo‘l bilan hal etish, kuch ishlatmaslik, ichki ishlarga aralashmaslik, inson huquqlari va asosiy erkinliklarini hurmat qilish tamoyillariga rioya qilish;

4) har bir davlatning milliy va jamoat xavfsizligi manfaatlarini himoya qilish uchun bunday huquq qonun bilan cheklanishi mumkinligini hisobga olgan holda, BMT hujjatlarida qayd etilgan axborot va g‘oyalarni izlash, olish va tarqatish huquqiga har kimning mos kelishi; shuningdek, axborot resurslaridan noto'g'ri foydalanish va ruxsatsiz aralashuvlarning oldini olish;

5) davlatlarning suvereniteti va ularning mavjud siyosiy, tarixiy va madaniy xususiyatlarini hurmat qilgan holda texnologik almashinuv erkinligi va axborot almashinuvining kafolatlangan erkinligi.

Axborot makonida xalqaro tinchlik va xavfsizlikning buzilishiga olib keladigan asosiy tahdidlar sifatida quyidagilar ko‘rib chiqiladi:

1) dushmanona harakatlar va bosqinchilik harakatlarini amalga oshirish uchun axborot texnologiyalari va vositalaridan foydalanish;

2) axborot makonida boshqa davlatning muhim tuzilmalariga maqsadli halokatli ta'sir ko'rsatish;

3) boshqa davlatning axborot resurslaridan ushbu resurslar axborot makonida joylashgan davlatning roziligisiz noto‘g‘ri foydalanish;

4) boshqa davlatning siyosiy, iqtisodiy va ijtimoiy tizimlariga putur yetkazish, aholini psixologik manipulyatsiya qilish, jamiyatni beqarorlashtirish maqsadida axborot makonidagi harakatlar;

5) xalqaro axborot makonidan davlat va nodavlat tuzilmalar, tashkilotlar, guruhlar va shaxslar tomonidan terroristik, ekstremistik va boshqa jinoiy maqsadlarda foydalanish;

6) xalqaro huquq tamoyillari va normalariga, shuningdek, davlatlarning milliy qonunchiligiga zid bo‘lgan axborotni transchegaraviy tarqatish;

7) millatlararo, irqiy va konfessiyalararo nafratni qo'zg'atuvchi, irqchilik va ksenofobik yozma materiallar, tasvirlar yoki nafratni qo'zg'atuvchi, targ'ib qiluvchi yoki qo'zg'atuvchi g'oyalar yoki nazariyalarning boshqa har qanday taqdimotini qo'zg'atuvchi axborotni tarqatish uchun axborot infratuzilmasidan foydalanish; irqi, rangi, milliy yoki etnik kelib chiqishi yoki diniga asoslangan omillar bahona sifatida foydalanilsa, har qanday shaxs yoki shaxslar guruhiga nisbatan kamsitish yoki zo'ravonlik;

8) jamiyatning psixologik va ma’naviy muhitini buzish, an’anaviy madaniy, axloqiy, axloqiy va estetik qadriyatlarni yemirish maqsadida

boshqa davlatlarning axborot makonida axborot oqimlari bilan manipulyatsiya qilish, axborotni dezinformatsiya qilish va yashirish;

9) axborot makonida amalga oshirilayotgan insonning asosiy huquq va erkinliklariga zarar yetkazadigan holda axborot-kommunikatsiya texnologiyalari va vositalaridan foydalanish;

10) eng yangi axborot-kommunikatsiya texnologiyalaridan foydalanishga qarshi kurashish, boshqa davlatlar zarariga axborotlashtirish sohasida texnologik qaramlik uchun sharoit yaratish;

11) axborotni kengaytirish, boshqa davlatning milliy axborot resurslari ustidan nazoratni qo'lga kiritish.

Ushbu tahdidlar xavfini oshiradigan qo'shimcha omillar:

1) dushmanlik harakatlarining manbasini aniqlashdagi noaniqlik, ayniqsa shaxslar, guruhlar va tashkilotlarning, shu jumladan boshqalar nomidan faoliyatni amalga oshirishda vositachilik funktsiyalarini bajaradigan jinoiy tashkilotlarning faolligi oshib borayotganini hisobga olgan holda;

2) axborot-kommunikatsiya texnologiyalariga e'lon qilinmagan buzg'unchi qobiliyatlarni kiritishning potentsial xavfi;

3) turli davlatlardagi axborot-kommunikatsiya texnologiyalari va ularning xavfsizligini ta'minlash darajasidagi farqlar (“raqamli bo'linish”);

4) xavfsiz va tez tiklanadigan axborot infratuzilmasini shakllantirishdagi milliy qonunchilik va amaliyotdagi farqlar.

Xalqaro axborot xavfsizligini ta'minlashning asosiy tamoyillari

Axborot maydoni insonning umumiy mulkidir. Uning xavfsizligi jahon sivilizatsiyasining barqaror rivojlanishini ta’minlashning asosidir.

Axborot makonida ishonch muhitini yaratish va qo'llab-quvvatlash uchun ishtirokchi-davlatlar quyidagi tamoyillarga rioya qilishlari zarur:

1) har bir ishtirokchi davlatning axborot makonidagi faoliyati ijtimoiy va iqtisodiy rivojlanishga hissa qo'shishi va xalqaro tinchlik va xavfsizlikni saqlash vazifalariga mos keladigan, umume'tirof etilgan tamoyillar va normalarga mos keladigan tarzda amalga oshirilishi kerak. xalqaro huquq, shu jumladan nizo va nizolarni tinch yo‘l bilan hal etish, xalqaro munosabatlarda kuch ishlatmaslik, boshqa davlatlarning ichki ishlariga aralashmaslik, davlatlarning suverenitetini, insonning asosiy huquq va erkinliklarini hurmat qilish tamoyillari;

2) ishtirokchi davlatlar xalqaro axborot xavfsizligi tizimini shakllantirish jarayonida xavfsizlikning ajralmasligi tamoyiliga amal qiladilar, ya'ni ularning har birining xavfsizligi barcha boshqa davlatlar

va dunyo xavfsizligi bilan uzviy bog'liqdir. butun jamiyatni himoya qiladi va o'z xavfsizligini boshqa davlatlar xavfsizligiga zarar etkazadigan tarzda mustahkamlamaydi;

3) har bir ishtirokchi davlat milliy axborot tizimlarini zamonaviy axborot-kommunikatsiya texnologiyalari bilan jihozlash darajasidagi farqlarni bartaraf etishga, axborot makonidagi tahdidlarning umumiy darajasini pasaytirish maqsadida “raqamli tafovut”ni kamaytirishga intilishi kerak;

4) axborot makonidagi barcha ishtirokchi davlatlar suveren tenglikdan foydalanadilar, bir xil huquq va majburiyatlarga ega bo‘ladilar hamda iqtisodiy, ijtimoiy, siyosiy yoki boshqa farqlardan qat’i nazar, axborot makonining teng huquqli sub’ektlari hisoblanadilar;

5) har bir ishtirokchi davlat suveren normalarni belgilash va milliy qonunlarga muvofiq o'z axborot makonini boshqarish huquqiga ega. Suverenitet va qonunlar ishtirokchi-davlat hududida joylashgan yoki uning yurisdiktsiyasiga boshqa tarzda tegishli bo'lgan axborot infratuzilmasiga nisbatan qo'llaniladi. A'zo davlatlar milliy qonunchilikni uyg'unlashtirishga intilishi kerak, ulardagi farqlar ishonchli va xavfsiz axborot muhitini shakllantirishga to'siqlar yaratmasligi kerak;

6) har bir ishtirokchi davlat o'z axborot makoniga, shu jumladan uning xavfsizligi va unda joylashtirilgan ma'lumotlarning mazmuni uchun javobgarlik tamoyiliga amal qilishi kerak;

7) har bir ishtirokchi davlat o'zining axborot makonini tashqi aralashuvsiz erkin rivojlantirish huquqiga ega va har bir boshqa davlat Birlashgan Millatlar Tashkiloti Nizomida mustahkamlangan xalqlarning teng huquqliligi va o'z taqdirini o'zi belgilashi tamoyiliga muvofiq ushbu huquqni hurmat qilishi shart;

8) har bir ishtirokchi davlat boshqa davlatlarning qonuniy xavfsizlik manfaatlarini hisobga olgan holda, suveren tenglik asosida axborot xavfsizligini ta'minlashda o'z manfaatlarini erkin va mustaqil ravishda belgilashi, shuningdek, o'z axborot xavfsizligini ta'minlash usullarini erkin tanlashi mumkin;

9) ishtirokchi davlatlar tajovuzkor “axborot urushi” xalqaro tinchlik va xavfsizlikka qarshi jinoyat ekanligini tan oladilar;

10) ishtirokchi davlatning axborot maydoni tahdid qilish yoki kuch ishlatish natijasida boshqa davlat tomonidan egallash ob'ekti bo'lmasligi kerak;

11) har bir ishtirokchi davlat, agar tajovuz manbai ishonchli tarzda aniqlangan va javob choralari adekvat bo‘lsa, o‘ziga qarshi axborot

makonida tajovuzkor harakatlar sodir bo‘lgan taqdirda o‘zini-o‘zi himoya qilishning ajralmas huquqiga ega;

12) har bir ishtirokchi davlat boshqa davlatlarning qonuniy xavfsizlik manfaatlarini, shuningdek, xalqaro tinchlik va xavfsizlikka ko‘maklashish zaruriyatini hisobga olgan holda milliy tartiblar asosida axborot makonida o‘zining harbiy salohiyatini belgilaydi. Ishtirokchi davlatlarning hech biri axborot makonida boshqa davlatlar ustidan ustunlikka erishishga harakat qilmaydi;

13) ishtirokchi davlat muzokaralar davomida ixtiyoriy asosda, shuningdek xalqaro huquq normalariga muvofiq ishlab chiqilgan kelishuvga muvofiq boshqa davlat hududida axborot xavfsizligini ta’minlash bo‘yicha o‘z kuchlari va vositalarini joylashtirishi mumkin;

14) har bir ishtirokchi-davlat transport, moliyaviy oqimlarni, aloqa vositalarini, xalqaro axborot vositalarini, shu jumladan ilmiy va ta’lim almashinuvini boshqarish bo‘yicha xalqaro axborot tizimlari faoliyatiga aralashmaslikni ta’minlash uchun zarur choralarni ko‘radi. umuman axborot makoniga salbiy ta'sir ko'rsatishi mumkin;

15) ishtirokchi davlatlar axborot makonini rivojlantirish sohasidagi ilmiy va texnologik ishlanmalarni, shuningdek, kiberxavfsizlikning global madaniyatini shakllantirishga qaratilgan ta’lim va ta’lim faoliyatini qo‘llab-quvvatlashi va rag‘batlantirishi kerak;

16) har bir ishtirokchi-davlat mavjud vositalar doirasida o‘z axborot makonida inson va fuqaroning asosiy huquq va erkinliklariga rioya etilishini, intellektual mulk huquqlariga, shu jumladan patentlar, texnologiyalar, tijorat sirlari, tovar belgilari va mualliflik huquqlariga rioya etilishini ta’minlaydi;

17) har bir ishtirokchi davlat so‘z erkinligini, axborot makonida fikr bildirishni, fuqarolarning shaxsiy hayotiga qonunga xilof ravishda aralashishdan himoya qilishni kafolatlaydi;

18) har bir ishtirokchi davlat asosiy erkinliklar va axborot makonidan terroristik foydalanishga samarali qarshi kurash o'rtasidagi muvozanatni saqlashga intiladi;

19) a'zo davlatlar fuqarolarning axborot makoniga kirishini cheklash yoki buzish huquqiga ega emas, milliy va jamoat xavfsizligini himoya qilish, shuningdek, milliy axborot infratuzilmasidan noto'g'ri foydalanish va ruxsatsiz aralashuvni oldini olish maqsadlari bundan mustasno;

20) ishtirokchi davlatlar axborot makonida biznes va fuqarolik jamiyati sherikligini rag'batlantiradi;

21) ishtirokchi davlatlar o'z fuqarolari, jamoat va davlat organlari,

boshqa davlatlar va jahon hamjamiyatining axborot makonidagi yangi tahdidlardan va ularning xavfsizligini yaxshilashning ma'lum usullaridan xabardor bo'lishini ta'minlash bo'yicha o'z majburiyatlarini tan oladilar.

Axborot makonida harbiy mojarolarning oldini olishning asosiy chora-tadbirlari. Ishtirokchi davlatlar axborot makonida yuzaga kelishi mumkin bo‘lgan nizolarni faol aniqlash, shuningdek, ularning oldini olish, inqiroz va nizolarni tinch yo‘l bilan hal etish bo‘yicha birgalikda sa’y-harakatlarni amalga oshirish choralarini ko‘rish majburiyatini oladi.

Shu maqsadda ishtirokchi davlatlar:

1) xalqaro tinchlik va xavfsizlikni saqlash, xalqaro iqtisodiy barqarorlik va taraqqiyotga, xalqlarning umumiy farovonligiga va kamsitishlardan xoli xalqaro hamkorlikka ko'maklashish maqsadida xalqaro axborot xavfsizligini ta'minlash sohasida bir-birlari bilan hamkorlik qilish majburiyatini oladilar;

2) o'z hududidan yoki o'z yurisdiktsiyasidagi axborot infratuzilmasidan foydalangan holda axborotning buzg'unchi ta'sirini oldini olish uchun barcha zarur choralarni ko'radi, shuningdek, o'z hududidan foydalangan holda amalga oshirilgan kompyuter hujumlari manbasini aniqlash, ushbu hujumlarga qarshi turish va oqibatlarini bartaraf etish bo'yicha hamkorlik qilish majburiyatini oladi;

3) axborot makonida tahdidlarning kuchayishiga, shuningdek, davlatlar o‘rtasidagi munosabatlarning keskinlashuviga va “axborot urushlari”ning paydo bo‘lishiga olib kelishi mumkin bo‘lgan rejalar, doktrinalarni ishlab chiqish va qabul qilishdan tiyiladi;

4) boshqa davlatning axborot makonining yaxlitligini to‘liq yoki qisman buzishga qaratilgan har qanday harakatlardan o‘zini tutadi;

5) boshqa davlatning ichki vakolatiga kiruvchi masalalarga aralashish uchun axborot-kommunikatsiya texnologiyalaridan foydalanmaslik majburiyatini oladi;

6) xalqaro munosabatlarda har qanday boshqa davlatning axborot makonini buzish maqsadida yoki nizolarni hal qilish vositasi sifatida unga qarshi kuch ishlatish bilan tahdid qilishdan yoki kuch ishlatishdan tiyiladi;

7) boshqa davlatning axborot makonida noqonuniy xatti-harakatlarni amalga oshirish uchun har qanday tartibsiz kuchlarni tashkil etish yoki ularni tashkil etishga undashdan tiyilish majburiyatini oladi;

8) boshqa davlatlarning ichki ishlariga aralashish yoki aralashish maqsadida tuhmatli bayonotlardan, shuningdek haqoratomuz yoki dushmanona tashviqotdan tiyilish majburiyatini oladi;

9) boshqa davlatlarning ichki ishlariga aralashish yoki xalqaro

tinchlik va xavfsizlikka zarar etkazuvchi, deb baholanishi mumkin bo'lgan yolg'on yoki buzib ko'rsatilgan xabarlarning tarqalishiga qarshi kurashish huquqiga ega va majburiyatini oladi;

10) “axborot qurollari” va ularni yaratish texnologiyalari tarqalishini cheklash choralarini koʻradi.

Axborot makonidagi harbiy mojarolarni hal qilishga qaratilgan chora-tadbirlar:

1) Ishtirokchi davlatlar axborot makonidagi nizolarni birinchi navbatda muzokaralar, surishtiruvlar, vositachilik, yarashtirish, arbitraj, sud muhokamasi, mintaqaviy organlarga yoki kelishuvlarga murojaat qilish yoki xalqaro tinchlik va xavfsizlikka xavf tug'dirmaydigan boshqa tinch yo'l bilan hal qiladilar.

2) Har qanday xalqaro nizo yuzaga kelgan taqdirda, nizoda ishtirok etuvchi davlatlarning “axborot urushi” olib borish usullari yoki vositalarini tanlash huquqi amaldagi xalqaro gumanitar huquq qoidalari bilan cheklanadi.

Axborot makonidan terroristik maqsadlarda foydalanishga qarshi kurashish maqsadida ishtirokchi davlatlar:

1) axborot makonidan terroristik maqsadlarda foydalanishga qarshi choralar ko'rish va buning uchun birgalikda hal qiluvchi harakatlar zarurligini tan olish;

2) terroristik xarakterdagi internet-resurslar faoliyatini toʻxtatish boʻyicha umumiy yondashuvlarni ishlab chiqishga intiladi;

3) kompyuterga hujum qilish tahdidlari, internetdan terroristik maqsadlarda foydalanish belgilari, faktlari, usullari va vositalari, terroristik tashkilotlarning axborot makonidagi intilishlari va faoliyati to'g'risida ma'lumot almashishni yo'lga qo'yish va kengaytirish zarurligini tushunadi. , shuningdek, internet tarmogʻidagi axborot resurslarini monitoring qilish, terroristik saytlar tarkibini qidirish va kuzatish, ushbu sohada sud-kompyuter ekspertizasini oʻtkazish, axborot makonidan foydalanishga qarshi kurashish boʻyicha faoliyatni huquqiy tartibga solish va tashkil etish boʻyicha tajriba va ilgʻor tajriba almashish. terroristik maqsadlar;

4) vakolatli organlarga axborot makonida terrorchilik harakatlarining oldini olish, bostirish va oqibatlarini bartaraf etishga qaratilgan tergov, qidiruv va boshqa protsessual tadbirlarni amalga oshirish, shuningdek aybdorlarni jazolash uchun zarur bo'lgan qonun hujjatlari va boshqa choralarni ko'radi. ular uchun jismoniy shaxslar va tashkilotlar;

5) ishtirokchi-davlat hududiga axborot-kommunikatsiya infratuzilmasining ayrim qismlariga huquqiy kirishni kafolatlovchi zarur qonunchilik va boshqa chora-tadbirlarni ko'radi, ularga nisbatan ulardan terrorchilik faoliyatini amalga oshirish yoki ularni amalga oshirish uchun foydalaniladi, deb hisoblash uchun qonuniy asoslar mavjud. axborot makonida yoki ulardan foydalanish bilan terroristik harakatlar yoki terroristik tashkilotlar, guruhlar yoki alohida terrorchilarning faoliyatini amalga oshirishga yordam beradigan faoliyat.

Xalqaro axborot xavfsizligi sohasida xalqaro hamkorlik

Ishtirokchi davlatlar ixtiyoriylik va o‘zarolik asosida axborot makonidan foydalangan holda jinoiy harakatlar, shu jumladan terroristik maqsadlardagi harakatlar oqibatlarini oldini olish, huquqiy tergov qilish va bartaraf etish bo‘yicha ishda ilg‘or tajriba almashadilar. Ayirboshlash ham ikki tomonlama, ham ko'p tomonlama asosda amalga oshirilishi mumkin. Axborotni taqdim etuvchi ishtirokchi davlat maxfiylik talablarini belgilashda erkindir. Bunday ma'lumotni olgan ishtirokchi davlat o'zaro yordam masalalarini muhokama qilishda uni taqdim etuvchi ishtirokchi davlat bilan munosabatlarida argument sifatida ishlatishi mumkin.

Har bir ishtirokchi davlat axborot makonidan harbiy foydalanish sohasida ishonchni mustahkamlash choralarini yaratishga intilishi kerak, jumladan:

1) axborot makonida xavfsizlikni ta'minlash bo'yicha milliy konsepsiyalar almashinuvi;

2) axborot makonidagi inqirozli hodisalar va tahdidlar hamda ularni bartaraf etish va zararsizlantirish bo'yicha ko'rilayotgan chora-tadbirlar to'g'risida tezkor ma'lumot almashish;

3) ishtirokchi davlatlarni tashvishga solishi mumkin bo'lgan axborot makonidagi faoliyat bo'yicha maslahatlashuvlar va harbiy xarakterdagi nizoli vaziyatlarni hal qilish bo'yicha hamkorlik.

Rossiya Federatsiyasining 2020 yilgacha bo'lgan davrda xalqaro axborot xavfsizligi sohasidagi davlat siyosatining asoslari.

Rossiya Federatsiyasi Prezidenti V. Putin tomonidan 2013 yil 24 iyulda PQ-1753-son bilan tasdiqlangan.

Xalqaro axborot xavfsizligi sohasidagi asosiy tahdidlarni, Rossiya Federatsiyasining xalqaro axborot xavfsizligi sohasidagi davlat siyosatining maqsadi, vazifalari va ustuvor yo'nalishlarini, shuningdek ularni himoya qilish mexanizmlarini belgilaydigan Rossiya Federatsiyasining strategik rejalashtirish hujjatini amalga oshirish.

Ushbu asoslar mo'ljallangan:

a) xalqaro axborot xavfsizligi tizimini shakllantirish, shu jumladan uni huquqiy, tashkiliy va boshqa qo'llab-quvvatlash turlarini takomillashtirish sohasidagi Rossiya tashabbuslarini xalqaro maydonda ilgari surish;

b) amalga oshirishda Rossiya Federatsiyasi ishtirok etadigan xalqaro axborot xavfsizligi sohasida davlatlararo maqsadli dasturlarni, shuningdek ushbu sohadagi davlat va federal maqsadli dasturlarni shakllantirish uchun;

v) xalqaro axborot xavfsizligi sohasida Rossiya Federatsiyasining davlat siyosatini amalga oshirishda idoralararo hamkorlikni tashkil etish;

d) iqtisodiyotning real sektorida axborot-kommunikatsiya texnologiyalaridan kengroq foydalanish orqali yetakchi jahon davlatlari bilan texnologik tenglikka erishish va uni saqlab qolish.

Xalqaro axborot xavfsizligi deganda tushuniladi - global axborot makonining shunday holati, unda shaxs, jamiyat va davlatning axborot sohasidagi huquqlarini buzish, shuningdek milliy muhim axborot infratuzilmasi elementlariga buzg'unchi va noqonuniy ta'sir ko'rsatish imkoniyati mavjud. istisno qilingan.

Xalqaro axborot xavfsizligi tizimi ostida global axborot makonining turli sub'ektlari faoliyatini tartibga solishga mo'ljallangan xalqaro va milliy institutlar majmuini nazarda tutadi.

Xalqaro axborot xavfsizligi tizimi strategik barqarorlikka tahdidlarga qarshi turish va global axborot makonida teng huquqli strategik sheriklikni rivojlantirishga qaratilgan.

Xalqaro axborot xavfsizligi sohasidagi asosiy tahdid axborot-kommunikatsiya texnologiyalaridan foydalanish hisoblanadi:

a) xalqaro huquqqa zid bo‘lgan harbiy-siyosiy maqsadlarda axborot quroli sifatida suverenitetni obro‘sizlantirishga, davlatlarning hududiy yaxlitligini buzishga, xalqaro tinchlik, xavfsizlik va strategik barqarorlikka tahdid soladigan dushmanona harakatlar va bosqinchilik harakatlarini amalga oshirish;

b) terroristik maqsadlarda, shu jumladan muhim axborot infratuzilmasi elementlariga buzg'unchi ta'sir ko'rsatish, shuningdek terrorizmni targ'ib qilish va terrorchilik faoliyatiga yangi tarafdorlarni jalb qilish;

v) suveren davlatlarning ichki ishlariga aralashish, jamoat tartibini buzish, etnik, irqiy va konfessiyalararo adovatni qo'zg'atish, nafrat va kamsitishni keltirib chiqaradigan irqchilik va ksenofobiya g'oyalari yoki

nazariyalarini targ'ib qilish, zo'ravonlikni qo'zg'atish;

d) zararli kompyuter dasturlarini yaratish, ulardan foydalanish va tarqatish orqali jinoyatlarni, shu jumladan kompyuter ma'lumotlariga noqonuniy kirish bilan bog'liq jinoyatlarni sodir etish.

Rossiya Federatsiyasining davlat siyosatining maqsadi - xalqaro axborot xavfsizligi tizimini shakllantirish uchun shart-sharoitlar yaratishga qaratilgan xalqaro huquqiy rejimni o‘rnatishga ko‘maklashishdan iborat.

Rossiya Federatsiyasining davlat siyosati maqsadiga erishish Rossiya Federatsiyasining quyidagi vazifalarni hal qilishda ishtirok etishi bilan yordam beradi:

a) ikki tomonlama, ko'p tomonlama, mintaqaviy va global darajadagi xalqaro axborot xavfsizligi tizimini shakllantirish;

b) suverenitetni obro'sizlantirishga, davlatlar hududiy yaxlitligini buzishga qaratilgan va xalqaro tinchlik, xavfsizlik va strategik barqarorlikka tahdid soladigan dushmanona harakatlar va tajovuzkorlik harakatlarini amalga oshirish uchun axborot-kommunikatsiya texnologiyalaridan foydalanish xavfini kamaytirish uchun shart-sharoitlar yaratish;

v) axborot-kommunikatsiya texnologiyalaridan terroristik maqsadlarda foydalanish tahdidlariga qarshi kurashish sohasida xalqaro hamkorlik mexanizmlarini shakllantirish;

d) axborot-kommunikatsiya texnologiyalaridan ekstremistik maqsadlarda, shu jumladan suveren davlatlarning ichki ishlariga aralashish maqsadida foydalanish tahdidlariga qarshi kurashish uchun shart-sharoitlar yaratish;

e) axborot-kommunikatsiya texnologiyalaridan foydalanish sohasida jinoyatchilikka qarshi kurashish sohasida xalqaro hamkorlik samaradorligini oshirish;

f) axborot-kommunikatsiya texnologiyalari sohasida davlatlarning texnologik suverenitetini ta'minlash va rivojlangan va rivojlanayotgan mamlakatlar o'rtasidagi axborot tafovutini bartaraf etish uchun shart-sharoitlar yaratish.

Ikki tomonlama, ko'p tomonlama, mintaqaviy va global darajadagi xalqaro axborot xavfsizligi tizimini shakllantirish muammosini hal qilish bilan bog'liq Rossiya Federatsiyasi davlat siyosatining asosiy yo'nalishlari:

a) Birlashgan Millatlar Tashkilotiga a'zo davlatlar tomonidan Xalqaro axborot xavfsizligini ta'minlash to'g'risidagi konventsiyani ishlab

chiqish va qabul qilish zaruratida Rossiya tashabbusini xalqaro maydonda ilgari surish uchun sharoit yaratish;

b) Birlashgan Millatlar Tashkilotining axborotlashtirish va telekommunikatsiyalar sohasidagi yutuqlar bo'yicha hukumat ekspertlar guruhining ishi natijasida chiqarilgan yakuniy hujjatlarda xalqaro axborot xavfsizligi tizimini shakllantirish sohasidagi Rossiya tashabbuslarini ta'minlashga ko'maklashish. Xalqaro xavfsizlik, shuningdek, Rossiya Federatsiyasining milliy manfaatlariga javob beradigan xalqaro axborot xavfsizligini ta'minlash sohasida Birlashgan Millatlar Tashkiloti shafeligida xulq-atvor qoidalarini ishlab chiqishda yordam berish;

v) muntazam ravishda ikki tomonlama va ko‘p tomonlama ekspert maslahatlashuvlarini o‘tkazish, Shanxay hamkorlik tashkilotiga a’zo davlatlar, Mustaqil Davlatlar Hamdo‘stligiga a’zo davlatlar, Kollektiv Xavfsizlik Shartnomasi Tashkilotiga a’zo davlatlar, BRICSga a’zo davlatlar bilan pozitsiyalar va harakatlar rejalarini muvofiqlashtirish. a’zo davlatlar, Osiyo-Tinch okeani iqtisodiy hamkorligi mamlakatlari, “Sakkizlik guruhi”, “Yigirmalik guruhi”ga a’zo davlatlar, xalqaro axborot xavfsizligi sohasidagi boshqa davlatlar va xalqaro tuzilmalar;

d) “Internet” axborot-telekommunikatsiya tarmog'ini boshqarishni xalqarolashtirish bo'yicha Rossiya tashabbusini xalqaro maydonda ilgari surish va bu kontekstda Xalqaro elektraloqa ittifoqining rolini oshirish;

e) Rossiya Federatsiyasining davlat siyosatini amalga oshirishda ishtirok etuvchi federal ijro etuvchi hokimiyat organlarining tarkibiy bo'linmalarini tashkiliy va kadrlar bilan mustahkamlash, shuningdek, ushbu sohadagi federal ijro etuvchi hokimiyat organlari faoliyatini muvofiqlashtirishni takomillashtirish;

f) xalqaro axborot xavfsizligi tizimini shakllantirish sohasidagi Rossiya tashabbuslarini ilgari surish uchun tahliliy, ilmiy va uslubiy yordamni takomillashtirishda Rossiya ekspert hamjamiyatining ishtiroki mexanizmini yaratish;

g) Rossiya Federatsiyasi va xorijiy davlatlar o'rtasida xalqaro axborot xavfsizligini ta'minlash sohasida hamkorlik to'g'risida xalqaro shartnomalar tuzish uchun shart-sharoitlar yaratish;

h) Shanxay hamkorlik tashkilotiga a’zo davlatlar hukumatlari o‘rtasidagi xalqaro axborot xavfsizligini ta’minlash sohasidagi hamkorlik to‘g‘risidagi Bitim doirasida o‘zaro hamkorlikni kuchaytirish va mazkur Bitimga a’zolik doirasini kengaytirishga ko‘maklashish;

i) xalqaro axborot xavfsizligi tizimini shakllantirish sohasidagi Rossiya tashabbuslarini ilgari surish uchun Birlashgan Millatlar

Tashkiloti va boshqa xalqaro tashkilotlarning ilmiy, tadqiqot va ekspert salohiyatidan foydalanish.

Rossiya Federatsiyasining axborot xavfsizligi sohasidagi ilmiy tadqiqotlarning asosiy yo'nalishlari:

Rossiya Federatsiyasi Xavfsizlik Kengashi kotibi N.P. tomonidan tasdiqlangan. Patrushev 2017 yil 31 avgust

Rossiya Federatsiyasining axborot xavfsizligini ta'minlashning umumiy ilmiy muammolari:

1 Axborot xavfsizligini ta'minlashning umumiy uslubiy muammolari:

1.1. Axborot xavfsizligi sohasida kontseptual (terminologik) apparatni shakllantirish muammolari.

1.2. Jamiyat hayotida tizim tuzuvchi omil sifatida axborot sohasini rivojlantirish muammolari.

1.3. Shaxs, jamiyat, davlat va xalqaro hamjamiyatning axborot xavfsizligiga tahdid va tahdidlarga qarshi kurashish muammolari.

1.4. Rossiya Federatsiyasining axborot xavfsizligi tizimini rivojlantirish muammolari.

1.5. Hozirgi bosqichda Rossiyaning raqobatbardoshligiga axborot sohasining ta'siri muammolari.

1.6. Shaxs, jamiyat va davlatning axborot xavfsizligini baholash muammolari.

1.8. Ko'p millatli rus xalqining ma'naviy va axloqiy qadriyatlarini saqlash muammolari.

1.9. Axborot xavfsizligiga tahdidlarni aniqlash, aniqlash, tasniflash, baholash muammolari.

2. Axborot xavfsizligini me'yoriy-huquqiy va normativ-texnik ta'minlashni rivojlantirish muammolari

3. Shaxsiy, guruh va ommaviy ong xavfsizligini ta'minlash muammolari:

3.1. Shaxs, jamiyat va davlatning buzg'unchi axborot ta'siridan xavfsizligini ta'minlash muammolari.

3.3. Rossiya fuqarolariga axborot ta'siriga qarshi kurashish muammolari, shu jumladan Vatan himoyasi bilan bog'liq tarixiy asoslar va vatanparvarlik an'analarini buzishga qaratilgan muammolar.

3.4. Terrorizmni targ'ib qilish uchun axborot texnologiyalaridan foydalanishga qarshi kurashish, terrorchilik faoliyatiga yangi tarafdorlarni jalb qilish, terrorchilik faoliyatini rejalashtirish va tashkil etish muammolari.

4. Axborot texnologiyalaridan jinoiy maqsadlarda foydalanishga qarshi kurashish muammolari.

5. Axborot texnologiyalaridan tajovuzkor va boshqa dushmanona foydalanish natijasida yuzaga kelishi mumkin bo'lgan harbiy mojarolarni to'xtatish va oldini olish muammolari.

Rossiya Federatsiyasining axborot xavfsizligini ta'minlashning ilmiy-texnik muammolari:

— zamonaviy axborot texnologiyalari, mahalliy sanoatning axborotlashtirish, telekommunikatsiya va aloqa vositalarini rivojlantirishning ilmiy-texnik muammolari;

— axborot resurslari, axborot tizimlari va aloqa tarmoqlarini muhofaza qilishning ilmiy-texnik muammolari;

— tezkor-qidiruv faoliyatida axborot texnologiyalaridan foydalanishning ilmiy-texnik muammolari;

— Rossiya Federatsiyasining kadrlar axborot xavfsizligi muammolari;

— xalqaro axborot xavfsizligi tizimini shakllantirish muammolari;

— davlat suverenitetini obro‘sizlantirishga, davlatlarning hududiy yaxlitligini buzishga, xalqaro tinchlik, xavfsizlik va strategik barqarorlikka tahdid soladigan dushmanona harakatlar va tajovuzkorlik harakatlarini amalga oshirishda axborot-kommunikatsiya texnologiyalaridan foydalanish xavfini kamaytirish muammolari.

1. “Axborot qurollarini” tarqatmaslikning xalqaro huquqiy rejimini o'rnatish, ulardan foydalanish xavfini kamaytirish muammolari.

2. Xalqaro huquq tizimida ochiqlikning maqbul darajasini ta'minlaydigan dushmanona harakatlar va bosqinchilik harakatlarini amalga oshirish uchun axborot-kommunikatsiya texnologiyalaridan foydalanish tahdidlariga qarshi kurashish sohasida “ishonchni mustahkamlash choralari” universal institutini shakllantirish muammolari.

3. “Axborot qurollari” yordamida davlatlararo nizolarni to'xtatish va oldini olish bo'yicha xalqaro huquqni moslashtirish va rivojlantirish muammolari.

4. Axborot-kommunikatsiya texnologiyalaridan dushmanona foydalanishni kvalifikatsiya qilish muammolari va xalqaro axborot xavfsizligi sohasidagi tahdidlarni monitoring qilishning davlatlararo tizimi modellari.

5. Axborot-kommunikatsiya texnologiyalaridan terroristik

maqsadlarda foydalanishga qarshi kurashish muammolari.

6. Transchegaraviy muhim axborot infratuzilmalarining axborot xavfsizligini ta'minlash muammolari.

7. “Internet” axborot-telekommunikatsiya tarmog'ining xavfsiz va barqaror ishlashi masalalarini hal qilishda davlatlarning teng ishtirokini ta'minlash muammolari.

8. Global axborot infratuzilmasidan ekstremistik maqsadlarda foydalanishga, shu jumladan suveren davlatlarning ichki ishlariga aralashishga qarshi chora-tadbirlarning davlatlararo tizimini shakllantirish va amalga oshirish muammolari.

9. Ekstremistik maqsadlarda, shu jumladan, suveren davlatlarning ichki ishlariga aralashish maqsadida axborot-kommunikatsiya texnologiyalaridan foydalanishning oldini olish ustidan doimiy nazoratni amalga oshirishning xalqaro mexanizmini yaratish muammolari.

10. Internet-axborot-telekommunikatsiya tarmog'ining barqaror va xavfsiz ishlashiga tahdid soladigan harakatlarni anonimlashtirish, har bir shaxsning barcha turdagi axborot va g'oyalarni izlash, olish va tarqatish huquq va erkinliklarini hurmat qilish bo'yicha chora-tadbirlar muvozanatini ta'minlash muammolari , ushbu huquq va erkinliklardan foydalanishda alohida majburiyatlar va alohida javobgarlik, shuningdek, boshqa shaxslarning huquqlari va obro‘-e’tiborini hurmat qilish hamda milliy xavfsizlik, jamoat tartibi, aholi salomatligi va ma’naviyatini ta’minlash uchun zarur bo‘lgan ularni qonuniy cheklash imkoniyatini hisobga olgan holda. .

11. Axborot-kommunikatsiya texnologiyalaridan foydalanish sohasida jinoyatchilikka qarshi kurashish sohasidagi muammolar.

12. Xalqaro axborot xavfsizligi tizimini shakllantirish sohasidagi Rossiya tashabbuslarini ilgari surish uchun tahliliy va ilmiy-uslubiy yordamni takomillashtirish muammolari.

13. Prognoz qilinadigan texnologik innovatsiyalarni joriy etishda xalqaro axborot xavfsizligi sohasida yangi tahdidlarni aniqlash muammolari.

14. Axborot-kommunikatsiya texnologiyalari sohasida davlatlarning texnologik suverenitetini himoya qilish va rivojlangan va rivojlanayotgan mamlakatlar o'rtasidagi axborot tafovutini bartaraf etish bo'yicha chora-tadbirlar muvozanatini ta'minlash muammolari.

15. Davlatlarning huquqni muhofaza qilish organlarining axborot-kommunikatsiya texnologiyalaridan foydalanish sohasida jinoyatchilikka qarshi kurashish sohasida xalqaro hamkorligini takomillashtirish

muammolari, shu jumladan jinoyatlarni tergov qilish jarayonida davlatlar huquqni muhofaza qilish organlari o‘rtasida axborot almashinuvi samaradorligini oshirish masalalari. axborot-kommunikatsiya texnologiyalaridan foydalanish sohasida, shuningdek, ushbu toifadagi jinoyatlarga oid ishlarni ko‘rishning tergov va sud amaliyoti usullari to‘g‘risida axborot almashish mexanizmini takomillashtirish.

Axborot xavfsizligi muammolari: rivojlanish alogizmlari. 1990-yillarning boshlarida, siyosatshunoslik asarlarida “axborot xavfsizligi” atamasi endigina paydo bo‘la boshlaganida, u belgilagan munosabatlar sohasi axborot urushining antitezasi sifatida tushunilgan edi. Bundan tashqari, axborot urushining o'zi o'sha paytda faqat davlatlararo kuch qarama-qarshiligi uslubida aniqlangan. Nodavlat sub'ektlar ham mojaro ishtirokchilari bo'lishi mumkinligi istisno qilinmadi, lekin ular odatda hokimiyat uchun qurolli kurashda qarama-qarshi bo'lgan ichki siyosiy kuchlar sifatida tushunildi. Keyin bunday qarama-qarshiliklar “urush bilan bog'liq bo'lmagan nizolar” deb ataldi, ko'pincha fuqarolar urushlari, milliy mustaqillik va muxtoriyat uchun kurash va shunga o'xshashlarni nazarda tutadi.

O'sha paytda faqat AQSh axborot tahdidiga qarshi kurashning faol himoyachisi edi. Harbiy axborot operatsiyalari sohasidagi birinchi ishlanmalar AQShda ham amalga oshirildi, u erda 1993 yildan boshlab har xil turdagi harbiy nizomlar, ko'rsatmalar va axborot operatsiyalarini o'tkazish doktrinalari tayyorlana boshladi.

1998 yilda Birlashgan shtab boshliqlari “Axborot operatsiyalarining qo'shma doktrinasi” deb nomlangan fundamental asarni nashr etdi, unda axborot urushi amaliy mavzu tavsifini oldi. O'sha paytda ma'lum sabablarga ko'ra, axborot makonida faol qarama-qarshilik uchun Internet va ijtimoiy tarmoqlarning ahamiyati haqida hech kim o'ylamagan, ammo psixologik operatsiyalar, ham taktik, ham strategik, axborot sohasiga bevosita bog'liq edi. Shunga qaramay, oradan yillar o'tib, 2004 yilda AQShning BMTning Xalqaro axborot xavfsizligi bo'yicha hukumat ekspertlar guruhidagi vakili axborot urushi xavfi yo'qligini, axborot urushining o'zi esa ximeradan boshqa narsa emasligini ta'kidladi. Vashington nuqtai nazaridan, kiberjinoyatni asosiy tahdid deb hisoblash kerak edi. Va shunga qaramay, rangli inqiloblardan keyin,

O'shandan beri ko'plab davlatlar va xalqaro tashkilotlar axborot xavfsizligi muammosi bilan shug'ullana boshladilar. Ayni paytda BMTning Xalqaro axborot xavfsizligi bo‘yicha hukumat ekspertlarining to‘rtinchi guruhi o‘z ishini yakunladi.

1998 yildan beri Birlashgan Millatlar Tashkiloti Bosh Assambleyasi har yili o'zining har bir sessiyasida deyarli har doim konsensus asosida ushbu muammoga bevosita bag'ishlangan “Xalqaro xavfsizlik kontekstida aloqa va axborotlashtirish sohasidagi yutuqlar” rezolyutsiyasini qabul qiladi. Bundan tashqari, ushbu rezolyutsiya xalqaro xavfsizlik masalalari bo'yicha birinchi qo'mita tomonidan qabul qilinadi. Uchinchi qo'mita uch yil davomida “Kiberxavfsizlik madaniyati” rezolyutsiyasini ilgari surmoqda.

Axborot xavfsizligi va axborot jamiyati masalalari kun tartibida doimiy o'rin egalladi. Xalqaro elektraloqa ittifoqi (XEI), uning homiyligida 2003 va 2005 yillarda ikki bosqichda. axborot xavfsizligi sohasidagi eng yirik zamonaviy forum – Axborot jamiyati bo‘yicha Butunjahon sammiti bo‘lib o‘tdi.

Axborot xavfsizligi va kiberxavfsizlik masalalari ana shunday xalqaro tashkilotlar uchun eng muhimlar ro'yxatidan joy olgan. ShHT, BRIKS, Yevropada Xavfsizlik va Hamkorlik Tashkiloti (EXHT), Janubi-Sharqiy Osiyo davlatlari assotsiatsiyasining Mintaqaviy xavfsizlik forumi (ARF) kabi. NATO va Kollektiv Xavfsizlik Shartnomasi Tashkiloti (ODKB) ushbu muammoning harbiy jihatlari ustida faol ishlamoqda. Terrorizmga qarshi kurash uzoq vaqtdan beri faqat internetdan tashviqot maqsadida foydalanish, yangi a’zolarni jalb qilish va terrorchilik hujumlarini uyushtirish bilan bog‘liq bo‘lgan. Kiberjinoyat masalalari asosiy ommaviy axborot vositalarining yetakchi maqolalarini tark etmaydi. Axborot xavfsizligi kun tartibiga tematik jihatdan u yoki bu tarzda bog'langan konferentsiyalar, simpoziumlar, seminarlar, davra suhbatlari va boshqa tadbirlarning aniq sonini hech kim bilmaydi.

Axborot xavfsizligi muammolari Stuxnet, Duqu, Flame, Gauss kabi zararli dasturlarning turli xil dasturiy muhitlarda ishlashi, Internet orqali tarqalishi va turli xil, shu jumladan tanqidiy dasturlarni to'liq o'chirishgacha jiddiy jismoniy zarar etkazishi mumkinligi haqidagi xabarlardan so'ng yangilandi. va ayniqsa xavfli ishlab chiqarish, transport, energiya ob'ektlari. Muhim infratuzilmalarni boshqarish uchun axborot tizimlari nafaqat himoya ob'ekti, balki hujumlar nishoniga ham aylandi. Mutaxassislar bu tahdidni 20 yil avval oldindan ko‘rgan va amalga oshirgan, biroq jahon hamjamiyatiga unga qarshi kurashish uchun butun axborot makonini (nafaqat aloqa tarmoqlari hamda Internet kabi apparat-dasturiy mahsulotlar) milliy va xalqaro himoyada bo‘lishi zarurligini tushuntirib bera olmadi.

Asta-sekin siyosatshunoslar uchun ham, siyosatchilar uchun ham

postindustrial jamiyat nafaqat tinch atom, balki tinch axborot makoniga muhtoj ekanligi ayon bo'ladi. Yadro qurollarini tarqatmaslik to'g'risidagi shartnoma (NPT) harbiy yadro texnologiyasi tarixida burilish nuqtasi bo'ldi. Albatta, postindustrial jamiyatda shunga o'xshash kelishuvni tuzish qiyin, ammo axborot tahdidiga qarshi kurashish hali ham shunga o'xshash miqyos va chuqurlikdagi ko'p tomonlama sa'y-harakatlarni talab qiladi. Agar buni amalga oshirish mumkin bo'lsa, insoniyat xalqaro munosabatlarda zo'ravonlikning befoydaligini anglab etganini aytish mumkin bo'ladi.

Ammo bugungi kunda hamma ham bunday vazifaning mohiyatini va shakllantirishni bir xil tushunmaydi. Bugungi kunda xalqaro axborot xavfsizligini ta'minlash bo'yicha umumiy nutqda ma'lum darajada an'anaviylik bilan liberal, konservativ va pragmatik deb ta'riflanishi mumkin bo'lgan uchta yo'nalish aniq belgilab qo'yilgan.

1) Liberallar. Ularni “Internet erkinligi himoyachilari” deb ham atash mumkin. Bugungi kunda axborot xavfsizligi masalalari bilan qiziquvchilarning aksariyati ushbu keng guruhga kiradi.

Liberallarning katta qismini yoshlar tashkil qiladi. Endi planshetlar paydo bo‘lishi bilan ularning ko‘pchiligi uchun hatto klaviaturadan foydalanish ham intellektual qiyinchilikka aylandi – barmog‘ingizni ekran bo‘ylab suring, xat yozish o‘rniga xuddi shu gadjetlar yordamida olingan suratlarni baham ko‘rishingiz mumkin. Bu guruh axborot almashish va unga kirishni shunday ko'radi.

Ushbu guruhning ikkinchi katta qismi - faol Internet foydalanuvchilari, ular o'zlarining asosiy mashg'ulotlarining tabiati bo'yicha muhim infratuzilmalar, armiya, xavfsizlik va huquqni muhofaza qilish organlari faoliyati, davlat sirlarini ifodalovchi masalalar - va umuman olganda davlatning faoliyati va xavfsizligi masalalari bilan. Albatta, bu guruh ham heterojendir, lekin bizning muammomiz nuqtai nazaridan uni bitta tezisga sodiqlik birlashtiradi - global tarmoq, birinchi navbatda, axborotdan foydalanish erkinligini va axborotni tarqatish erkinligini ta'minlashi kerak.

Internet erkinligi himoyachilari orasida xavfsizlikka faqat hech kim va hech narsa tomonidan mutlaq, cheklanmagan erkinlik orqali erishish mumkin, deb hisoblashadi. Biroq, liberal yondashuv tarafdorlari erkinlik va xavfsizlikni emas, balki Internetni amalda nazorat qiluvchi va undan foydalanadigan, bolalar pornografiyasi va terrorchilik xurujlarini amalga oshirish bo'yicha ko'rsatmalar, qurol-yarog' sotuvchilari va eng xavfli narsalarni tarqatadiganlarning buyrug'i, siyosiy va moliyaviy

manfaatlarini himoya qiladi. tovarlar va xizmatlar.

Qiziq, kelajakda Internet bir necha global tarmoqlarga bo‘linganda ularning ritorikasi qanday o‘zgaradi – ularning erkinlik haqidagi tushunchalari bir-biri bilan raqobatlasha oladigan yangi tarmoqlar erkinligini o‘z ichiga oladimi? Savol shu tarzda qo'yilsa, javob aniq bo'lmaydi. Yana bir muqobil tarmoqning parchalanishi bo'lishi mumkin, bu bir mamlakatda nazariy jihatdan mahalliylashtirilgan alohida domenlar yoki ularning guruhlarining ko'plab ko'zgularini shakllantirishni o'z ichiga oladi.

2) Konservatorlar, qog'oz axborot tarafdorlari. Bular, ehtimol, 19-asr boshlari darajasida o'zlarining onglarini doimiy ravishda saqlab qolishga qaror qilishgan, xavfsiz ma'lumot almashinuvi tarafdori bo'lib, hujjatlarga kirishni cheklash imkoniyatini ta'minlaydilar. Biroq, tan olish kerakki, bugungi kunda ularning soni juda oz va u tobora kamayib bormoqda. G'alati, bu ma'lumotni tushunish - hujjat sifatida - Rossiyada ham, boshqa mamlakatlarda ham huquqiy normalarning asosiy qismini o'rnatadi.

Konservatorlar ham har doim ham nimani xohlashlarini bilishmaydi. Hech kim hujjat nima ekanligini aniqlay olmaydi - matnli qog'ozmi yoki boshqa narsami? Uning etarli belgisi, ro'yxatga olish raqami yoki matni nima? Lekin chizmalar va chizmalar haqida nima deyish mumkin? Va shunga o'xshash savollar juda ko'p: hujjatda bitta raqam bormi, matnda yoki hujjatdagi chizmada biron bir ma'no bor-yo'qligini qanday aniqlash mumkin va natijada aniq nimani saqlash kerak va nima bo'lishi kerak? hujjat bilan ishlaganda almashtiriladimi?

3) Pragmatistlar, axborotning mavjudligi va harakatining barcha shakllarini hisobga olish muhimligini tushunadiganlar va axborotni fundamental, immanent mavjudot toifalari bilan bog'laydiganlar. Dastlab, bu pozitsiyalarni harbiylar egallab, elektron urushni axborot vositalari, bombalar - elektr kalitlari, elektron jihozlarni yaroqsiz holga keltiradigan kimyoviy va biologik vositalar, psixotrop dorilar va boshqalar deb atashadi. Bu erda hal qiluvchi omil - axborotga, uni qayta ishlash tizimlariga, shu jumladan inson ongiga, shuningdek, uni uzatish va saqlash tizimlariga ta'sir qilish printsipi.

Bunday holda, ma'lumotlar ancha kengroq ta'riflanishi kerak. Xususan, bunday ma'lumotlar shaxsga bevosita bog'liq emasligini qabul qilish kerak. Axborot nafaqat miya faoliyatining semantik natijasi, unda hosil bo'lgan va mahalliylashtirilgan, balki har qanday o'zaro ta'sirning kommunikativ asosi sifatida ko'rib chiqilishi kerak. Keyin ma'lum

bo'ladiki, u moddiy va umuman olganda, ideal dunyoning barcha ob'ektlari bilan almashinadi, o'zaro ta'sir o'tkazishga qodir, u turli vaqtlarda uzatilishi va qabul qilinishi mumkin, bu hodisa bilan bog'liq bo'lishi shart emas, bu teologik bilish mumkin. Kompyuter tarmoqlari va aloqa tarmoqlaridagi ommaviy axborot vositalarida himoya qilinishi kerak bo'lgan ma'lumotlar mavjud.

Muammoga yondashuvlari bilan farq qiluvchi va uning turli tomonlarini birinchi o'ringa qo'yadigan uch yo'nalish chiziqli va izchil bo'lishi shart bo'lmagan bilishning tabiiy jarayonini aks ettiradi.

Birinchi yondashuv tarafdorlari. Internetni nazorat qilish huquqlarini birlashtirish yoki qayta taqsimlashga intilish, shu bilan birga ushbu huquqlarga egalik qilish bilan bog'liq katta moliyaviy oqimlarni saqlab qolish yoki qayta taqsimlash. Shuning uchun bu erda asosiy rolni ushbu bozorning eng yirik o'yinchilaridan biri bo'lgan XEI o'ynaydi. Shuning uchun, o'z manfaatlarini yashirmasdan, unga Internetni yaratgan, asosan uni nazorat qiladigan va, shubhasiz, unga bo'lgan tabiiy huquqlaridan voz kechishni istamaydigan Qo'shma Shtatlar qarshi.

Ikkinchi yondashuv saylovlarda bo'lgani kabi, o'z yo'lini taklif qilishdan ko'ra, muxolifatdan ovozlarni chalg'itishi mumkin bo'lgan eski va ehtimol o'lib borayotgan tendentsiyani ifodalaydi.

Uchinchi, pragmatik yondashuv tarafdorlari birinchi ikkitasiga qarshi turing. Axborot jamiyati bo‘yicha Butunjahon forumida deyarli barcha mamlakatlar vakillari internet boshqaruvini xalqarolashtirish yoqlab ovoz berdi va bu g‘oya Rossiya tomonidan emas, balki Yevropa Ittifoqi tomonidan ilgari surildi. Shu bilan birga, YeI vakillarini forumda hozir bo'lgan “katta aka” delegatsiyasi bilan bu masala bo'yicha to'g'ridan-to'g'ri mojaro to'xtatmadi.

Internet boshqaruvini xalqarolashtirish, albatta, yaxshi va ijobiy jarayon, lekin bu muammo emas. Axborot (nafaqat kiber) makon o'z-o'zidan zaif bo'lmasligi va shu bilan birga inson ijtimoiy faoliyatining boshqa sohalariga harbiy, terroristik yoki jinoiy (ajralmas triada) tahdidlarini amalga oshirish uchun manba yoki kanal bo'lmasligi kerak. Davlat esa axborot xavfsizligining kafolati bo'lishi va o'z hududidan yoki axborot makonidan amalga oshirilayotgan harakatlar uchun javobgar bo'lishi kerak. Bu, birinchi navbatda, axborot sohasidagi faol qarama-qarshilik, ya'ni harbiy harakatlar tahdidiga tegishli. Jamiyat nafaqat tashqi, balki ichki xavfsizlikni ta'minlash funktsiyasini ham davlatga topshirdi.

Axborot makoniga har qanday turdagi qoidalar, me’yorlar va

boshqa cheklovlarning kiritilishiga qarshi bo‘lganlar ko‘pincha inson huquqlariga, xususan, Inson huquqlari umumjahon deklaratsiyasining 19-moddasiga murojaat qiladilar, unda “Har kim fikr erkinligi huquqiga ega. va ifodalash; bu huquq har qanday ommaviy axborot vositalari orqali va davlat chegaralaridan qat'i nazar, o'z fikriga aralashish va izlash, olish va ma'lumot va g'oyalarni tarqatish erkinligini o'z ichiga oladi.

Shu bilan birga, xuddi shu Deklaratsiyaning oxirgidan oldingi 29-moddasida birining erkinligi boshqasining erkinligi boshlangan joyda tugashi “internetdagi inson huquqlari himoyachilari” ning bahs-munozaralaridan qutulib qolishini yaqqol ko‘rsatib turibdi. Xususan, maqolada cheklovchi emas, balki demokratik kontekstni tushunish uchun to'liq iqtibos keltirish kerak bo'lgan quyidagi qoidalar mavjud:

1. Har bir insonning jamiyat oldidagi majburiyatlari borki, bundagina uning shaxsi erkin va har tomonlama rivojlanishi mumkin.
2. Har kim o'z huquq va erkinliklarini amalga oshirishda faqat boshqa shaxslarning huquq va erkinliklari munosib tan olinishi va hurmat qilinishini ta'minlash, axloq, jamoat tartibining adolatli talablariga javob berish maqsadidagina qonunda belgilangan cheklashlarga duchor bo'ladi. va demokratik jamiyatdagi umumiy farovonlik.
3. Ushbu huquq va erkinliklarning amalga oshirilishi hech qanday holatda Birlashgan Millatlar Tashkilotining maqsad va tamoyillariga zid bo‘lmasligi kerak.

Bu erda biz quyidagi alogizmlarni ajratib ko'rsatishimiz mumkin.

Alogizm bir: harbiy komponent axborot xavfsizligi bo'yicha nutqni tark etdi. Bu bahsli emas, lekin ayni paytda uning mohiyati bo'yicha ko'rib chiqilmaydi. Uning oldini olish bo‘yicha chora-tadbirlarni qabul qilish o‘rniga ta’lim sohasida ishonchni mustahkamlash, kompyuter imkoniyatlarini oshirish, raqamli tafovutni kamaytirish va hokazolar muhokama qilinmoqda. Ehtimol, 1990-yillarning boshiga nisbatan muhimroq va dolzarbroq masalalar mavjud. Muammolar. Harbiy axborotni rivojlantirish sohasidagi kuchlarni joriy moslashtirishdagi status-kvoni saqlab qolish, axborot ta'sir vositalarini ishlab chiqarish va qabul qilish, Internet nazoratini xalqarolashtirish va oqimlarni nazorat qilish masalalarini kun tartibidan olib tashlash kerak. unga bog'langan pul, boshqariladigan “umumjahon tarmog'i” orqali ta'sir qilish imkoniyatini saqlab qolish. Ijtimoiy guruhlar, ommaviy axborot vositalari va ommaviy ongga, ularning g'oyalari va qadriyatlarini keng targ'ib qilish.

Harbiy axborot tahdidi muammosini ko'rib chiqishning barcha yondashuvlari orasida xalqaro gumanitar huquqning axborot makonidagi

nizolarga nisbatan qo'llanilishini muhokama qilish ajralib turadi**.** Rossiya har doim amaldagi qonun axborot operatsiyalariga taalluqli degan pozitsiyada bo'lib kelgan, ammo uni takomillashtirish kerak, chunki u axborot tahdidlari qonuniy yo'l bilan ko'rib chiqilmagan yillarda shakllangan. Bundan farqli o‘laroq, 1999-yilda chiqarilgan va 2000-yilda qayta nashr etilgan Pentagon hujjatida “hozirda xalqaro huquqda axborot operatsiyalariga hech qanday cheklovlar yo‘qligi” aniq ko‘rsatilgan.

2004 yil kuzida Stokgolmda NATO konferentsiyasida Rossiya delegatsiyasining taklifi bilan xuddi shu tezis Yevropa harbiy huquqshunoslari tomonidan ishonchli tarzda asoslab berildi. Ammo 2009 yilda, ikkinchi IIB GGE paytida, AQSh hukumati eksperti jus ad bellum tamoyillarini ta'kidlab, boshqacha yondashuvni eslatib o'tdi.jus ad bellum va jus in bello kibermakondagi mojarolarni hal qilish uchun juda maqbuldir.

Ikkinchi alogizm: Bugungi kunga qadar axborot xavfsizligi ikkiga bo'lingan: biznesning axborot xavfsizligi, madaniyatning axborot xavfsizligi va boshqalar paydo bo'ldi.

Axborot xavfsizligi brendga aylandi. Bu muammoning mohiyatidan chalg'itadi va axborot xavfsizligi haqidagi bilim illyuziyasini, noto'g'ri ma'noni yaratadi.

Alogizm uchinchi. Yuqorida ta’kidlanganidek, “axborot xavfsizligi kurashchilari”ning eng yirik armiyasi global tarmoq yangi internet madaniyatini shakllantirgan yangi dunyo degan g‘oyani qattiq himoya qilib, internet erkinligi tarafdori. Ammo bu dunyo fuqarolari kimlar? Ilg'or shaxs endi blogger bilan bog'lanadi, har bir o'zini hurmat qiladigan odam, shu jumladan prezident ham o'z blogiga ega, garchi besh yil oldin, eng yaxshisi, uning bosh sahifasi bo'lgan va bloglar haqida umuman hech kim bilmagan. . Butun dunyo internet va blogosferaga bog'langan degan g'oya shakllanmoqda. Biroq, jiddiy muhokamada, barcha axborot xavfsizligi mutaxassislari bir ovozdan muhim infratuzilmalarning hech birida Internet yo'qligini aytishadi - hatto jiddiy biznesda ham, mijoz bilan munosabatlar tugaydigan joyda tugaydi. Va Internet, umuman olganda,

Alogizm to'rtinchi shundan iboratki, hamma axborot xavfsizligini ta'minlashga harakat qiladi, lekin hech kim axborot nima ekanligini, qaerda va qanday mavjudligini tushunishga harakat qilmaydi. Masalan, “Yangi falsafiy ensiklopediya” nashrida “Axborot nazariyasi” maqolasiga havola bilan cheklangan. O'z navbatida, havola qilingan maqolada bu nazariya “maxsus ilmiy intizom, axborotni yig'ish, uzatish, qayta ishlash va saqlash jarayonlarining matematik jihatlarini tahlil qilish” ta'kidlanadi.

Bu kabi ma'lumotlar haqida bir so'z aytmaydi.

Xuddi shunday holat xorijda ham kuzatilmoqda. AQSH Mudofaa vazirligining elektron lug‘atida “axborot xavfsizligi”, “axborot hujumi”, “axborot operatsiyasi” va hokazo atamalar berilgan bo‘lsa-da, “axborot” atamasi mavjud emas.

Beshinchi alogizm. Demokratik hamjamiyat tushunchasida axborot xavfsizligi ko'pincha axborotdan foydalanish va uni tarqatish erkinligining antipodi ifodasi sifatida qabul qilinadi. Ammo shuni unutmaslik kerakki, har qanday jamiyat a’zolari shu jamiyat tomonidan ishlab chiqilgan huquq tizimi doirasida harakat qila boshlagandagina tashkilotga aylanadi. Tashkilotning asosi har doim xulq-atvor normalari va ularni ongli ravishda idrok etishdir. Axborot xavfsizligi masalasida, ayniqsa uning xalqaro komponentida aslida nimani ko'ramiz? Axborot makonida davlatlar va boshqa munosabatlar sub'ektlarining xatti-harakatlari uchun normalar va qoidalarni joriy etish imkoniyatini rad etish. Buning o'rniga kiberxavfsizlik madaniyati taklif etiladi. Ushbu yondashuv 1990-yillarning boshida BMT va YUNESKO tomonidan qabul qilingan tinchlik madaniyatining tinchlikparvarlik kontseptsiyasi bilan bog'liq.

Oltinchi alogizm -zamonaviy xalqaro siyosiy nutqda noma’lum sabablarga ko‘ra davlatning axborot makonida suvereniteti va uning axborot makonidan sodir etilgan harakatlari uchun davlatning javobgarligi g‘oyalari qarama-qarshi qo‘yilmoqda. Mas'uliyatni qo'llab, suverenitetni rad etayotganlarning mantiqi qanday? Ma'lumki, majburiyatlar faqat huquqlarga asoslanishi mumkin va aksincha. Qanday qilib siz nazorat qilish huquqiga ega bo'lmagan narsa uchun javobgar bo'lish kerak va suveren nazorat bo'lmasa, javobgarlik ham yolg'iz bo'lmaydi? Agar aniqlangan tajovuzkor Internet hujumi uchun o'nlab mamlakatlarda joylashgan botnetni yaratgan bo'lsa, bu davlatlar ham uning harakatlari uchun javobgar bo'lishi kerakmi? Botnetlarni yaratish usulining o'ziga xosligi shundaki resurslar egasi tajovuzkor tomonidan ulardan foydalanishdan bexabar. Bunday foydalanuvchi uchun javobgarlikka tortilishi uchun, hech bo'lmaganda, davlat foydalanuvchining biznesida to'sqinlik qilishi mumkin bo'lgan kiberxavfsizlik madaniyatini va tegishli nazoratni amalga oshirish huquqiga ega bo'lishi kerak, ammo u baribir (qonun bo'yicha) ularga rioya qilishi shart.

Aksincha, suverenitet suverenning suveren huquqlari tatbiq etiladigan sohalardagi har qanday xatti-harakatlari uchun javobgarligini

bildirmaydimi? Shunisi e'tiborga loyiqki, bu erda axborot makonidagi mamlakatlarning odob-axloq kodeksining qabul qilinishi juda o'rinli bo'lardi. Bunday kodni ishlab chiqish g'oyasi AQSh ma'muriyati tomonidan ishlab chiqilgan va 2011 yil 22 mayda Barak Obama tomonidan taqdim etilgan Kibermakonda Harakatlar xalqaro strategiyasida ham mavjud. Kodeks uchun BMT Bosh Assambleyasining 66-sessiyasida ShHT mamlakatlari tomonidan taklif etilgan xalqaro axborot xavfsizligi sohasidagi xatti-harakatlar qoidalari asos bo‘lishi mumkin. Bunday hujjat xalqaro miqyosda kiberxavfsizlik madaniyatini joriy qilish uchun asos bo'lishi mumkin, bu tabiiy ravishda milliy darajaga prognoz qilinadi. Biroq, bu fikr o'jarlik bilan rad etiladi.

Alogizm ettinchi liberallar lageri nazariyotchilarining g'oyalaridagi qiziq ziddiyatda yotadi. Liberallar ijtimoiy sohani axborot xavfsizligi sohasiga kiritishga qat'iyan qarshi, lekin ayni paytda Internet va ijtimoiy tarmoqlarga e'tibor qaratishadi. Demokratik davlat davlat va jamoat xavfsizligini, xususan, muhim infratuzilmalarning ishonchli ishlashini ta'minlash uchun mavjudligiga hech kim shubha qilmaydi - bu uning asosiy vazifalari, jamiyat unga berilgan huquqlar va suverenitet masalasi bu holda hech kim ko'tarilmaydi.

Shu sababli, axborot xavfsizligiga nisbatan davlatni yo'q qilish taklifi xavfli bo'lib, bu tarmoqdagi anarxiyaga olib kelishi mumkin.

Davom etish mumkin, lekin busiz ham xalqaro va jamoatchilik munosabatlarida foydalanish uchun axborot xavfsizligining mantiqiy va adekvat kontseptsiyasini yaratish hali tugallanmaganligi ayon bo'ladi.

3.3-§. Kiberxavfsizlik siyosati: O‘zbekiston yondashuvi

O‘zbekiston Respublikasi hududida axborot xavfsizligi siyosatini ishlab chiqish bo‘yicha mazkur mavzuda “davlat va xo‘jalik boshqaruvi organlarida, shuningdek mahalliy davlat hokimiyati organlarida axborot xavfsizligi siyosatini ishlab chiqish hamda amalga oshirishning asosiy tamoyillari va tartibini (keyingi o‘rinlarda) ko‘rib chiqamiz.

Mazkur mavzuda tashkilotda xavfsizlikni boshqarish bo'yicha amaliy chora-tadbirlarni tanlash, shuningdek, tashkilotlar o'rtasida ma'lumot almashishda ma'lumotlarning butunlik, foydalanuvchanlik va maxfiyligini ta'minlash uchun asosdir.

Ushbu mavzuda O‘zDSt 1047:2003, O‘zDSt 2927:2015, O‘zDSt ISO/IEC 27000:2014 ga muvofiq atamalar va ta’riflardan foydalanadi.

Tashkilotning axborot xavfsizligi siyosati - bu tashkilot o'z faoliyatidagi axborot xavfsizligi sohasidagi hujjatlashtirilgan ko'rsatmalar, qoidalar, protseduralar va amaliyotlar to'plami.

Siyosatni ishlab chiqish va amalga oshirishning maqsadlari quyidagilardan iborat:

— asosiy axborot tizimlari va resurslarini aniqlash va himoya qilish;

— axborot xavfsizligini boshqarish tizimini (keyingi o'rinlarda AXBT deb yuritiladi) joriy etishning tashkiliy-uslubiy bazasini shakllantirish.

Siyosatni ishlab chiqishda hal qilinishi kerak bo'lgan asosiy vazifalar quyidagilardan iborat:

— axborot aktivlarini tajovuzkorlarning noqonuniy harakatlaridan kelib chiqadigan tahdidlardan himoya qilish;

— tizimning uzluksiz ishlashini boshqarish;

— avariyalar, xodimlarning qasddan noto'g'ri harakatlari, texnik nosozliklar, axborotni qayta ishlash, uzatish va saqlashda noto'g'ri texnologik va tashkiliy qarorlar qabul qilish xavfini kamaytirish va mumkin bo'lgan zararni kamaytirish, texnologik jarayonlarning normal ishlashini ta'minlash;

— tashkilotning axborot xavfsizligini buzuvchi modelini ishlab chiqish;

— tashkilotning axborot xavfsizligiga potentsial tahdidlar ro'yxatini ishlab chiqish va ularni tahlil qilish;

— obyektning axborot resurslarini tasniflash va ularni nazorat qilish;

— AXBTga talablarni shakllantirish;

— axborot xavfsizligini ta'minlash bo'yicha xodimlarning majburiyatlarini belgilash.

Siyosatni ishlab chiqish uchun tashkilot rahbarining buyrug'i bilan ishchi guruh tasdiqlanadi, uning tarkibiga quyidagi shaxslar kiritilishi kerak:

— tashkilot rahbariyatining vakili;

— axborot xavfsizligi uchun mas'ul, kadrlar bo'limi boshlig'i (kadrlar bo'limi);

— texnik xodimlarning vakili (axborot xavfsizligi ma'muri, tarmoq ma'muri, ma'lumotlar bazasi ma'muri yoki boshqa vakolatli xodimlar (xodim)).

Agar kerak bo'lsa, tashkilotning boshqa xodimlarini, uchinchi tomon ixtisoslashtirilgan tashkilotlarini yoki mutaxassislarni jalb qilish mumkin.

Siyosatni ishlab chiqish jarayoni quyidagi bosqichlarga bo'linadi:

Birinchi bosqich.

Xavfsizlikning dastlabki auditi, shu jumladan axborot xavfsizligi holatini dastlabki tekshirish va inventarizatsiya qilish, tashkilot xavfsizligiga tahdidlarni aniqlash, himoyaga muhtoj resurslarni aniqlash, xavflarni aniqlash.

Audit jarayoni axborot xavfsizligining joriy holatini tahlil qiladi, mavjud zaifliklarni, faoliyatning eng muhim sohalarini va tashkilotning xavfsizlik tahdidlariga eng sezgir jarayonlarini aniqlaydi.

Auditni o'tkazish sizga tashkilotning axborot xavfsizligi tahdidlari va zaif tomonlarini aniqlashga, siyosatni ishlab chiqish uchun dastlabki ma'lumotlarni olishga yordam beradi.

Tashkilot auditi davomida quyidagilar amalga oshiriladi:

— tashkilot tomonidan O‘zbekiston Respublikasi qonun hujjatlari, O‘zbekiston Respublikasi Prezidenti va O‘zbekiston Respublikasi Vazirlar Mahkamasining farmon va qarorlari talablariga muvofiqligini o‘rganish va tahlil qilish, uni toifalarga muvofiqlashtirish;

— O'zbekiston Respublikasining normativ-huquqiy hujjatlari, shuningdek normativ-huquqiy hujjatlar, tashkilotda axborot xavfsizligini ta'minlash masalalarini tartibga soluvchi hujjatlarni muvofiqlashtirish;

— tashkilotning kompyuterlari va serverlarini birlamchi ekspertizadan o'tkazish, ya'ni ishlatiladigan operatsion tizimlar, dastur sozlamalarini tahlil qiladi;

— tashkilot veb-saytini axborot xavfsizligi tahdidlari va zaifliklari uchun tahlil qilish;

— tashkilot hududi, perimetri va binolarini jismoniy himoya qilishni ta'minlash bo'yicha amalga oshirilgan chora-tadbirlarni tahlil qilish, ya'ni xavfsizlik tizimini, kirishni boshqarish vositalarini, yong'in xavfsizligi tizimini va boshqalarni tahlil qilish;

— tashkilot xodimlarining tashkilotda belgilangan axborot xavfsizligi qoidalaridan xabardorligini suhbat orqali baholash;

— tashkilotning axborot va moddiy resurslarini turkumlashtirish va inventarizatsiya qilish tahlili.

Ikkinchi bosqich.

Tashkilotning axborot xavfsizligi siyosati loyihasini ishlab chiqish.

Siyosatni ishlab chiqishda quyidagi asosiy qoidalarga amal qilish kerak:

— siyosat amaldagi qonunchilikga va davlat standartlari talablariga to'liq bo'ysunishi kerak;

— siyosat matni faqat ikki tomonlama talqin qilishga yo'l qo'ymaydigan aniq va bir ma'noli tilni o'z ichiga olishi kerak.

Umuman olganda, siyosat amalga oshirish jarayonida foydalanuvchilarning, ma'murlarning va boshqa mutaxassislarning talab qilinadigan xatti-harakatlari haqida aniq tasavvurga ega bo'lishi kerak. Axborot tizimlari va axborot xavfsizligi vositalaridan foydalanish, shuningdek, axborot almashish va axborotni qayta ishlash operatsiyalarini bajarish. Siyosat tashkilotdagi barcha manfaatdor tomonlarga cheklovsiz taqdim etilishi mumkin bo'lgan ommaviy hujjatdir.

Uchinchi bosqich.

Tashkilotning axborot xavfsizligi siyosatini muvofiqlashtirish va amalga oshirish. Ishlab chiqilgan siyosat loyihasi belgilangan tartibda Axborot texnologiyalarini rivojlantirish vazirligiga tasdiqlash uchun yuboriladi.

O‘zbekiston Respublikasi va vakolatli organlarning o‘zaro aloqalari va kelishilganidan keyin tashkilot rahbarining buyrug‘i bilan kuchga kiradi. Shu bilan birga, tasdiqlangan siyosatni to'liq amalga oshirish uchun uni ishlab chiqish kerak. Xodimlarning lavozim tavsiflari, bo'linmalar to'g'risidagi nizom, tashkilotning shartnomaviy (shartnoma) majburiyatlari axborot xavfsizligini ta'minlash bo'yicha majburiyat va majburiyatlarni o'z ichiga olishi kerak.

Tashkilotning barcha xodimlarini tanishtirish tartibini ta'minlash va tasdiqlangan siyosat talablari va qoidalari, shuningdek, axborot xavfsizligini ta’minlash bo‘yicha muntazam tushuntirish ishlarini olib borish kerak.

Agar siyosat talablari tashkilotdan tashqarida qolsa, uchinchi shaxslar bilan shartnoma majburiyatlari axborot xavfsizligi talablarini o'z ichiga olishi kerak.

Tashkilotning axborot xavfsizligi siyosatini qayta ko'rib chiqish va yangilash.

Siyosat yiliga kamida bir marta, shuningdek quyidagi hollarda ko'rib chiqilishi kerak:

— axborot xavfsizligi bo'yicha yangi normativ-huquqiy hujjatlar va normativ hujjatlarni o'zgartirish va tasdiqlashda;

— konfiguratsiyani o'zgartirish, qo'shish yoki olib tashlashda;

— ob'ekt ma'lumotlarini himoya qilishning texnik vositalarining konfiguratsiyasi va sozlamalarini o'zgartirishda;

— mansabdor shaxslar - foydalanuvchilarning tarkibi va vazifalari o'zgartirilganda.

Axborot jarayonlari texnologiyasi o'zgarganda yoki axborotni himoya qilishning yangi vositalaridan foydalanilganda siyosat to'liq ko'rib chiqilishi kerak. Tashkilotning axborot xavfsizligi bo'yicha faoliyati siyosatga muvofiqligi uchun muntazam ravishda tekshirilishi kerak. Siyosatni yangilash va samaradorligini baholash tashkilot axborot infratuzilmasining tasdiqlangan siyosat talablari va qoidalariga muvofiqligi yuzasidan ichki va tashqi audit o‘tkazish yo‘li bilan amalga oshiriladi.

Auditning muntazamligi siyosat bilan belgilanadi, ichki audit kamida olti oyda bir marta, tashqi audit esa yiliga kamida bir marta o'tkazilishi kerak.

Axborot xavfsizligi siyosatini chiqarish tartibi

Axborot xavfsizligi siyosatining tuzilishi

Siyosatning tuzilishi va uning tafsilotlari tashkilotning xususiyatlariga qarab farq qilishi mumkin, ammo ular quyidagi bo'limlarni o'z ichiga olgan odatiy tuzilishga asoslanishi kerak:

— Kirish;
— Normativ havolalar;
— Shartlar va ta'riflar;
— Belgilar va qisqartmalar;
— Qo'llash sohasi;
— Maqsad va vazifalar;
— Asosiy fikrlar;
— Himoya ob'ektlari;
— Axborot xavfsizligi xavfi va tahdid modeli;
— Axborot xavfsizligini buzuvchi modeli;
— Axborot xavfsizligi choralari;
— Axborot xavfsizligi hodisalariga javob;
— Aloqa kanallarining xavfsizligini ta'minlash;
— Mas'uliyatni taqsimlash;
— Siyosatni ko'rib chiqish va yangilash tartibi;

Bundan tashqari, siyosat tashkilot rahbariyati tomonidan belgilangan tartibda tasdiqlangan quyidagi hujjatlarni o'z ichiga olishi yoki ularga havolalarni o'z ichiga olishi mumkin:

— Mahalliy (korporativ) tarmoq va xavfsiz tarmoq ulanishlarini tashkil etish to'g'risidagi nizom;

— Tarmoq infratuzilmasi va xavfsizlik devori darajasida axborot xavfsizligini ta'minlash to'g'risidagi nizom;

— Mahalliy (korporativ) tarmoqning tizim administratori uchun ko'rsatmalar;

— Tizim va amaliy dasturiy ta'minotni yangilash, shuningdek, ma'lumotlarni zaxiralash va tiklash to'g'risidagi nizom;

— Parolni himoya qilish bo'yicha ko'rsatmalar;

— Virusdan himoya qilish bo'yicha ko'rsatmalar;

— Ma'lumotlarni saqlash vositalari, mobil qurilmalar, ma'lumotlarni saqlash qurilmalari bilan ishlashda xavfsizlikni ta'minlash bo'yicha ko'rsatmalar;

— Avtomatlashtirilgan tizimning axborot resurslariga kirish matritsasini ishlab chiqish qoidalari;

— Foydalanishga ruxsat berilgan dasturlar ro'yxati;

— Internet va korporativ elektron pochta bilan ishlash bo'yicha ko'rsatmalar;

— Tashkilotning axborot aktivlarini boshqarish tartibi;

— Axborotni texnik muhofaza qilishni tashkil etish bo'yicha ko'rsatmalar;

— Kriptografik axborotni himoya qilishni tashkil etish bo'yicha ko'rsatmalar;

— Himoya qilinishi kerak bo'lgan axborot bilan ishlash tartibi;

— Favqulodda (g'ayritabiiy) vaziyatlarda tashkilotning uzluksiz ishlashi va tiklanishini ta'minlash rejasi.

Siyosat bo'limlarining mazmuni

Kirishda tashkilot haqida umumiy ma'lumotlarni o'z ichiga olishi kerak. Normativ hujjatlar bo'limi siyosatda havola qilingan barcha normativ hujjatlar ro'yxatini o'z ichiga olishi kerak. Atamalar va ta'riflar bo'limida barcha ishlatilgan atamalar ta’riflari kiritish kerak. Belgilar va qisqartmalar bo'limi siyosatda ishlatiladigan barcha belgilar va qisqartmalarni o'z ichiga olishi kerak. Qo'llash sohasi bo'limida siz hujjatning ko'lamini va uning amal qilish chegaralarini belgilashingiz kerak. Maqsad va vazifalar bo‘limida siyosatning asosiy maqsad va vazifalari keltirilishi kerak. Asosiy qoidalar bo'limida tashkilotda axborot xavfsizligini ta'minlash tamoyillari, usullari va choralarini ko'rsatish kerak. Himoya ob'ektlari bo'limida siz tashkilotning himoyalangan

aktivlarini ko'rsatishingiz kerak. Tashkilotning aktivlari quyidagilardan iborat:

— tashkilot xodimlari, tasodifiy va ruxsat etilmagan ta'sirlarga va ularning xavfsizligi buzilishiga sezgir bo'lgan axborot resurslari, shu jumladan taqdim etish shakli va turidan qat'i nazar, hujjatlar va ma'lumotlar massivlari ko'rinishida taqdim etilgan ommaviy ma'lumotlar;

— dasturiy ta'minot resurslari - operatsion tizimlar va amaliy dasturlar, ishlab chiqish vositalari va yordamchi dasturlari, server ilovalari va xizmatlari;

— jismoniy resurslar - kompyuter va aloqa uskunalari, ma'lumotlar tashuvchilar, binolar va boshqalar.

Axborot xavfsizligi xavfi va tahdid modeli bo'limida tashkilotdagi axborot xavfsizligi xavflarini, shu jumladan uchinchi tomon tashkilotlari bilan o'zaro aloqalar bilan bog'liq bo'lganlarni tahlil qilishning asosiy tamoyillarini taqdim etish kerak. Agar biznes maqsadlarida tashkilotning axborot aktivlari va axborotni qayta ishlash vositalariga uchinchi shaxslarning kirishi zarur bo'lsa, shuningdek, uchinchi shaxslardan tovarlar va xizmatlarni olishda, axborot xavfsizligi uchun yuzaga kelishi mumkin bo'lgan oqibatlarni va nazorat qilish talablarini aniqlash uchun xavf tahlilini o'tkazish kerak. Bunday faoliyat uchinchi tomon tashkiloti bilan tuzilgan shartnomalarda muvofiqlashtirilishi va belgilanishi kerak.

Agar tashqi tashkilotlarga tashkilotning axborotni qayta ishlash vositalariga yoki axborot aktivlariga kirishiga ruxsat berish zarurati tug'ilsa, muayyan nazorat uchun talablarni belgilash uchun xavflarni aniqlash kerak. Uchinchi shaxslar tomonidan kirish bilan bog'liq xavflarni aniqlashda uchinchi shaxsga kirish zarur bo'lgan ma'lumotlarni qayta ishlash vositalarini e'tiborga olinishi kerak.

Tashkilotlar, agar yuqori darajadagi autsorsingdan foydalanilsa yoki bir nechta uchinchi tomonlar ishtirok etsa, tashkilotning ichki aloqalarini boshqarish jarayonlari bilan bog'liq xavflarga duch kelishi mumkin.

Boshqaruv elementlari turli uchinchi tomonlar bilan tuzilgan shartnomalarni tavsiflaydi, masalan:

— internet provayderlari, telefon xizmatlari, texnik xizmat ko'rsatish va qo'llab-quvvatlash xizmatlari kabi xizmat ko'rsatuvchi provayderlar;

— boshqariladigan xavfsizlik xizmatlari;

— axborot texnologiyalari tizimlari, axborotni saqlash xizmatlari, call-markazlar kabi ob'ektlar yoki operatsiyalarni autsorsing qilish;

— apparat ta'minoti va texnik xizmat ko'rsatish xodimlari dasturiy ta'minot;

— tozalash, qo'riqlash, ovqatlanish va boshqa maishiy xizmatlar bilan shug'ullanadigan xodimlar;

— vaqtinchalik xodimlar, talabalar va shartnoma ishchilari (mijozlar).

Ushbu kelishuvlar uchinchi tomonlar bilan bog'liq xavflarni kamaytirishga yordam beradi.

Axborot xavfsizligiga potentsial tahdidlar paydo bo'lish xususiyatiga ko'ra ikki turga bo'linadi: tabiiy (ob'ektiv) va sun'iy (sub'ektiv). Axborot tizimining o'ziga nisbatan tahdidlarning manbalari tashqi va ichki bo'lishi mumkin.

Barcha tahdid manbalari tahdid tashuvchisi (tahdid manbai) turiga qarab sinflarga bo'linadi:

— qasddan yoki tasodifiy huquqbuzarlik sifatida kvalifikatsiya qilinishi mumkin bo'lgan sub'ektning harakatlari (inson omili) natijasida yuzaga keladigan tahdid manbalari;

— texnogen texnik tahdidlar manbalari anglatadi insonning texnokratik faoliyati bilan belgilanadi;

— bashorat qilib bo'lmaydigan yoki oldindan ko'rish mumkin bo'lgan, ammo insoniyat bilimi va imkoniyatlarining hozirgi darajasida oldini olish mumkin bo'lmagan tabiat hodisalaridan kelib chiqadigan tahdidlarning tabiiy manbalari.

Axborot xavfsizligini buzuvchilar bo‘limida axborot xavfsizligini buzuvchilar tasnifi berilgan. Axborot xavfsizligini buzuvchilar mansubligiga ko'ra ikki guruhga bo'linadi: ichki va tashqi. Ichki potentsial qoidabuzarlar - bu axborotlashtirish ob'ektlari hududiga kirish huquqiga ega bo'lgan tashkilot xodimlari.

Tashkilotning axborot xavfsizligini ta'minlash bo'yicha asosiy chora-tadbirlar quyidagilarga bo'linadi:

— huquqiy choralar;

— axloqiy va axloqiy choralar;

— tashkiliy chora-tadbirlar;

— texnologik chora-tadbirlar;

— muhandislik tadbirlari;

— dasturiy ta'minot va apparat ta'minoti chora-tadbirlari;

— tashqi foydalanuvchilar bilan munosabatlarda xavfsizlik choralari.

Axborot xavfsizligini ta’minlashning huquqiy chora-tadbirlariga O‘zbekiston Respublikasi qonunlari va axborot bilan ishlash qoidalarini tartibga soluvchi, axborotni qayta ishlash va undan foydalanish jarayonida axborot munosabatlari ishtirokchilarining huquq va majburiyatlarini belgilovchi, shuningdek, huquqbuzarliklar uchun javobgarlikni belgilovchi boshqa normativ-huquqiy hujjatlar kiradi. Axloqiy va chora-tadbirlar axborot texnologiyalari tarqalishi bilan an'anaviy ravishda shakllangan yoki rivojlanayotgan xatti-harakatlar normalarini o'z ichiga oladi. Ushbu normalar ko'pincha majburiy emas, chunki qonun bilan tasdiqlangan normativ hujjatlar, ammo ularga rioya qilmaslik shaxsning, bir guruh odamlarning yoki umuman tashkilotning obro'-e'tiborini pasayishiga olib kelishi mumkin. Axloqiy va axloqiy me'yorlar ham yozilmagan, ham yozilmagan bo'ladi, ya'ni ular ma'lum bir qonun yoki qoidalar kodeksida (nizomida) rasmiylashtiriladi. Ma'naviy va axloqiy himoya choralari profilaktik bo'lib, tashkilot jamoasida sog'lom axloqiy muhitni yaratish uchun doimiy ishlashni talab qiladi.

Tashkiliy chora-tadbirlar asosan xodimlar bilan ishlash, muhofaza qilish ob'ektlarini joylashtirish va joylashtirishni tanlash, jismoniy va yong'indan himoya qilish tizimlarini tashkil etish, ko'rilgan chora-tadbirlarning bajarilishini nazorat qilish va himoya qilish choralarini amalga oshirish uchun shaxsiy javobgarlikni belgilashga qaratilgan. Ichki antropogen, texnogen sonini kamaytirish choralari qo'llaniladi.

Tahdidlarni tashkiliy usullar bilan bartaraf etish axborotni himoya qilishning eng kam xarajatli chorasidir. Texnologik himoya choralari ma'lum turdagi ortiqcha (tarkibiy, funktsional, axborot, vaqtinchalik va boshqalar) foydalanishga asoslangan va xodimlarning huquq va vakolatlari doirasida xato va huquqbuzarliklarga yo'l qo'yish ehtimolini kamaytirishga qaratilgan turli texnologik echimlar va texnikalarni o'z ichiga oladi.

Bu choralarga quyidagilar kiradi:

— mas'uliyatli ma'lumotlarni ikki marta kiritish tartib-qoidalaridan foydalanish;

— mas'uliyatli operatsiyalarni faqat bir nechta shaxslarning kelishuvi mavjud bo'lganda boshlash;

— chiquvchi va kiruvchi xabarlar tafsilotlarini tekshirish tartiblari va boshqalar.

Muhandislik va texnik usullar axborot xavfsizligini ta'minlash talablarini hisobga olgan holda binolar, inshootlar, muhandislik

tarmoqlari va transport kommunikatsiyalarini optimal qurishga qaratilgan.

Muhandislik tadbirlari quyidagilarni o'z ichiga oladi:

— uskunalar va binolarning elektr muhofazasini ta'minlash;
— binolarni tekshirish;
— binolarni vayronagarchilikdan himoya qilish;
— uskunalarni optimal joylashtirish;
— muhandislik kommunikatsiyalarini optimal joylashtirish;
— vizual himoya vositalaridan foydalanish;
— binolarni akustik ishlov berish;
— konditsioner tizimlaridan foydalanish.

Texnik chora-tadbirlar axborotni himoya qilish, vaziyatni nazorat qilishning maxsus texnik vositalaridan foydalanishga asoslanadi va tashqi tahdidlarning texnik vositalar yordamida axborotga ta'sir qilish harakatlari bilan bog'liq tahdidlarni bartaraf etishga qaratilgan.

Ushbu chora-tadbirlarning ba'zilari texnogen tahdid manbalarining ta'sirini bartaraf etishi va ob'ektiv, sub'ektiv va tasodifiy zaifliklarning ta'sirini kamaytirishi mumkin.

Texnik chora-tadbirlar quyidagilarni o'z ichiga oladi:

— qayta ishlashning texnik vositalarining ortiqchaligi;
— aloqa kanallarining ortiqchaligi;
— ajratilgan aloqa kanallaridan foydalanish;
— axborot resurslarining zaxira nusxasini (dublikatini) yaratish;
— fazoviy shovqin tizimini yaratish;
— akustik va tebranish shovqin tizimini yaratish;
— birliklar va jihozlarni ekranlash;
— kafolatlangan quvvat manbalaridan foydalanish;
— axborot uzatish uchun aloqa kanallarini nazorat qilish;
— axborotlashtirish ob'ektlarida axborotni ushlash uchun elektron qurilmalarning yo'qligini nazorat qilish.

Dasturiy ta'minot va texnik vositalar axborotni qayta ishlash jarayoni bilan bevosita bog'liq bo'lgan tahdidlarning namoyon bo'lishini bartaraf etish uchun mo'ljallangan. Dasturiy-texnik chora-tadbirlarni amalga oshirish tahdidlarning ichki antropogen manbalarining ta'sirini sezilarli darajada kamaytiradi. Dasturiy ta'minot va apparat choralari guruhi quyidagi choralarni birlashtiradi:

— axborotni qayta ishlash vositalaridan foydalanishni cheklash (dasturiy ta'minot, texnik vositalar);

— himoyalangan ob'ektlarga (himoyalangan ma'lumotlarga) kirishni cheklash;

— sub'ektlarga (foydalanuvchilarga) kirishni nazorat qilish;

— tashqi va ichki axborot oqimlarini boshqarish;

— tuzilish va maqsadni yashirish;

— ma'lumotlarning haqiqiyligini tasdiqlash;

— transformatsiya (shifrlash, kodlash) uzatish paytida ma'lumot saqlash;

— foydalanilmagan xizmatlarni bloklash;

— dasturiy ta'minotning yaxlitligi, dasturiy ta'minot va apparat konfiguratsiyasi monitoringi;

— virusga qarshi himoya;

— axborot xavfsizligi hodisalari va hodisalari monitoringi;

— korporativ tarmoq foydalanuvchilarining harakatlarini kuzatish.

Uchinchi shaxslarga axborot va tashkilot aktivlariga kirish huquqini berishda axborot xavfsizligining barcha belgilangan talablariga e'tibor qaratish va tashqi foydalanuvchilar bilan ishlashda xavfsizlik choralarini ko'rish kerak.

Uchinchi shaxslarga tashkilotning har qanday aktivlariga kirish huquqini berishdan oldin, axborot xavfsizligi bilan bog'liq quyidagi shartlarni ko'rib chiqish kerak (berilgan kirish turi va darajasiga qarab, ularning hammasi ham qo'llanilishi mumkin emas):

— tashkilot aktivlarini, shu jumladan axborot va dasturiy ta'minotni himoya qilish va ma'lum zaifliklarni boshqarish tartiblari;

— aktivlar, masalan, ma'lumotlarning yo'qolishi yoki o'zgartirilishi tufayli buzilganligini aniqlash uchun protseduralar;

— aktivlarning yaxlitligi;

— nusxa ko'chirish va oshkor qilish cheklovlari;

— taqdim etilayotgan tovarlar va xizmatlar tavsifi;

— mijozlarga kirishning turli shartlari, talablari va afzalliklari.

Kirishni nazorat qilish shartnomalari quyidagilarni o'z ichiga oladi:

— ruxsat etilgan kirish usullari va noyob foydalanuvchi identifikatorlari va parollarini boshqarish va ulardan foydalanish;

— Imtiyozlar va foydalanish huquqini berish jarayoni;

— aniq ruxsat berilmagan har qanday kirishni taqiqlash printsipi;

— foydalanuvchining kirish huquqlarini bekor qilish yoki kirishni bloklash jarayoni;

— Axborot xavfsizligining buzilishi va xavfsizlik tizimidagi zaif bo'g'inlarni aniqlash hodisalari to'g'risida xabar berish, xabardor qilish va tekshirish tartiblari;

— kirish uchun har bir xizmat tavsifi;

— rejalashtirilgan xizmat ko'rsatish darajasi va qabul qilinishi mumkin bo'lmagan xizmat darajalari;

— tashkilotning aktivlari bilan bog'liq har qanday faoliyatni kuzatish va bekor qilish huquqi;

— tashkilot va mijozning tegishli majburiyatlari;

— huquqiy masalalar bo'yicha majburiyatlar va agar shartnoma chet eldagi mijozlar bilan hamkorlikni o'z ichiga olgan bo'lsa, turli xil milliy huquq tizimlarini hisobga olgan holda ma'lumotlarni himoya qilish qonunlari kabi qonuniy talablarga qanday rioya qilish kerakligi;

— intellektual mulk huquqlari va mualliflik huquqlari, shuningdek har qanday qo'shma ishni himoya qilish.

Tashkilot aktivlariga kirish huquqiga ega bo'lgan uchinchi tomon xodimlariga qo'llaniladigan axborot xavfsizligi talablari taqdim etilgan ma'lumotlarning tasnifiga va ularni qayta ishlash vositalariga qarab sezilarli darajada farq qilishi mumkin. Ushbu xavfsizlik talablari uchinchi tomon tashkilotining xodimi bilan tuzilgan shartnomada aks ettirilishi mumkin, unda barcha ma'lum xavflar va axborot xavfsizligi talablari mavjud.

Uchinchi shaxslar bilan tuzilgan shartnomada boshqa xavfsizlik talablari ham bo'lishi mumkin. Uchinchi shaxslarning kirish huquqi to'g'risidagi shartnomada boshqa tegishli tomonlarni jalb qilish uchun ruxsatnoma, shuningdek ularning kirish va ishtirok etish shartlari ko'rsatilishi kerak.

Axborot xavfsizligi hodisalariga javob berish bo'limi axborot xavfsizligi intsidentlariga javob berish jarayonining tavsifini o'z ichiga olishi kerak, unda axborotni qayta ishlashning avtomatlashtirilgan sohalari uchun tizim auditi vositalari, shuningdek, tashkilotning barcha xodimlari uchun axborot xavfsizligi hodisalari haqida xabar berish tartiblari va boshqa holat ma'lumotlarini himoya qilish tizimlari kiradi.

Ushbu bo'limda hodisalarga javob berish mexanizmlari tasvirlangan bo'lishi kerak, masalan, axborot xavfsizligi buzilishi hodisalari aniqlanganligi to'g'risidagi ma'lumotlar rahbariyatga xabar qilinadi va

belgilangan tartibda axborot xavfsizligi ma'muriga xabar qilinadi. Hujjatlar yoki tegishli ko'rsatmalar bilan tartibga solinmagan mustaqil va ruxsatsiz harakatlar qilish taqiqlanadi.

Axborotning sizib chiqishi kanallari aniqlanganda keyingi chiqib ketishining oldini olish maqsadida axborotni qayta ishlash hududini mahalliylashtirish choralari ko‘riladi va tashkilotda himoyalangan axborotni qayta ishlash bilan bog‘liq jarayonlar to‘xtatiladi. Zararli dasturlarni yuqtirgan taqdirda, “Tashkilotning virusga qarshi himoyasi bo'yicha yo'riqnoma” ga muvofiq etkazilgan zararni bartaraf etish choralari ko'riladi.

Tashkilotdagi hodisalarni samarali boshqarish uchun ushbu bo'lim axborot xavfsizligi hodisalari va zaif tomonlarini samarali va tezkor hal qilish uchun javobgarlik va tartiblarni tavsiflashi kerak. Bunga javoban axborot xavfsizligi hodisalarini doimiy takomillashtirish, kuzatish, baholash va umumiy boshqarish jarayonlari qo'llanilishi kerak.

Axborot xavfsizligi intsidentlariga tez, samarali va tashkiliy javob berishni ta'minlash uchun hodisalarni boshqarish tartibi ishlab chiqilishi va tasdiqlanishi kerak. Xabarlardan tashqari axborot xavfsizligi hodisalarini aniqlash uchun hodisalar va axborot tizimining zaifliklari, tizimlar, ogohlantirishlar va zaifliklarni kuzatib borish kerak. Axborot xavfsizligi hodisalarini boshqarish maqsadlari rahbariyat bilan kelishilgan bo'lishi kerak, axborot xavfsizligi hodisalarini boshqarish uchun mas'ul bo'lgan xodimlar e'tiboriga tashkilotning intsidentlarni hal qilishning ustuvor yo'nalishlarini etkazish kerak.

“Aloqa kanallari xavfsizligini ta'minlash” bo'limi.

Aloqa kanallari axborot kabellariga ulanish yoki soxta elektromagnit nurlanish va boshqa kabellarda pikap orqali ma'lumotni olib tashlash orqali ma'lumotlarga ruxsatsiz kirish ehtimolini kamaytirishga, shuningdek, kabel uskunalarini elektromagnit parazitlardan va mexanik shikastlanishlardan himoya qilishni ta'minlashga qaratilgan bo'lishi kerak.

Simsiz aloqa kanallarini himoya qilish trafikni tinglash, xizmat ko'rsatishni rad etish, ruxsatsiz ulanish kabi hujumlarni kamaytirishga qaratilgan bo'lishi kerak.

“Mas'uliyatni taqsimlash” bo'limi. Ushbu bo'lim siyosatning muhim bo'limlaridan biri bo'lib, tashkilotning axborot xavfsizligini rahbariyat tomonidan boshqarish, mas'uliyatni taqsimlash va axborot xavfsizligi masalalarini muvofiqlashtirish tamoyillarini aks ettirishi kerak. Ushbu

bo'limda axborot xavfsizligi bo'yicha barcha mas'uliyatlar aniq belgilanishi kerak.

Axborot resurslarini to'g'ri himoya qilishni ta'minlash maqsadida tashkilot barcha axborot resurslarining hisobini yuritishi kerak. Buning uchun barcha resurslar aniqlanishi va shakllantirilishi, shuningdek, tashkilotning avtomatlashtirilgan tizimlarining axborot resurslari reestri (keyingi o'rinlarda Reyestr deb yuritiladi) yangilanib turishi kerak.

Ro'yxatga olish kitobi falokatni tiklash uchun zarur bo'lgan barcha ma'lumotlarni, jumladan, manba turi, formati, joylashuvi, zaxira ma'lumotlari va toifalarni o'z ichiga olishi kerak. Ushbu reestr boshqa registrlarni keraksiz ravishda takrorlamasligi kerak, lekin ularning mazmuni muvofiqligi ta'minlanishi kerak. Buning uchun resursni ofisda ro'yxatdan o'tkazgandan so'ng, berilgan raqam resurs joylashgan avtomatlashtirilgan tizim reyestriga o'chiriladi.

Reestr - bu tashkilot idorasida ro'yxatdan o'tgan va himoya qilinishi kerak bo'lgan tashkilotning barcha axborot resurslarini o'z ichiga olgan hujjat (qog'oz yoki elektron tashuvchilarda). Tashkilot rahbarining qarori bilan reestr butun tashkilot yoki uning tarkibiy bo'linmasi uchun yuritilishi mumkin.

Barcha axborot resurslari uchun ularning egalari tayinlanishi kerak, ular ushbu resurslarning xavfsizligini ta'minlash uchun javobgardir.

Resursning to'g'ri toifalarga bo'linishini ta'minlash, toifalarni va ushbu manbaga kirish huquqlarini aniqlash va vaqti-vaqti bilan ko'rib chiqish resurs egasining mas'uliyatidir. Agar kerak bo'lsa, resurs egalari nazoratni amalga oshirish va qo'llab-quvvatlash mas'uliyatini tashkilotdagi boshqa xodimlarga topshirishlari mumkin, ammo resursning etarli darajada himoyalanganligini ta'minlash uchun javobgarlik resurs egasida qoladi. Axborot resurslarini inventarizatsiya qilishda ularning saqlanishi reestr bo‘yicha va reestrda ko‘rsatilgan joylashgan joyda amalda mavjudligi tekshiriladi.

Axborotni texnik muhofaza qilishni tashkil etish bo'yicha ko'rsatmalartashkilotda qo'llaniladigan axborotni texnik himoya qilish usullari va vositalari to'g'risidagi ma'lumotlarni o'z ichiga olishi kerak. Kriptografik axborotni himoya qilishni tashkil etish bo'yicha ko'rsatmalartashkilotda qo'llaniladigan axborotni kriptografik himoya qilish usullari va vositalari to'g'risidagi ma'lumotlarni o'z ichiga olishi kerak.

Himoya qilinishi kerak bo'lgan ma'lumotlar bilan ishlash tartibiNoto'g'ri ishlov berish tashkilotga zarar etkazishi mumkin bo'lgan

axborot resurslari ro'yxatini, ushbu axborot resurslari bilan ishlashga qo'yiladigan talablarni, buzilganlik uchun javobgarlikni va ushbu talablarni bajarish bo'yicha kelishuvni (majburiyatni) o'z ichiga olishi kerak.

Axborot xavfsizligini ta'minlash sohasidagi faoliyatni tartibga soluvchi normativ-huquqiy hujjatlar va normativ hujjatlar ro'yxati:

O'zDSt 1047:2003 Axborot texnologiyalari. Shartlar va ta'riflar.

O'zDSt 2927:2015 Axborot texnologiyalari. Axborot xavfsizligi, atamalar va ta'riflar.

O'zDSt 2814:2014 Axborot texnologiyalari. Avtomatlashtirilgan tizimlar.

Axborotga ruxsatsiz kirishdan himoyalanish darajasi bo'yicha tasniflash

O'zDSt 2815:2014 Axborot texnologiyalari.

O'zDSt ISO/IEC 27000:2014 Axborot texnologiyalari. Xavfsizlik usullari. Axborot xavfsizligini boshqarish tizimlari. Umumiy ko'rinish va lug'at.

O'zDSt ISO/IEC 27001:2009 Axborot texnologiyalari. Xavfsizlik usullari. Axborot xavfsizligini boshqarish tizimlari. Talablar.

O'zDSt ISO/IEC 27002:2008 Axborot texnologiyalari. Xavfsizlik usullari. Axborot xavfsizligini boshqarish amaliyoti.

O'zDSt ISO/IEC 27003:2014 Axborot texnologiyalari. Xavfsizlik usullari. Axborot xavfsizligini boshqarish tizimini joriy qilish bo'yicha qo'llanma.

O'zDSt ISO/IEC 27005:2013 Axborot texnologiyalari. Xavfsizlik usullari. Axborot xavfsizligi risklarini boshqarish.

O'zDSt ISO/IEC 27007:2015 Axborot texnologiyalari. Xavfsizlik usullari. Axborot xavfsizligini boshqarish tizimlarini tekshirish bo'yicha ko'rsatmalar.

O'zDSt ISO/IEC 27008:2015 Axborot texnologiyalari. Xavfsizlik usullari. Axborot xavfsizligini nazorat qilish bo'yicha auditorlik qo'llanmasi.

O'zDSt ISO/IEC 27010:2015 Axborot texnologiyalari. Xavfsizlik usullari. Tarmoqlar va tashkilotlar o'rtasidagi aloqada axborot xavfsizligini boshqarish bo'yicha qo'llanma.

O'zDSt ISO/IEC 27035:2015 Axborot texnologiyalari. Xavfsizlik usullari. Axborot xavfsizligi hodisalarini boshqarish.

O'zDSt ISO/IEC-1:2008 Axborot texnologiyalari. Xavfsizlik usullari. Axborot texnologiyalari xavfsizligini baholash mezonlari. 1-qism. Kirish va umumiy model.

O'zDSt ISO/IEC-2:2008 Axborot texnologiyalari. Xavfsizlik usullari. Axborot texnologiyalari xavfsizligini baholash mezonlari. 2-qism. Funktsional xavfsizlik talablari.

O'zDSt ISO/IEC-3:2008 Axborot texnologiyalari. Xavfsizlik usullari. Axborot texnologiyalari xavfsizligini baholash mezonlari. 3-qism: Xavfsizlik kafolati talablari.

3.4-§. Geopolitika va kiberxavfsizlik

Milliy davlatlar o'rtasidagi munosabatlarga kelsak, kiberhujumga javob berish alohida ahamiyatga ega va o'sib bormoqda. Geosiyosatni tahlil qilishning eng muhim nuqtalaridan biri bu kiber hujumga qarshi mumkin bo'lgan javob va ma'lum bir chora qanday qabul qilinishi. Ilgari aytilgan javoblar doirasini hisobga olgan holda, milliy qaror qabul qiluvchilar milliy davlatlar qanday munosabatda bo'lishini baholashlari kerak, shu sababli geosiyosat ushbu javoblarga haqiqiy javoblarni ham, reaktsiyalarni ham tushunish muhimligini ta'kidlaydi.

Kiber bilan bog'liq hujumlar va tadbirlarning quyidagi misollari kiberxavfsizlik va geosiyosat o'rtasidagi muhim munosabatlarni ta'kidlaydi:

1-misol: ba'zilar Rossiya hukumatini 2008 yilda Rossiyaning Gruziyaga bostirib kirishiga olib kelgan harbiy kurashlar paytida Gruziya millatidagi rasmiy veb-saytlarga uyushgan jinoyatchilikka hujum qilish yoki rag'batlantirishda gumon qilmoqdalar.

2-misol: 2009-2010 yillarda hukumat tomonidan yaratilgan murakkab kompyuter qurti degan shubhalar paydo bo'ldi Stuxnet Eron atom zavodini o'chirish uchun bo'shatilgan edi sentrifugalar qurol darajasida boyitilgan uran ishlab chiqarish uchun ishlatilishi mumkin. Noma'lum manbalar va chayqovchilar qo'shma Shtatlar va Isroil hukumatlari qurtni ishlab chiqishi va tarqatishi mumkinligini ta'kidladilar.

3-misol: Amerika Mudofaa vazirligi urushni rejalashtirish va urush qilishning ajralmas qismi sifatida Internetga asoslangan mudofaa va tajovuzkor kiber strategiyalarni tuzadigan kiber qo'mondonlik tuzilmasini yaratdi.

4-misol: 2014 yil May oyida G'arbiy Pensilvaniyada AQShning oltita qurboniga, shu jumladan atom elektr stantsiyalari, metallar va quyosh mahsulotlari sanoatiga qaratilgan kompyuterni buzish, josuslik va

boshqa huquqbuzarliklar uchun beshta xitoylik harbiy amaldor ayblandi. Ayblov xulosasi bir necha yillik vahiylardan so'ng, Xitoy harbiylari va boshqa agentlari AQShning yirik korporatsiyalari va media kompaniyalarida tijorat sirlarini o'g'irlash va jurnalistlar qanday hikoyalar ustida ishlayotganini bilish uchun kompyuterlarga kirishgan.

5-misol: 2014 yil oktyabr oyida rus xakerlari NATO, Ukraina hukumati va G'arb biznesiga josuslik qilish uchun Microsoft Windows dagi nuqsondan foydalanayotgani aniqlandi.

6-misol: Taniqli Ponemon instituti sentyabr oyida xabar 2014 bu 43% Amerika Qo'shma Shtatlarida firmalar o'tgan yili ma'lumotlar buzilishi tajribali edi. Chakana savdo buzilishlari, xususan, o'tgan yili virulentlik hajmi kattalashgan edi. Eng dahshatli buzilishlardan biri 2014 yil iyul oyida JP Morgan Chase & Co-da topilgan., bu erda 76 million xonadon va 7 million kichik biznes ma'lumotlari buzilgan. Buzilishi Ukraina sodir voqealar ustidan Rossiyada Putin rejimi tomonidan o'ch edi, agar Obama ma'muriyati rasmiylari hayron qilgan.

7-misol: bugungi kunda dalillarda shaxslarning ekspluatatsiyasi turlari orasida o'g'irlangan milliy identifikator raqamlari, o'g'irlangan parollar va to'lov ma'lumotlari, o'chirilgan onlayn identifikatorlar va barcha onlayn suhbatlar va tugmachalarni bosish va hatto haydovchisiz mashinalarni yozib oladigan josuslik vositalari mavjud.

8-misol: ushbu hisobot nashr etilishidan bir necha kun oldin, Apple-ning iCloud bulutga asoslangan ma'lumotlarni saqlash tizimi Xitoyda foydalanuvchilarning parollarini o'g'irlash va ularning hisob qaydnomalariga josuslik qilishga qaratilgan hujumning maqsadi edi. Ba'zi faollar va xavfsizlik bo'yicha mutaxassislar Xitoy hukumati hujumni uyushtirgan deb gumon qilishdi, ehtimol iPhone 6 mamlakatda mavjud bo'lganligi sababli. Boshqalar hujum hukumat tashabbusi bilan amalga oshiriladigan darajada murakkab emas deb o'ylashdi.

Geosiyosat o'rtasidagi munosabatlarni anglatadi milliy davlatlar va ularning geografiya va milliy-davlat siyosati o'rtasidagi munosabatlarga alohida e'tibor qaratib, ularning katta global hamjamiyat bilan aloqasi:

“Geosiyosat o'z vazifasi sifatida geosiyosiy diss-kurslarni buzishni o'z zimmasiga oladi: pregiven yoki umumiy joylarda siyosat geografiyasini emas, balki siyosatning geografik spetsifikatsiyasi siyosatini ilgari surish. Xavfsizlik va geosiyosat dualistik tarzda ishlaydi. Bir tomondan, diplomatiya va tashqi siyosat odatda maxfiylik bilan qoplangan baland muammolar sifatida tasavvur qilinadi. Boshqa tomondan, va ixtisoslashgan tilga ishonish bilan bir qatorda, xavfsizlik va

geosiyosatning nutqi joylar va o'ziga xosliklar haqidagi umumiy rivoyatlarga katta ahamiyat beradi. Aksariyat geosiyosiy mulohazalar rasmiy emas, balki amaliydir. Bu ezoterik akademik va texnik dalillarga emas, balki sog'lom fikrga asoslanadi".

Ushbu mavzuda kiberxavfsizlik va geosiyosat o'rtasidagi munosabatlar ularning qo'shilishining murakkabligini aks ettiruvchi alohida misollarni tahlil qilish orqali ko'rib chiqiladi. Tahlil xalqaro huquq, xususan o'zini himoya qilish va mutanosiblikka taalluqlidir. Bashorat qilish va izchillikni aks ettiruvchi milliy-davlat qarorlarini qabul qilish global tartibni sezilarli darajada oshiradi. Biroq, tahdidlar— haqiqiy yoki seziladimi-mintaqaviy va global barqarorlikka keskin ta'sir qiladi. Shu nuqtai nazardan, milliy davlatlarning muayyan inqiroz nuqtalariga bir tomonlama, ikki tomonlama yoki ko'p lateral ravishda qanday javob berishini baholash geosiyosiy mulohazalarning amaliy ta'sirini tushunish uchun juda muhimdir.

Samarali geosiyosat nazariy va amaliy o'rtasidagi to'qnashuvni talab qiladi. Birinchisi, milliy rahbarlardan xalqaro huquq, millatlararo munosabatlar, moliya, geografiya va harbiy kuch, xususan, uning chegaralarini o'z ichiga olgan keng ko'lamli masalalarni tushunishni talab qilmoqda. Ikkinchisi taktik va strategik masalalarning ahamiyatini anglagan holda, ushbu aniq fanlarni ichki siyosatga ham, jahon hamjamiyatiga ham sezgirlik bilan amalga oshirishni talab qiladi. Garchi prima facie, taktik va strategik mulohazalar dissonansni taklif qilsa-da, samarali milliy rahbarlar ikkalasini ham qaror qabul qilish jarayoniga qo'shishga qodir.

Yuqorida aytib o'tganimizdek, geosiyosat-bu milliy davlatlar o'rtasidagi munosabatlar va ularning katta global hamjamiyat bilan aloqasi bo'lib, geografiya va milliy-davlat siyosati o'rtasidagi munosabatlarga alohida e'tibor qaratilgan. Geografiya va katta global hamjamiyatga e'tibor geosiyosatda hal qiluvchi rol o'ynaydi.

Quyidagilarni ko'rib chiqing: bu 1924 yilda dahshatli yer zilzilasi Osiyoni urdi, yuz minglab odamlarga ta'sir qildi va minglab kilometr uzoqlikdagi tsunamiga sabab bo'ldi. Biroq, axborot tizimlarining etishmasligi sababli, tsunami yo'lida bo'lganlarni ogohlantirishning yoki zilziladan jabrlangan shaxslar uchun yordam so'rashni ogohlantirishning etarli usuli yo'q.

Endi 2020 yilni ko'rib chiqing, sunami yo'lida nafaqat boshqalarni xabardor qilish, balki zilziladan zarar ko'rganlar uchun boshqalardan yordam so'rash ham tezroq. Biroq, buni so'rash har doim ham natija

bermasligi mumkin. Biz yangiliklar qayta ishlanadigan dunyoda yashayapmiz va bizning qo'limizda doimiy ma'lumotlar mavjud. Shu sababli, dunyoning turli burchaklarida har kuni sodir bo'ladigan cheksiz vahshiyliklar va adolatsizliklar to'g'risida doimiy ravishda xabardor bo'lish mavjud. Har qanday kunda qochqinlar inqirozi, tibbiy virus, jismoniy falokat yoki inson tomonidan qilingan hujum mavjud.

Shunday qilib, geosiyosat bilan biz yashayotgan tobora globallashib borayotgan dunyo katta ta'sir ko'rsatadigan milliy davlatlar o'rtasidagi munosabatlar va ularning katta hamjamiyat bilan aloqasi. Kiberxavfsizlik ma'nosida tobora globallashgan dunyoning ta'sirini ko'rib chiqing.

2-misolda ko'rinib turganidek, virus, Stuxnet Eronning yadroviy imkoniyatlarini o'chirish uchun jo’natildi. Ushbu virusning joriy etilishi yangiliklar kanallarida va butun dunyo bo'ylab odamlar tan olgan narsalarda keng tarqalgan. Nafaqat bu, balki kimning virusni mamlakatning yadroviy qobiliyatiga kiritish qobiliyati faqat kiber tomonidan moslashtirilgan innovatsion texnikalar tufayli mumkin.

Eronda, ehtimol, boshqa mamlakatlar yadro imkoniyatlari to'g'risida o'zlarining hisobotlari bilan yoki, ehtimol, qurilayotgan yoki hozirda mavjud bo'lgan yadroviy inshootlarning hujjatlarini yozib olgan kuzatuv ma'lumotlari bilan xabardor bo'lishgan. Ushbu texnologiya dronlar yoki boshqa sun'iy yo'ldosh kuzatuvi shaklida kelgan. Shunday qilib, tobora ortib borayotgan globallashgan dunyo bo'lib, mamlakatlar Eron kabi bir mamlakat ushbu imkoniyatlarga ega ekanligini bilishdan xavotirda edilar.

Bundan tashqari, agar yadroviy inshoot bilan bog'liq ma'lumotlarning kiritilishi 1924 yilda sodir bo'lgan bo'lsa, Stuxnet virusi juda to'g'ri bajarganidek, yadro inshootlarini yo'q qilish yoki jiddiy ravishda buzish imkoniyati ham bo'larmidi. Shunday qilib, nafaqat ma'lumotlarning kiritilishi geosiyosat haqidagi tasavvurimizni sezilarli darajada o'zgartirdi, balki bu ma'lumotlarga qanday munosabatda bo'lishimiz yanada katta rol o'ynaydi.

Taktik fikrlash faqat zudlik bilan yo'naltirilgan qaror qabul qilishni aks ettiradi, strategik fikrlash esa tezkor natijalar va ta'sirlardan mahrum bo'lgan uzoq muddatli istiqbolni chuqur tushunish va qadrlashni aks ettiradi. Ehtimol, vaziyatlar tor nuqtai nazarni oqlaydi yoki belgilaydi. Jahon hamjamiyati moliya, xavfsizlik, chegara nazorati, atrof-muhit, sog'liqni saqlash va tabiiy resurslar kabi keng ko'lamli masalalarda hamkorlikni kuchaytirishni nazarda tutadi. Milliy rahbarlar, tushunarli, birinchi navbatda, ichki fikrlarni ta'kidlaydilar; shunga qaramay, samarali geosiyosat xalqaro ishlar ichki qarorlarni qabul qilishda hisobga olinsa,

milliy manfaatlar sezilarli darajada oshishini taklif qiladi. Birgalikda, puxta geosiyosat tahlili milliy davlatlar va korporatsiyalar o'rtasidagi munosabatlarni va milliy davlat ichida korporatsiyani himoya qilish uchun burch mavjudligini o'z ichiga oladi. Bundan tashqari, xususan, muayyan milliy davlatlar va xalqaro hamjamiyat, umuman olganda, haqiqiy yoki qabul qilingan tahdidlar oldida suverenitet chegaralari bilan bog'liq dilemmalarga duch kelishmoqda.

Masalan: Eronning yadroviy dasturni ishlab chiqish majburiyatidan kelib chiqadigan muammolar xalqaro hamjamiyatni Eron suvereniteti va xalqaro aralashuv chegaralari bo'yicha alohida variantlarni ko'rib chiqishga majbur qildi. Xalqaro hamjamiyatning aksariyati yadroviy Eronning mintaqaviy va xalqaro miqyosdagi tahdidlarini tan oladi. Shunga qaramay, Eronga qurolli hujumdan chiqib ketish xavotirlari keng ko'lamli iqtisodiy va diplomatik sanktsiyalarni qo'llashga katta hissa qo'shdi, ularning samaradorligi ochiq savol.

Yadroviy Eron tahdidiga tegishli javobni aniqlashda xalqaro hamjamiyat harbiy choralar bo'yicha qo'shimcha noqulayliklarni namoyish etdi. Tushunarli bo'lsa-da, kengroq savol tug'iladi: xalqaro hamjamiyat Eronning yadro dasturini bajarishiga to'sqinlik qilmasligi kerak. Milliy rahbarlar qarorlarni qabul qilish jarayonida qanday ishtirok etishlari va hal qilishlari geosiyosatning amaliy bajarilishini tushunish uchun juda muhimdir.

Misol uchun, Shimoliy Koreya tomonidan amalga oshirilgan Sony-ga kiber hujumni ko'rib chiqishda uch xil mamlakat manfaatdor tomonlardir.

Kiberhujum an'anaviy urush harakatiga o'xshashmi yoki yo'qligini hal qilishni talab qiladi. An'anaviy urushda a shtati b shtatidagi jismoniy nishonlarga tanklar va samolyotlar bilan hujum qiladi, kiber hujum esa birinchi navbatda xususiy yoki davlat infratuzilmasiga qilingan hujumdir. Hujumning oqibatlari jismoniy hujumdan tashqariga chiqishi mumkin: ehtimol tarmoq yoki tizimni o'chirib qo'yish ta'siri, hatto shaxslar o'ldirilgan taqdirda ham, ma'lum bir binoga zarar etkazmaydi. Shunday qilib, korporatsiyalarning zaifligi va ularning milliy davlatga bo'lgan munosabati o'z korporatsiyalari uchun milliy davlatlar oldidagi majburiyatning kuchayganligini tan oladi.

Kiber hujumning sezilarli ta'siri va uning zaifligi tahdidlar, o'zini himoya qilish va javoblar doirasi va chegaralarini o'z ichiga olgan asosiy tamoyillarni qayta tiklashni oqlaydi. Geosiyosat kontekstidagi eng muhim savollardan biri bu kiberhujum jismoniy javobni oqlaydimi; agar qayta

tuzilgan bo'lsa, milliy davlat kiberhujum uchun javobgar bo'lgan xaker-davlat yoki shaxsga jismoniy hujum qilishi mumkinmi.

Geosiyosat, kiberxavfsizlik va o'zini himoya qilishning birlashuvini hisobga olgan holda, kiber hujum shaxslar, korporatsiyalar va milliy davlat uchun xavf tug'diradi. Garchi bu o'zini himoya qilishni qonuniylashtirsa-da, bu savol mutanosiblikdir. BMT Nizomining 51-moddasiga binoan, milliy davlat hujumga uchraganidan keyin o'zini himoya qilish bilan shug'ullanish huquqiga ega:

“Xavfsizlik Kengashi xalqaro tinchlik va xavfsizlikni ta'minlash uchun zarur choralarni ko'rmaguncha, Birlashgan Millatlar tashkiloti a'zosiga qarshi qurolli hujum sodir bo'lsa, ushbu Nizomda hech narsa shaxsning yoki jamoaviy o'zini himoya qilish huquqini buzmaydi. O'zini himoya qilish huquqini amalga oshirishda a'zolar tomonidan ko'rilgan choralar darhol xavfsizlik Kengashiga xabar qilinadi va ushbu Nizomga muvofiq xavfsizlik Kengashining vakolati va javobgarligiga hech qanday ta'sir ko'rsatmaydi. xalqaro tinchlikni saqlash yoki tiklash uchun zarur deb hisoblagan har qanday vaqtda va xavfsizlik”.

Birlashgan Millatlar tashkiloti tashkil etilganda, ikkinchi Jahon urushidan so'ng, milliy davlatlar asosan nodavlat aktyorlar va terroristik tashkilotlar bilan ziddiyatga ega emas edilar. Biroq, keyingi o'n yilliklarda mojaro millat davlatlaridan kelib chiqib, millat davlatlariga qarshi bo'lgan millat davlatlariga qarshi chiqdi. Shunga ko'ra, muvaffaqiyatli kiberhujumdan so'ng tergovning muhim nuqtasi mas'ul tomonning o'z nomidan yoki milliy davlatning nomidan harakat qiladigan milliy davlat yoki nodavlat aktyor ekanligini aniqlashdir.

Davlatning kiberhujumga qanday va qachon munosabatda bo'lishini belgilaydigan to'rt xil variant mavjud.

Variant 1: o'z nomidan harakat a nonstate aktyor: tajovuzkor bir tug'diradi, agar darhol yoki kelajakdagi tahdid shundan keyin milliy davlat ushbu shaxsni quyidagicha belgilashi mumkin qonuniy maqsad. Kelajakdagi tahdidni aniqlash etarli aqlni talab qiladi bu milliy davlatning ushbu shaxsni “jalb qilish” qarorini oqlaydi.

Variant 2: millat nomidan proksi (kanal) vazifasini bajaruvchi nodavlat aktyor-davlat: hujum qilingan davlat-davlat qonuniy maqsad-bu nodavlat aktyor yoki uning nomidan milliy davlat hujumni nodavlat aktyor amalga oshirdi.

Variant 3: kiberhujum bilan shug'ullanadigan milliy davlat: agar milliy davlat shug'ullansa kiberhujum bilan shug'ullanadi bu urush harakati va javob sifatida qaralishi mumkin milliy davlat BMT

ko'rsatmalariga muvofiq harakat qilishi kerak.

Variant 4: boshqa milliy davlat nomidan vakil (o'tkazgich) vazifasini bajaradigan milliy davlat.

Yuqorida sanab o'tilgan variantlar bilan, variantlar qanday tushunishimiz uchun har bir variantni haqiqiy hayot sharoitida qo'llash foydali bo'ladi. 1-variant o'z nomidan bajaruvchi bir nodavlat aktyor aratilgan. Bu korporatsiya, Sony, boshqa mamlakatga qarshi kiber hujumni amalga oshirganida sodir bo'ladi. Bu biz Shimoliy Koreyada yoki Sony buzilishida muhokama qilgan vaziyatdan rolning o'zgarishi. Biroq, bu haqda o'ylash muhim ahamiyatga ega. Agar Sony Shimoliy Koreyaga qarshi kiber hujumni amalga oshirgan bo'lsa, ular qonuniy tahdid deb hisoblanadimi va shu bilan Shimoliy Koreyaga BMT Nizomiga muvofiq o'zini himoya qilishga imkon beradimi? Shimoliy Koreya Sony-ni jalb qilish qarorini oqlaydigan etarli aqlga ega bo'lishi kerak, ammo agar ular bunday aqlga ega bo'lsa, o'zini himoya qilish harakati o'rinli bo'ladi.

2-variant milliy davlat nomidan proksi (kanal) vazifasini bajaruvchi nodavlat aktyorga qaratilgan. Misol uchun, Agar Apple AQSh hukumati rahbarligi ostida harakat qilsa, Xitoyda minglab foydalanuvchi telefonlariga kirsa. Xitoy o'z-o'zini himoya bahs BMT Nizomiga muvofiq, Amerika qo'shma Shtatlari qarshi qasos mumkin. Xitoy maqsad Apple yoki AQSh hukumatida oqlanganligini aniqlashi kerak edi. Buning uchun 1-variantda talab qilinganidek, etarli aql va tegishli, qonuniy maqsad kimligini aniqlash uchun qo'shimcha echish kerak.

3-variant kiberhujum bilan shug'ullanadigan haqiqiy milliy davlatga qaratilgan. Ushbu stsenariy hujum qilingan davlat o'zini himoya qilish niqobi ostida boshqa milliy davlatni jalb qilishi mumkinligini aniqlashda eng oson ko'rinadi. Agar haqiqiy milliy davlat kiberhujumga duch kelsa, ehtimol u urush harakati sifatida qaralishi mumkin va hujum qilingan davlat BMT ko'rsatmalariga muvofiq harakat qilishi mumkin.

Yakuniy variant, 4-variant, agar milliy davlat boshqa milliy davlat uchun proksi-server yoki kanal vazifasini bajarayotgan bo'lsa, paradigmani muhokama qiladi. Misol uchun, AQSh Ukrainaga qarshi harakat qilib, Rossiyaga qarshi kiber hujumni amalga oshirdi. Yoki BMT Nizomiga binoan Ukrainaga qarshi qaytish hujumini amalga oshirish kerakmi, chunki AQSh Ukraina uchun harakat qilar edi. Bu qiyinroq savol tug'diradi va barcha variantlar singari, o'zini himoya qilishning har qanday shakli bilan shug'ullanishdan oldin etarli aqlni talab qiladi.

Masalan-kiberxavfsizlik sohasida bo'lmasa ham: bir necha yil oldin Isroildagi terakt begunoh odamlarning hayotiga Zomin bo'ldi; hujum

uchun mas'ul tashkilot Suriyada joylashganligi aniqlandi. Isroil havo kuchlari (IAF) terroristik tashkilotlarning Suriyadagi o'quv bazalariga hujum qilgan bo'lsa-da, Isroil rasmiylari na Suriya, na Suriya suvereniteti mo'ljallangan maqsad emasligini da'vo qilishdi. Terroristik tashkilot o'z-o'zidan harakat qilganmi yoki Suriya yoki Eron uchun kanal sifatida harakat qilganmi, muhim tekshiruv nuqtasi. O'quv bazasiga hujum qilish to'g'risidagi qaror Suriya yoki Eronning mumkin bo'lgan roli haqidagi katta savolni chetlab o'tganligini ko'rsatmoqda. Shunga qaramay, murakkab geosiyosiy tahlil qarshi hujum uchun qonuniy maqsadning shaxsini eng aniq baholash uchun milliy-davlat va nodavlat aktyor o'rtasidagi munosabatlarni aniqlashni talab qiladi.

Suriya suvereniteti aniq IAF tomonidan Suriya havo buzilishi tomonidan buzilgan edi, bu argument eng yaxshi soxta paydo bo'lardi.

Aksincha, Iafning Suriyaning yadroviy qobiliyatini rivojlantirish bo'yicha sa'y-harakatlari uchun muhim ahamiyatga ega bo'lgan ob'ektga hujumi, avvalgi reyd terroristik bazalarga (Suriyada joylashgan) qaratilgan bo'lsa, ikkinchisi hujum Suriyaning aniq maqsadlariga qaratilgan edi. Shunga qaramay, ikkala hujum ham Suriya suverenitetini buzdi; terrorizm yoki aksilterrorizm milliy davlat mo'ljallangan maqsad bo'lmaganida milliy-davlat suverenitetini buzishni oqlaydimi degan savol tug'iladi.

Shimoliy Koreyaning Sony - ga hujumi: agar nodavlat aktyor (X guruhi) hujumni Shimoliy Koreya nomidan sodir etgan bo'lsa, Qo'shma Shtatlar hujum uchun kim javobgarligini aniqlashda quyidagi muammolarni hal qilishi kerak edi: X guruhi hujum uchun javobgardir va agar razvedka hamjamiyati ushbu aktyorlarni aniqlay oladimi yoki ular qonuniy maqsadmi.

Agar Qo'shma Shtatlar Shimoliy Koreyani Sony-ga qilingan hujum uchun javobgar deb hisoblasa, Shimoliy Koreyaga hujum qilish to'g'risida qaror Sony Pictures-ga hujumni aniqlashni talab qiladi, bu Qo'shma Shtatlarga hujum qilishga o'xshaydi. Biroq, geosiyosiy va harbiy haqiqatlar x guruhiga hujum qilish Shimoliy Koreyani nishonga olishdan farq qiladi. Garchi Sony, shubhasiz, o'zining intellektual mulkiga hujum qiladigan muhim va muhim korporatsiya bo'lsa-da, bu Amerika fuqarolik maqsadlariga qarshi jismoniy terrorizm harakatini sodir etishga teng kelmaydi. Ta'kidlash joizki, avvalgi loyihani o'qigan o'quvchi bu taklifga qo'shilmaydi va korporatsiyaga qilingan hujum milliy davlatga qilingan hujumga teng, chunki korporatsiyalar milliy davlatlar uchun juda muhimdir. Kiber terrorizm, an'anaviy terrorizm va an'anaviy urush

o'rtasidagi farqlar keyinchalik berilgan savollar bilan ta'kidlangan.

Oldingi misollardan ko'rinib turibdiki, an'anaviy terrorizm bilan ham, Shimoliy Koreya yoki Sony misolida ham qonuniy maqsadni aniqlash ko'pincha eng bahsli masala hisoblanadi. Biroq, bu nafaqat eng bahsli, balki eng muhim hisoblanadi. Javob berish va mutanosib ravishda javob berish uchun bu javob qonuniy maqsadga qarshi qaratilgan bo'lishi kerak. Keling, qonuniy maqsad nima ekanligini muhokama qilishni davom ettirish uchun quyidagi misollarni ko'rib chiqaylik.

Quyidagilarni ko'rib chiqing: siz tez-tez ish uchun sayohat qilasiz; bu hafta siz Vashington Dalles aeroportida o'tirasiz va aeroportning bepul xizmatiga kirasiz. Bu so'nggi bir necha yil ichida ko'plab aeroportlar amalga oshirgan imtiyozdir va ko'plab sayohatchilar nafaqat tez-tez kirishadi, balki ular bundan katta foyda ko'rishadi. Ko'pgina sayohatchilar bu vaqtni ish bilan shug'ullanish, yozishmalarga javob berish yoki Netflix-dagi sevimli shousining so'nggi qismini tomosha qilish uchun ishlatishadi.

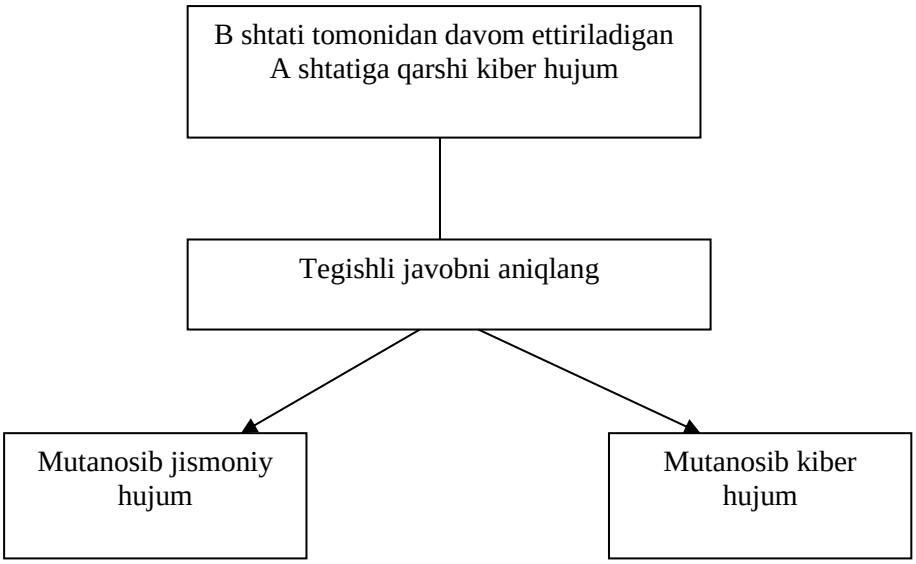
Biroq, ko'plab ekspertlarning ta'kidlashicha, bepul zonalar kiber xakerlar uchun issiq cho'ntaklar. Aytishlaricha, bepul kirish orqali siz bir vaqtning o'zida old eshikni ochasiz va kiberhujumchilarga kompyuter tizimingizga kirishga ruxsat berasiz. Endi tasavvur qiling-a, kiberhujumchi sizning ma'lumotlaringizga Vashington Dalles aeroportidagi bepul xizmat orqali kirib, o'zlarining ish ofislarida o'zlarining ish kompyuterlari orqali kirishmoqda.

Qonuniy maqsadni nafaqat oldingi misol uchun, balki kiberhujumchini aniqlay olmaslik uchun ham aniqlash qiyin. Quyidagilarni ko'rib chiqing. Tasavvur qiling-a, siz shaxsni o'g'irlash qurboni bo'lasiz. Kitobning keyingi misollarida ko'rinib turganidek, bu Qo'shma Shtatlarda juda keng tarqalgan muammo, chunki jismoniy shaxslar boshqasining ijtimoiy sug'urta raqamini o'g'irlashadi va bu ma'lumotlardan kredit kartalari, bank hisob raqamlarini ochish, kredit olish va o'z shaxsini to'liq ishlatish uchun foydalanadilar.

Bu sodir bo'lgandan keyin qiyinchilik kompensatsiyada. Sizning ma'lumotlaringiz A orqali buzilganligini tasavvur qiling kiberxavfsizlik hujumi qarshi qaratilgan maqsad, mashhur idoraviy do'kon. So'nggi bir necha yil ichida Target kiberxavfsizlik buzilishi qurboni bo'ldi, natijada 70 million kishi kredit karta maxfiyligini xakerlar uchun yo'qotdi.

Sony-ga qilingan hujumga Amerikaning javobi kiber qarshi hujum edi, ishonchli manbalarga ko'ra, hujum kamida ikki kun davomida Shimoliy Koreyaning Internet infratuzilmasiga ikki marta ta'sir

ko'rsatgan. Shunday qilib, kiber hujumga javob, dastlabki hujum uchun javobgar shaxsni jismoniy nishonga olish emas, balki kiber qarshi hujum bo'ladi. Bu model, an'anaviy operatsion aksilterror javob farq, bu kiber o'z-o'zini mudofaa va an'anaviy o'z-o'zini mudofaa o'rtasidagi farqlarni yoritgan uchun muhim geosiyosiy oqibatlarga ega.



3.1-rasm. Javob variantlari

Terroristik hujum uchun javobgar shaxsni nishonga olish o'rniga, kiber terrorizmga qarshi kurash hujum qiluvchi tashkilot yoki davlatning infratuzilmasiga qaratilgan.

Agar maqsad korporatsiya bo'lsa, unda milliy davlatning Internet infratuzilmasiga hujum qilish nomutanosibdir; bunday qarshi hujum kasalxonalarga, suv tizimlariga va transport turlariga sezilarli ta'sir ko'rsatish qobiliyatiga ega. Geosiyosat kontekstida bunday qarshi hujum anteni xavfli ravishda ko'taradi. Xalqaro huquq kontekstida bu nomutanosib javobni taklif qiladi. Shunga qaramay, milliy davlat javob berish huquqiga va majburiyatiga ega: savol kiberhujumga javob berishning toqatli chegaralari nimada. Geosiyosat va xalqaro huquqning konturlari strategik va huquqiy cheklovlar qarorlarni qabul qilish jarayoniga xos ekanligini ko'rsatadi.

Kengroq, geosiyosiy mulohazalarning sezgirligini aks ettiruvchi uchta mumkin bo'lgan javob mavjud: infratuzilmaga jiddiy zarar etkazadigan Shimoliy Koreyaning maqsadlariga to'g'ridan-to'g'ri hujum

qilish, cheklangan infratuzilma shikastlanishi bilan xabar yuborish yoki Shimoliy Koreyaga to'g'ridan-to'g'ri emas, balki Shimoliy Koreyaning sho'ba korxonasi yoki kanaliga hujum qilish.

Shimoliy Koreyaning nishonlariga to'g'ridan-to'g'ri hujum qilish, infratuzilmaga katta zarar etkazish. Ushbu stsenariyda Amerika Shimoliy Koreyaning asosiy infratuzilmasiga qarshi kiber hujumni boshlaydi. Bunga elektr tarmoqlari, suv tizimi, transport vositalarini boshqarish (samolyotlar yoki avtoulovlar uchun) va Shimoliy Koreya aholisining kundalik hayotiga katta ta'sir ko'rsatadigan bir qator boshqa variantlar kirishi mumkin. Shunday qilib, ta'sir aniq shaxslarga qaratilgan cheklangan jismoniy qarshi hujumga qaraganda sezilarli bo'ladi.

Shimoliy Koreyaga qarshi qarshi hujumdan chalg'itadi va Shimoliy Koreyaning subsid-iary yoki kanaliga qarshi qarshi hujumga qaratilgan. Ushbu stsenariyda Qo'shma Shtatlar Sony nomidan harakat qilmoqda. Umuman olganda, Shimoliy Koreya Qo'shma Shtatlardan keyin kelmadi, aksincha ular Sony-dan keyin kelishdi. Shunday qilib, Qo'shma Shtatlar bunday harakatga javoban Sony nomidan amalga oshiriladi. Shuning uchun, uchinchi variant Qo'shma Shtatlar Shimoliy Koreyaning Sony singari shunga o'xshash sho'ba korxonasi yoki kanaldan keyin borishni o'z ichiga oladi. Bu ikkinchi variantdan shunga o'xshash savollarni tug'diradi. Umuman olganda, ushbu parametr tartibga solish qiyin bo'lgan bir qator variantlarni yaratadi.

STUXNET

Ishonchli manbalarga ko'ra, Eronning yadroviy inshootiga Stuxnet nomli juda murakkab kompyuter virusi hujum qilgan. Aksariyat ekspertlarning ta'kidlashicha, virus Isroil yoki AQSh tomonidan kiritilgan.

Eronning yangi paydo bo'lgan atom sanoati Amerika va Isroil keng dunyo uchun xavf tug'diradimi yoki yo'qligini aniqlashni talab qiladi. Ushbu satrlar yozilgach, Eronning yadroviy qobiliyati bo'yicha murakkab muzokaralar olib borilmoqda. Muzokaralar, ularning natijalaridan qat'i nazar, Eronning tahdidiga tezkor javob berishga oid xalqaro huquq va geosiyosat masalalarini hal qilmaydi. O'tgan yillar davomida Eron rahbarlari bir necha bor Isroilga yadroviy qurol bilan hujum qilish bilan tahdid qilishgan.

Bosh vazir Netanyaxuning aniq ogohlantirishicha, Isroil dunyo rahbarlarini oldindan ishonch hosil qilishdan tortinmaydi va Eronning yadroviy imkoniyatlarini cheklash bo'yicha muzokaralar olib borish juda muhim edi. Xalqaro huquq nuqtai nazaridan Netanyaxuning

ogohlantirishining asosi Isroilning o'zini himoya qilish huquqi edi. Netanyaxu 51-moddaga tayangan bo'lsa-da, muzokaralar uchun asos tahdidlar va ogohlantirishlar haqiqiy samara berishi va shu bilan bevosita mintaqaga va katta xalqaro hamjamiyatga sezilarli ta'sir ko'rsatishi haqidagi xavotirni aks ettiradi.

Samarali geosiyosat inqirozni boshqarish va zararni nazorat qilish sharoitida tahdidni o'z ichiga olish muhimligini ko'rsatadi. Biroq, mintaqaviy barqarorlik favqulodda ahamiyatga ega bo'lsa-da, milliy rahbariyatning asosiy majburiyati uning tinch aholisining xavfsizligi va farovonligidir. Demak, milliy xavfsizlik o'rtasida muayyan davlatlar tomonidan belgilanadigan va amalga oshiriladigan tabiiy keskinlik va ma'lum bir milliy davlatdan tashqariga chiqadigan kengroq mintaqaviy va xalqaro manfaatlar mavjud. Kiber bu keskinlikni sezilarli darajada yoritadi:

“Kiberxavfsizlik masalasi AQSh–Xitoy munosabatlarida katta ahamiyatga ega bo'lsa-da, uni hal qilish uchun qadamlar tabiatda ibtidoiy bo'lib qolmoqda. 13 yil 2013 aprelda AQSh Davlat kotibi jon Kerri ikki tomon kiberxavfsizlik bo'yicha ishchi guruh tuzishga kelishib olganini e'lon qildi. Bir hafta o'tgach, AQSh raisi Bosh shtab boshliqlari General Martin Dempsi Xitoy generali Fang Fenghui bilan qo'shma konferentsiya chaqirdi, u AQSh bilan ishlashga va'da berdi, chunki yirik kiberhujumning oqibatlari yadroviy bomba kabi jiddiy bo'lishi mumkin. Xalq Ozodlik armiyasi Bosh shtabi boshlig'i va Markaziy harbiy komissiya a'zosi General Fang, taraqqiyot tez bo'lmasligi mumkinligi haqidagi ogohlantirish bilan kiberxavfsizlik mexanizmini o'rnatishga tayyorligini ta'kidladi”.

Etakchi mutaxassislar bilan suhbatlar Stuxnetning murakkabligi va murakkabligiga oydinlik kiritdi. Biroq, kompyuter virusining texnik jihatlari bizning ixtiyorimizdan tashqarida; kiber mojaroning tabiati qiziqish uyg'otadi. Shu nuqtai nazardan, Stuxnetning ta'sirchan texnologiyasi muhim e'tiborni jalb qilgan bo'lsa-da, kengroq so'rov uning asoslari va oqibatlariga qaratilgan. Shu nuqtai nazardan, Isroil Mudofaa kuchlari (IDF) shtab boshlig'i podpolkovnik tomonidan qabul qilingan qaror. General Gadi Eizenkot, kiber filialni tashkil etish uchun kiber urush va terrorizm tahdidlari va xavf-xatarlarini aks ettiradi. Filial kiber urush-terrorizm xavfsizligining keskin rivojlangan strategik ahamiyatini aks ettiruvchi mudofaa va hujum qobiliyatlarini birlashtiradi.

Hujum-mudofaa qobiliyatining kombinatsiyasi, mutanosiblikning xalqaro huquq printsipi kontekstida, agar maqsad hayotiy xavf tug'dirsa,

milliy davlatning kompyuter tizimiga hujum qilish o'zini himoya qilishning qonuniy shakli ekanligini ko'rsatadi. Ogohlantirish: kompyuter virusi va boshqa qo'shimcha choralarning ta'siri sezilgan tahdidni keltirib chiqaradigan maqsadga qaratilgan. Eronga kelsak, kompyuter virusini joriy etish, agar o'zini himoya qilish chorasi tajovuzkor va tajovuzkor maqsadlarda ishlatilishi mumkin bo'lgan atom sanoatiga tegishli bo'lsa, mutanosiblikni aks ettiradi.

“Kiber hujumni harbiy qarorlarni qabul qilish kontekstida qo'yish kiber hujumlardan foydalanishga ta'sir qiladi. Millatlar Stuxnetdan keyin AQSh yoki uning ittifoqchilariga qarshi jismoniy zarar etkazadigan kiber hujumni boshlash ehtimoli ko'proq emas va ular josuslik va siyosiy majburlash uchun kiber texnikalardan foydalanishni to'xtatmaydilar. Biz ushbu qobiliyatga ega bo'lgan mamlakatlardan AQSh va uning ittifoqchilariga qarshi zarar, vayronagarchilik yoki qurbonlarga (josuslik va jinoyatchilikdan farqli o'laroq) olib kelishi mumkin bo'lgan jismoniy zararli hujumlarni ko'rmadik, chunki ular zo'ravonlik bilan javob berish xavfini juda yuqori deb baholaydilar. Bu ularni AQShga qarshi samolyotlar yoki raketalarni uchirishdan saqlaydigan bir xil fikrdir, ammo xalqaro amaliyot va qonun josuslik va jinoyatchilikka javoban kuch ishlatishni oqlamaydi, zo'ravonlik bilan javob berish xavfini kichik va maqbul qiladi.

Stuxnet dizaynerlarining kreditiga garovga zarar etkazmaslik uchun ehtiyotkorlik bilan yozilgan. Boshqa tajovuzkorlar unchalik ehtiyot bo'lmasliklari mumkin, ammo bu Stuxnet kodiga kirish bilan hech qanday aloqasi yo'q. Potentsial raqiblar hali ham AQShga qarshi kuch ishlatish to'g'risida qaror qabul qilishda foyda va xavfning bir xil hisob-kitoblaridan o'tmoqdalar va ular nafaqat kiberhujum emas, balki barcha harbiy aktivlardan foydalangan holda AQShning harbiy javobi bilan to'sqinlik qilmoqdalar. Endi ular stuxnetni har qanday ommaviy hujumni oqlashning bir qismi sifatida keltirishlari mumkin, ammo bu ularning qaror qabul qilishining bir qismi emas, balki bahona bo'ladi. Xalqlar Stuxnetdan keyin AQSh yoki uning ittifoqchilariga qarshi kiberhujum uyushtirish ehtimoli ko'proq emas.

AQShning Stuxnetdagi ishtiroki darajasi noaniq bo'lsa-da, AQSh milliy xavfsizligining keng ifodasi Eron atom kuchiga aylanishi bilan Amerikaning muhim manfaatlariga ta'sir ko'rsatishini ko'rsatmoqda. To'g'ridan—to'g'ri va ehtimol keskin ravishda Isroil milliy rahbarlari doimiy ravishda yadroviy Eron Isroil xavfsizligiga ekzistensial tahdid soladi, deb ta'kidlamoqda. Ochiq savol bo'lsa-da, intensiv munozaralar va

turli xil fikrlar bilan bog'liq bo'lsa-da, Stuxnetning joriy etilishi kiber, geosiyosat va o'zini himoya qilish o'rtasidagi munosabatlarning operatsion oqibatlarini aniq ko'rsatib beradi.

Ogohlantirish sezilgan tahdidni ta'kidlaydi. Keyin qo'shimcha savol tug'iladi: qabul qilingan tahdidni qanday aniqlash mumkin? Tahdid sifatida qabul qilinishi mumkin bo'lgan ko'p narsalar mavjud, ammo agar mamlakatlar tahdid sifatida qabul qilinishi mumkin bo'lgan har qanday narsaga munosabat bildirsa, ularda vaqt va pul tugaydi.

Kompyuter virusi haqiqatan ham qabul qilingan tahdid bilan tahdid qilinishini ta'minlash mumkin. Bundan tashqari, savol tug'iladi, kompyuter virusiga kirish va uni amalga oshirish uchun zarur bo'lgan texnologiya va ma'lumotlarga kirish mumkinmi, bu tahdidni sezishi mumkin va aslida aytilgan tahdidni yaxshilashi mumkinmi? Biz doimo moslashadigan va rivojlanayotgan texnologik dunyoda yashayapmiz va uning ustida qolish tirishqoqlik va pulni talab qiladi. Ko'pincha, kerakli kompyuter virusi yoki texnikasini bajarishga qodir bo'lganlar bir nechta odamlarga torayadi.

Nazorat savollari.

1. AQSh federal hukumati kiberxavfsizlik siyosatini qanday belgilab bergan?
2. Kongress kiberxavfsizlik siyosatini shakllantirishda qanday ahamiyatga ega?
3. Internet jinoyatlari kiberxavfsizlikni qanday ta'minlaydi?
4. Xalqaro axborot xavfsizligini ta'minlash to'g'risidagi konventsiya qachon va qayerda o'tkazilgan?
5. Xalqaro axborot xavfsizligi sohasida qaysi asosiy tahdidlar ko'rib chiqiladi?
6. Xalqaro axborot xavfsizligini ta'minlashning asosiy tamoyillari nimalar?
7. Xalqaro axborot xavfsizligi sohasida ishtirokchi davlatlar o'rtasida qaysi muhim tamoyillar mavjud?
8. Ishtirokchi davlatlar xalqaro axborot xavfsizligini ta'minlashda qaysi asosiy omillarni ko'zda tutadilar?
9. Xalqaro axborot xavfsizligi sohasida tajovuzlar va “axborot urushi”ni oldini olish uchun qanday chora-tadbirlar olib boriladi?
10. Xalqaro axborot xavfsizligi sohasidagi davlat siyosati bo'yicha Rossiya Federatsiyasining tutgan qadam va o'tkazgan reformalar nimalardir?
11. Kiberxavfsizlik siyosati tuzish jarayonida qaysi bosqichlar

bo'ladi?

12. Kiberxavfsizlik siyosati tuzish jarayonida amalga oshiriladigan audittan nimalar aniqlanadi?

13. Kiberxavfsizlik siyosati tuzish jarayonida siyosat loyihasi qanday tuziladi?

14. Kiberxavfsizlik siyosati tuzish jarayonida siyosatning muvofiqlashtirilishi va amalga oshirilishi uchun nimalar kerak?

15. Kiberxavfsizlik siyosati tuzish jarayonida siyosatning yangilanishi qachon kerak?

16. Kiberxavfsizlik siyosati tuzish jarayonida qanday tekshiruvlar o'tkaziladi?

17. Kiberxavfsizlik siyosati tuzish jarayonida ichki va tashqi audit qanday amalga oshiriladi?

18. Axborot xavfsizligi siyosati chiqarish jarayonida qaysi bosqichlar bo'ladi?

19. Kiberxavfsizlik va geosiyosatga oid qanday misollar mavjud?

20. Kiberxavfsizlik va geosiyosat o'rtasidagi munosabatlarni baholashda qanday o'zgaruvchilar muhimdir?

21. Kiberxavfsizlik va geosiyosat o'rtasidagi munosabatlarda milliy davlatlar qanday javob berishlari kerak?

22. Kiberxavfsizlik va geosiyosat o'rtasidagi munosabatlarda qanday jarayonlar amalga oshirilishi kerak?

IV BOB. KIBERXAVFSIZLIK SIYOSATINI AMALGA OSHIRISH

4.1-§. Kiberxavfsizlik siyosatini amalga oshirish va rivojlantirish

Axborot xavfsizligi siyosatini shakllantirish va ulardan foydalanish keng tarqalgan bo'lib qo'llanilishiga va tashkilotlar axborot xavfsizligini boshqarishga katta resurslarni sarflashiga qaramay, xavfsizlik siyosatini samarali va maqsadli ishlab chiqish hamon murakkabligicha qolmoqda. Masalan, siyosatlar chiqarilishi mumkin, lekin yangi tartibga soluvchi talablar yoki biznes jarayonlaridagi o'zgarishlarni o'z ichiga olishi uchun ko'rib chiqilmaydi, buning natijasida huquqiy mas'uliyat va eskirgan siyosatlar e'tibordan chetda qoladi. Ushbu mavzuning asosiy maqsadi barqarorlikni ta'minlaydigan axborot xavfsizligi siyosatini ishlab chiqish uchun yo'l xaritasini taqdim etishdir. Mavzu siyosatni ishlab chiqish usullari bo'yicha joriy adabiyotlarni o'rganadi va turli yondashuvlarni taqqoslaydi. Taqqoslash natijalariga ko'ra, Axborot xavfsizligi siyosatini ishlab chiqish hayotiy tsikli (ISP-DLC) taklif etiladi. Tavsiya etilgan hayot tsikli yondashuvi tashkilotning xavfsizlik siyosatining keng qamrovli, samarali va barqaror bo'lishini ta'minlaydi.

Bugungi kunda har qanday shakl va o'lchamdagi tashkilotlar, agar ular tobora kuchayib borayotgan raqobat muhitida omon qolish va yaxshiroq rivojlanishni xohlasalar, axborot tizimlari va texnologiyalarini ishtiyoq bilan qabul qilishlari kerak. Binobarin, tashkiliy axborot tizimlariga kiritilgan ma'lumotlarning yaxlitligi, maxfiyligi va mavjudligini ta'minlash uchun xavfsizlik nazoratini joriy etish juda muhimdir.

Tashkilot o'z axborot aktivlarini himoya qilishga to'g'ri yondashuvga ega bo'lishi uchun unga yaxshi rejalashtirilgan va samarali axborot xavfsizligi siyosati kerak. Siyosatni "maksadga muvofiq deb topilgan harakat yo'nalishi, asosiy tamoyil yoki protsedura" yoki "sug'urta guvohnomasi" sifatida belgilash mumkin. Ushbu ta'rifdan foydalanib, siyosat deganda, birinchidan, amalga oshirilishi kerak bo'lgan harakat yoki amal qilinishi kerak bo'lgan protsedura, ikkinchidan, berilishi mumkin bo'lgan bayonot yoki deklaratsiya nazarda tutilishini ta'kidlaydi. Demak, agar protsedura to'g'ri bajarilgan bo'lsa, unda "sug'urta guvohnomasi" buzilmagan bo'lishi kerak bo'ladi, aynan shundagina tashkilot o'z maqsad va vazifalariga javob bera oladi.

Samarali xavfsizlik siyosatini amalga oshirish, ayniqsa, axborot xavfsizligini boshqarish sohasida muhim ahamiyatga ega. Axloqiy jihat

shundaki, texnik nazorat qanchalik kuchli bo’lmasin, xavfsizlik har doim tashkilot ichidagi odamlarga bog’liq. Axborot xavfsizligi dasturida insonlar ko’pincha eng zaif bo’g’in deb ataladi. Biroq, agar axborot xavfsizligi buzilishi yoki hodisasi xabardor bo’lmagan yoki ehtiyotsiz xodimning harakatlari tufayli yuzaga kelsa, direktorlar kengashi va yuqori rahbariyat ushbu xodimning xatti-harakati uchun shaxsan javobgar bo’lishi mumkinligi ko’p xam e’tiborga olinmaydi. Shuning uchun inson omilini e’tiborsiz qoldirmaslik kerak. Tashkilot tegishli xavfsizlik choralariga ega bo’lishi uchun u o’z xodimlarining harakatlarini tartibga soluvchi hujjatlashtirilgan siyosatlarga muhtoj.

Ilmiy doiralar va amaliyotchilar hamjamiyatida axborot xavfsizligi siyosati tashkiliy kontekstda ishonchli xavfsizlik amaliyotlarini tarqatish va qo’llash uchun asos ekanligi to’g’risida tobora kuchayib borayotgan konsensus mavjud. Ular ta’kidlaganidek: Xech bo’lmaganda professional xavfsizlik mutaxassislari orasida rasmiy siyosat xavfsizlikning zaruriy sharti ekanligi ma’lum.

Ushbu mavzuda samarali axborot xavfsizligi siyosatiga ega bo’lishning ahamiyati va bunday siyosatlarni amalga oshirishdagi mumkin bo’lgan muammolar ko’rib chiqiladi. Axborot xavfsizligi siyosatini ishlab chiqishning beshta yondashuvi yoki usullari solishtiriladi. Taqqoslash natijalari axborot xavfsizligi siyosatini ishlab chiqishning hayotiy tsikli (ISP-DLC) yondashuviga kiritilgan. ISP-DLC ni ishlab chiqishdan maqsad axborot xavfsizligi siyosati joriy va o’zgaruvchan tashkilot ehtiyojlari va biznes maqsadlariga javob berishini va siyosatga muvofiqligini ta’minlash uchun vositalarni taqdim etishdan iborat. Bu haqiqatan ham keng qamrovli, samarali va barqaror axborot xavfsizligi siyosatiga olib keladi.

Samarali axborot xavfsizligi siyosatiga ega bo’lishning ahamiyati. Axborot xavfsizligi siyosati tashkilot ma’lumotlarini himoya qilish uchun nima qilish kerakligini belgilaydi. Xavfli muammolarni hal qilish uchun sifatli siyosatiga ega bo’lish tashkilotning umumiy xavfsizligini yaxshilash bilan bog’liq kengroq qamrovni ta’minlashi mumkin, shuningdek, siyosatlar tanqidiy ko’rib chiqilsa, huquqiy nuqtai nazardan ham foydali bo’lishi mumkin. Axborot xavfsizligi siyosati tashkilotning axborotni himoya qilish bo’yicha to’liq siyosatini belgilashi kerak. Odatda u yuqori darajadagi siyosat bayonotidan va qo’shimcha batafsil siyosiy hujjatlardan iborat. Siyosat tashkilotning huquqiy va me’yoriy talablarga rioya qilishi uchun zarur bo’lgan barcha choralarni o’z ichiga olishi kerak.

Xavfsizlik siyosati hujjatlarining ahamiyati shundan iboratki, agar operatsiyani shubha ostiga qo’yadigan axborot xavfsizligi hodisasi ro’y bersa, u kuchga kiradi, ya’ni real ishlashini ko’rsatib beradi.

Bundan tashqari, agar kompaniya uchun axborot xavfsizligi siyosatini ishlab chiqish va amalga oshirish majburiyati bo’lmasa ham, ixtiyoriy ishlab chiqilgan siyosat tashkilot uchun quyidagi sabablarga ko’ra foydali bo’ladi:

(i) Axborot xavfsizligi siyosati tashkilotning axborot aktivlarining qiymatini, haqiqiyligi, maxfiyligi va yaxlitligini himoya qilgan holda biznesni eng yaxshi olib borish yo’lini topishga undashga sabab bo’ladi;

(ii) Mutaxassislarning ta’kidlashicha, Internetdan foydalanish qonunchiligi hali ham juda chalkash bo’lgan bu davrda, axborot xavfsizligi siyosatiga ega korxonalar o’zlarini keraksiz bosh og’rig’idan himoya qilishlari mumkin bo’ladi.

Xalqaro miqyosda qabul qilinadigan standartlarni tan oladigan va ularga mos keladigan samarali axborot xavfsizligi siyosatiga ega bo’lgan kompaniyalar teskari yondashuvni qo’llaydigan kompaniyalarga nisbatan aniq ustunlikka ega bo’lishadi. Axborot xavfsizligi siyosatiga ega bo’lmagan yoki bunday siyosatga ega bo’lgan, lekin siyosat samarali amalga oshirilmagan kompaniyalar xakerlar, krakerlar va boshqa tahdid agentlarining hujumlari qurboni bo’lishlari mumkin. Bu oxir-oqibat mijozlar ishonchini va aktiv qiymatini yo’qotishiga olib keladi.

Axborot xavfsizligi siyosatiga nima uchun ehtiyoj borligini ko’rib chiqqandan so’ng, kompaniyalar (xususan, direktorlar kengashi), agar ular kompaniyaga samarali axborot xavfsizligi siyosati mavjud bo’lmagan holda ishlashiga imkon bersa, ehtiyotsiz, beparvo va mas’uliyatsiz deb nomlanishi mumkinligi aniq bo’lishi kerak. Bundan tashqari, oldingi muhokamadan ma’lum bo’lishi kerakki, bunday siyosatga ega bo’lishning muhim sababi direktorlar va yuqori boshqaruvga tegishli ehtiyotkorlik va sinchkovlik bo’yicha o’z majburiyatlarini bajarganliklarini sudda aniq dalillar bilan taqdim etishda yordam berishdir. Axborotni o’z qiymatiga ko’ra boshqarish va o’z axborot aktivlarining maxfiyligi, yaxlitligi va foydalanuvchanligini himoya qilish orqali tashkilotlar nafaqat o’zlarining qonuniy va me’yoriy talablariga javob berishi, balki biznesning muhim afzalliklarini ham amalga oshirishi mumkin.

Samarali axborot xavfsizligi siyosatini amalga oshirishdagi muammolar. Mavjud adabiyotlarda axborot xavfsizligi siyosatini ishlab chiqish asoslariga urg’u berilgan. Biroq, adabiyotda tasvirlangan usullar

qanchalik yaxshi amalga oshirilganligi aniq emas. Tadqiqotlar shuni ko’rsatdiki, bunday siyosatlarga ega bo’lgan kompaniyalar texnik xizmat ko’rsatish va siyosatlarga rioya qilishga etarlicha e’tibor bermaydilar. Shunday qilib, ko’pgina tashkilotlarda xavfsizlik siyosati davomli hayot-tsikliga ega bo’lmasligi tufayli uning faoliyati javonda tugaydi.

Xavfsizlik siyosatini ishlab chiqishda boshdan kechirgan qiyinchiliklar tufayli shakllangan mualliflar o’zlarining savollariga javob olish uchun ko’pincha boshqa tashkilotlarning siyosatlariga, tijoratda mavjud bo’lgan manbalarga yoki Internet kabi ommaviy manbalarda mavjud shablonlarga murojaat qilishadi. Ko’pincha, bunday yondashuvga rioya qilish zaruriyatiga ko’nikma va tushunchaning yetishmasligi sabab bo’ladi. Biroq, natijada olingan hujjat o’zi himoya qilishi kerak bo’lgan tashkilot kontekstida axborot xavfsizligi bo’yicha tegishli ko’rsatma bermaydi.

Samarali xavfsizlik siyosatini shakllantirish juda talabchan va murakkab faoliyat bo’lishi mumkin; shu sababli, mualliflar tashkilotlarning huquqiy va me’yoriy talablarga javob berishini ta’minlash va shu bilan birga, axborot xavfsizligini boshqarish bo’yicha eng yaxshi amaliyotlarni ta’minlash uchun ushbu muhim hujjatga nima kiritilishi kerakligi kabi savollar bilan kurashadi. Shunisi e’tiborga loyiqki, siyosatni shakllantirish faqat jarayonning boshlanishi. Texnik xizmat ko’rsatish va muvofiqlikni monitoring qilish ushbu dastlabki bosqichdan ko’ra muhimroqdir va odatda jarayonda qo’shimcha qiyinchiliklar sifatida namoyon bo’ladi. Siyosatlar tashkilotning biznes maqsadlarini qo’llab-quvvatlashi va kuchaytirishi kerak. Shu sababli, axborot xavfsizligi siyosatini shakllantirish, qabul qilish va amalga oshirish muammosini hal qilishni taklif qiladigan har qanday yechim ushbu bo’limda ta’kidlangan muammolarni hal qilishi kerak.

Mavjud xavfsizlik siyosatini ishlab chiqish usullari. Mavjud manbalarni ko’rib chiqish tashkilotlarning xususiy xavfsizlik siyosatini ishlab chiqishda foydalanishi mumkin bo’lgan bir qator yondashuvlar yoki usullarni ochib beradi. Bu yondashuvlar jadval formatida taqdim qilinadi, unda har bir manba tomonidan taklif qilingan bosqichlarni o’xshash jarayonning bir qismini tashkil etuvchi toifalarga guruhlashga harakat qilinadi. Masalan, 1-guruhga bo’lingan bosqichlar odatda siyosatni ishlab chiqishdan oldingi xavflarni baholash jarayoni bilan bog’liq. 2-guruh siyosatni qurish uchun zarur bo’lgan bosqichlar bilan shug’ullanadi, masalan, siyosat loyihasini ishlab chiqish. 3-guruh siyosatni amalga oshirish bosqichiga e’tibor qaratadi, 4-guruh esa

siyosatni monitoring qilish va saqlashga qaratilgan. 5-guruh menejment uchun asosiy rollarni ta’kidlaydi, 6-guruh esa umuman xodimlar uchun xuddi shunday jarayonni qo’llaydi. E’tibor bering, ma’lum bir manba tomonidan taklif qilingan qadamlarning raqamlanishi, ma’lum bir guruhdagi bosqichlarni toifalarga bo’lish talabi tufayli qadamlar jadvalda ketma-ket ko’rsatilmasa ham saqlanib qoladi.

Taqqoslash mualliflar bir xil qadamlar bo’yicha kelishib olgan ba’zi o’xshashliklarni ochib beradi, shuningdek, ma’lum bir muallif boshqalar muhim deb hisoblagan biron bir qadamni eslatmagan bo’shliqlarni ko’rsatadi. Masalan, DTI xavfni baholash guruhining bir qismi sifatida talab qilinadigan harakatlarni eslatmaydi, CTRG esa xavfni baholashni siyosatni qurish uchun biron bir qadam qo’yishdan oldin amalga oshiriladigan asosiy qadam deb hisoblaydi.

4.1-jadval

Axborot xavfsizligi siyosatini ishlab chiqish usullari

	Control Data	**CTRG (Computer Technology Research Group)**	**DTI**	**SANS Institute**	**Woodward**
1-Guruh **Risklarni baholash bosqichlari**	1. Mumkin bo’lgan tahdid va risklarni aniqlash	1.Qanday aktivlar himoyaga muhtojligini aniqlash			1. Riskni o’rganish
	2.Himoya qilinadigan aktivlarni aniqlash	2.Har bir aktiv uchun himoya darajasini aniqlash			
		3.Internetdan foydalanishni aniqlash			
		4.Mavjud tahdidlarni aniqlash			
		5. Aniqlangan tahdidlarni qanday hal qilishni o’rganish			

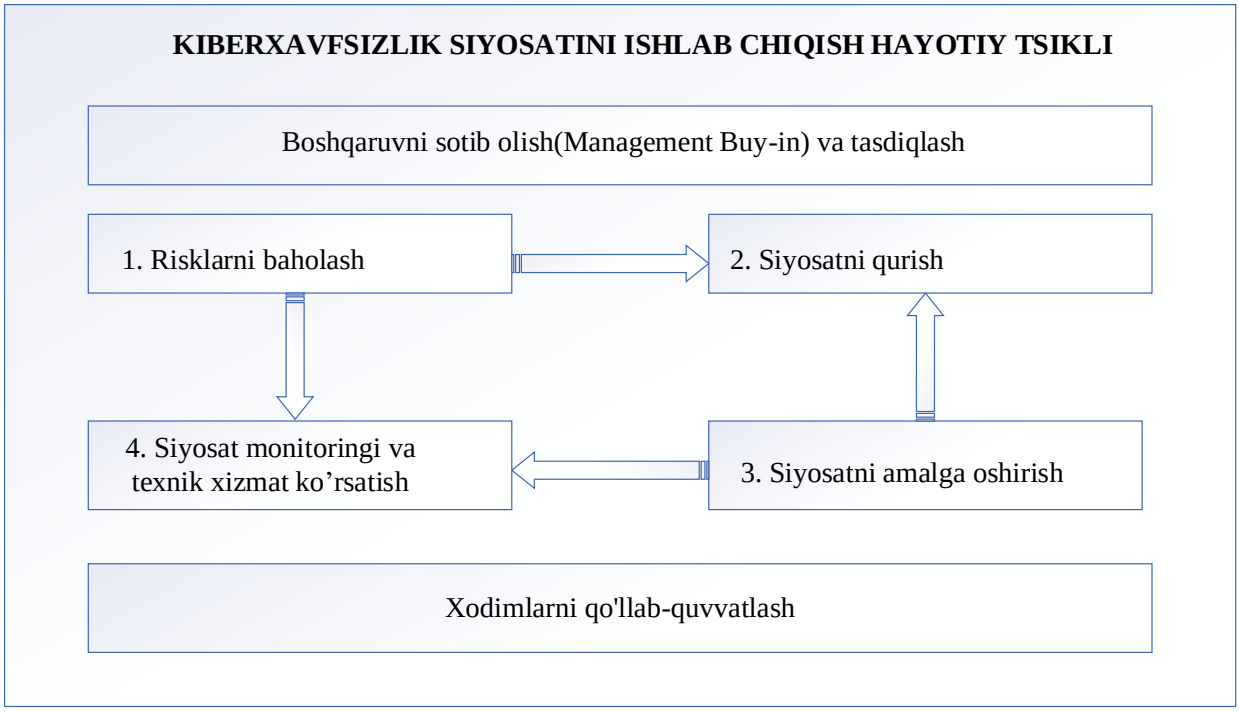
		6. Ta’sir darajasini baholashni o’tkazish			
2-Guruh Siyosat qurilishi bosqichlari		7. Xavfsizlik siyosati loyihasini tuzish	1.Siyosat mazmunini tadqiq qilish	1. Siyosatni yozish	2.Siyosatni shakllantirish
		9.Siyosatda qayta tiklash bo’limini qo’shish	2.Siyosat loyihasini ishlab chiqish		
3-Guruh Siyosatni amalga oshirish bosqichlari	3.Aktivlarni himoya qilish strategiyasini qo’llash	8. Amalga oshirish rejasini ishlab chiqish	3. Xodimlarga siyosat namunalarini berish	2. Siyosatni nashr qilish	3.Siyosatni amalga oshirish bo’yicha standartlarni ishlab chiqish
		10.Foydalanuvchilarni o’qitish			

4-Guruh Siyosat monitoringi va texnik xizmat ko'rsatish bosqichlari	4. Ishonchni ta'minlash uchun siyosatni sinab ko'rish		4. Monitoring va texnik xizmat ko'rsatish	3.Siyosatni qayta ko'rib chiqishni talab qilish	5. Ko'rib chiqish
5-Guruh Boshqaruvni sotib olish(Management Buy- in) va tasdiqlash bosqichlari			5.Boshqaruv rozilini olish		4. Rahbariyatdan hamkorlikni olish
6-Guruh Xodimlarni qo'llab-quvvatlash bosqichlari		11. Insidentlarga javob berish			

Yuqoridagi jadvaldan ko'rinib turibdiki, mualliflar xavfsizlik siyosati hujjatini ishlab chiqishning asosiy bosqichlarini taklif qilishadi. Yuqorida 1-jadvalda keltirilgan tahlildan olingan ma'lumotlar 1-rasmda ko'rsatilganidek, axborot xavfsizligi siyosatini ishlab chiqishning hayotiy tsikliga kompleks yondashuvni taklif qilish uchun jamlangan va to'ldirilgan. Ushbu maqsadga erishish uchun guruhlar toifalarga ajratilib berilgan. 1-jadvalda sanab o'tilgan qadamlar taklif qilingan Axborot xavfsizligi siyosatini ishlab chiqishning hayot tsiklini (ISP-DLC) yaratish bosqichlarini tashkil qilish uchun amalga oshiriladi. Masalan, 1-guruh (xavfni baholash) ISP-DLCning 1-bosqichiga aylanadi. Xuddi shu narsa ISP-DLCning 2-4 bosqichlariga aylangan 2-4-guruhlarga ham tegishli. Boshqaruv va umuman xodimlar rolini qamrab oluvchi 5 va 6-guruhlar

ISP-DLC fazalarining har biriga taalluqli deb hisoblanadi. Bosqichlarning har biri rahbariyat tomonidan ko’rsatma va xodimlarning yordamini talab qiladi. Shu sababli, boshqaruvni qo’lga olish va tasdiqlash va xodimlarni qo’llab-quvvatlash ISP-DLC ning barcha to’rtta bosqichini qamrab olgan gorizontal chiziqlar sifatida tasvirlangan. Axborot xavfsizligi siyosatini ishlab chiqishning taklif etilayotgan hayotiy tsikli keyinchalik keng qamrovli, samarali va barqaror axborot xavfsizligi siyosatini ta’minlash uchun tashkilotlar amal qilishi kerak bo’lgan yo’l xaritasi bo’lib xizmat qiladi. ISP-DLC keyinchalik batafsilroq muhokama qilinadi.

Kiberxavfsizlik siyosatini ishlab chiqish hayotiy tsikli (KXSIHT) yondashuvi. Taklif etilayotgan ISP-DLC to’rtta asosiy bosqichdan iborat: xavflarni baholash, siyosatni qurish, siyosatni amalga oshirish, siyosat monitoringi va texnik xizmat ko’rsatish. Har bir bosqichni har bir bosqichda sodir bo’ladigan harakatlar batafsil tavsiflangan bosqichlarga kengaytirilishi mumkin, chunki bundan keyin qisqacha muhokama qilinadi. Shuni yodda tutish kerakki, siyosatni ishlab chiqish iterativ va uzluksiz jarayondir. Texnologiya, ishbilarmonlik muhiti va qonuniy muvofiqlik talablaridagi o’zgarishlar tufayli siyosatni amalga oshirish bosqichi har doim ushbu o’zgarishlarni o’z ichiga olgan texnik xizmat ko’rsatish bosqichi va siyosat ko’rsatmalarining operativ bajarilishini ta’minlaydigan monitoring bosqichi (ya’ni, siyosatga muvofiqlik) bilan davom etadi.



4.1-rasm. Axborot xavfsizligi siyosatini ishlab chiqish hayotiy sikli

Boshqaruvni sotib olish va tasdiqlash ISP-DLC diagrammasining yuqori qismida tasvirlangan va barcha bosqichlarni muvaffaqiyatli siyosatni ishlab chiqish hayotiy tsiklining muhim tarkibiy qismi sifatida qamrab oladi. Yuqori boshqaruv oxir-oqibat tashkilot farovonligi uchun javobgardir. Ular odatda o'zlarining boshqaruv yordami va yo'nalishini aniqlash uchun siyosatdan foydalanadilar. Rahbariyat xavfsizlik siyosatini qo'llab-quvvatlamasa, ular mavjud bo'lmasligi ham mumkin. Ushbu siyosat barcha xodimlarga etkazilishi kerak. Xodimlar bilan hamkorlik qilish zarurati ISP-DLC diagrammasiga qo'llab-quvvatlovchi tarzda siyosatni ishlab chiqishning butun hayotiy tsiklini qamrab oluvchi gorizontal chiziq sifatida kiritilgan. Xodimlar tegishli darajadagi xavfsizlikni ta'minlash uchun shaxs sifatida nima qilishlari va qilmasliklari kerakligini bilishlari kerak. Shuning uchun siyosatni ishlab chiqishning butun hayoti davomida menejerlar va xodimlar o'rtasidagi aloqa strategiyasi zarur.

Rahbariyat va xodimlarning roli quyida har bir asosiy bosqichning kichik komponenti sifatida muhokama qilinayotgan muayyan bosqichga taalluqli masalalarni yoritish orqali batafsil muhokama qilinadi.

1-bosqich: Risklarni baholash. Risklarni baholash bosqichi tashkilot himoya qilmoqchi bo'lgan biznes aktivlarini aniqlaydi va quyidagi savollarni berish orqali ushbu aktivlarga potentsial tahdidlarni ko'rib chiqadi:

- Nimani himoya qilish kerak? (masalan, aktivlar)
- Aktivlar nimadan yoki kimdan himoyalanishi kerak? (masalan, tahdidlar va zaifliklar)
- Tashkilot tegishli himoyaga ega bo'lish uchun qancha mablag' sarflashga tayyor?
- Biznes uchun xarajat va foyda qanday?

Bosqich to'rtta kichik bosqichdan iborat: aktivlarni aniqlash, zaifliklar va tahdidlarni aniqlash, xavflarni baholash natijalarini umumlashtirish, mumkin bo'lgan chora-tadbirlar va nazoratni baholash. Ushbu kichik bosqichlar ketma-ket bajarilishi kerak va natija aniqlangan xavflarni kamaytirishni ta'minlash uchun xavfsizlik siyosatiga nimani kiritish kerakligini hal qilish uchun ishlatiladi.

Boshqaruvni sotib olish va xodimlarni qo'llab-quvvatlash. Risklarni baholash natijalariga ko'ra, rahbariyat xavfni maqbul darajaga kamaytirish uchun tavsiya etilgan nazoratni amalga oshirish xarajatlari va foydalarini baholashi kerak. Agar ko'zda tutilgan xarajatlar byudjet doirasida bo'lsa, siyosat qurilishining keyingi bosqichi boshlanishi

mumkin. Aks holda, xavfni kamaytirish strategiyalari byudjet doirasida bo'lishi uchun qayta ko'rib chiqilishi yoki byudjetni oshirishi kerak. Siyosatni ishlab chiqish hayotiy tsiklining ushbu bosqichida menejmentni jalb qilish asosiy talab hisoblanadi, holbuki, umuman olganda, xodimlar faqat xavflarni baholash nuqtai nazaridan jalb qilinadi.

2-bosqich: Siyosat qurilishi. Xavfsizlik siyosati ushbu bosqichda xavflarni baholash bosqichida kelishilgan tahdidlar va zaifliklar keltirib chiqaradigan xavflarni kamaytirish bo'yicha xulosalar va tavsiyalar asosida ishlab chiqiladi. Ushbu bosqich, shuningdek, siyosatni yaratish jarayonida biznes strategiyalari va maqsadlari va qonuniy talablarni ko'rib chiqadi. Bosqich quyidagi kichik bosqichlardan iborat: Bir sahifalik siyosat bayonoti va yuqori darajadagi xavfsizlik talablari rejasini ishlab chiqish, Yuqori darajadagi siyosat bayonotini ko'rib chiqish va tasdiqlash, Batafsil siyosiy hujjatlar loyihasini ishlab chiqish, Batafsil siyosat bayonotlarini ko'rib chiqish va tasdiqlash, Tasdiqlangan xavfsizlik siyosatlarini nashr etish.

Axborot xavfsizligi siyosatini yozish jarayoni erishish kerak bo'lgan tegishli boshqaruv maqsadlarini tanlashni o'z ichiga oladi. Boshqaruv maqsadi muayyan jarayonda nazorat tartib-qoidalarini amalga oshirish orqali erishilishi kerak bo'lgan istalgan natija yoki maqsadning bayoni sifatida aniqlanadi. Boshqarish maqsadi, shuningdek, tegishli xavfsizlikni boshqarish vositalaridan foydalanish orqali amalga oshiriladigan axborot xavfsizligining eng yaxshi amaliyoti sifatida ko'rilishi mumkin. Tanlangan nazorat maqsadlari talablariga javob beradigan bir sahifali siyosat bayonoti va yuqori darajadagi xavfsizlik talablari rejasi tuziladi. Ushbu loyiha tashkilotning yuqori darajadagi tashvishlarini aks ettiruvchi ideal axborot xavfsizligi siyosatini yaratish uchun boshlang'ich nuqtani taqdim etadi. Loyiha yuqori darajadagi siyosat bayonotini ko'rib chiqish va tasdiqlash uchun ijrochi va yuqori rahbariyatga taqdim etiladi. Tasdiqlangan taqdirda, yuqori darajadagi siyosat bayonotiga asoslangan batafsil dasturiy hujjat loyihasi yana rahbariyatga tasdiqlash uchun taqdim etiladi; va tasdiqlansa, xavfsizlik siyosati chop etishga tayyor bo'ladi.

Siyosat loyihalari va yakuniy xavfsizlik siyosati hujjatlarini ko'rib chiqish va tasdiqlash bo'yicha rahbariyatning ajralmas rolidan tashqari, siyosatni xodimlarga to'g'ri yetkazilishini ta'minlash uchun ularning siyosatga aniq sodiqligi va qo'llab-quvvatlashi zarur. Tashkilotni bo'lajak o'zgarishlarga tayyorlash va shaxslarga yangi siyosatni shakllantirishga

ta’sir o’tkazish imkonini berish uchun siyosatni qurish bosqichida auditoriyaning fikr-mulohazalarini bildirish imkonini beruvchi aloqa rejasini boshlash kerak. Ishtirok etish foydalanuvchilarni majburiyatni tayyorlashdan qabul qilishgacha va oxir-oqibat majburiyat bosqichiga o’tkazishda muhim ahamiyatga ega.

Bundan tashqari, yangi yoki yangilangan xavfsizlik siyosati muqarrar ravishda kimningdir ish uslubida nimanidir o’zgartiradi va bunday o’zgarishlar qanchalik kichik bo’lmasin, e’tiborni talab qiladi. O’zgarishlarning ta’sirini uning muvaffaqiyatli amalga oshirilishiga ishonch hosil qilish uchun baholash kerak. Shuning uchun hozirgi muhitni tushunish juda muhimdir. Masalan, ushbu savollar xodimlarning yangi xavfsizlik siyosatini muvaffaqiyatli qo’llab-quvvatlash qobiliyatini baholash uchun siyosatni qurish bosqichida berilishi kerak:

— Kimga ta’sir qiladi?
— Tashkilot muhiti xavfsizlik muhimligini tushunadimi?
— Tashkilot muhiti yangi siyosatning tarkibiy qismlari va uni amalga oshirishning asosiy masalalarini qanday joriy qilishni talab qiladi?
— Yangi siyosat amalga oshirilganda nima bo’lishi kutilmoqda?

Yuqorida aytib o’tilgan jihatlar xodimlarning yangi siyosatlarni qabul qilishini va qo’llab-quvvatlashini ta’minlash uchun siyosatni amalga oshirish bosqichida ko’rib chiqilishi kerak.

3-bosqich: siyosatni amalga oshirish. Siyosat qurilishini tugatgandan so’ng, yangi xavfsizlik siyosati hujjatini amalga oshirish vaqti keldi. Endi dizaynni haqiqatga aylantirish uchun batafsil amalga oshirish rejasi talab qilinadi. Ushbu bosqich quyidagi kichik bosqichlarni o’z ichiga oladi: Batafsil tartib va ko’rsatmalar orqali xavfsizlik va nazorat talablarini aniqlash, Axborot xavfsizligi majburiyatlarini taqsimlash, Xavfsizlik va nazorat talablarini sinovdan o’tkazish, Xavfsizlik va nazorat talablarini amalga oshirish, Xavfsizlik siyosati bo’yicha doimiy trening va xabardorlikni amalga oshirish.

Tashkilotning yuqori martabali a’zolari bilan muloqot butun tashkilot tomonidan xavfsizlik siyosatini qabul qilish ehtimolini oshiradi va majburiyat bosqichlarida shaxslarni rag’batlantirishga yordam beradi. Xavfsizlik siyosatining tasdiqlangan yakuniy nusxasi barcha xodimlarga osonlikcha taqdim etilishi kerak. U barcha foydalanuvchilarga rasmiy ravishda etkazilishi kerak va foydalanuvchilar imzo qo’yish va unga rioya qilishga rozilik berish orqali siyosat o’qilgan va tushunilganligini tan olishlari kerak. Keyingi talab yangi siyosat bo’yicha xavfsizlik bo’yicha

xabardorlik va trening dasturlarini ishlab chiqish bo'ladi. Ushbu dasturlar siyosatni amalga oshirish bosqichining juda muhim bosqichlari hisoblanadi, chunki ularning asosiy roli xodimlarning siyosatni amalga oshirishda faol rol o'ynashga undash orqali munosabatini o'zgartirishdan iborat bo'ladi..

4-bosqich: Siyosat monitoringi va texnik xizmat ko'rsatish. Ushbu bosqich ikkita asosiy faoliyatdan iborat, ya'ni. monitoring va texnik xizmat ko'rsatish.

Siyosat monitoring. Axborot xavfsizligi siyosati amalga oshirilgandan so'ng, tashkilotlar xavfsizlik siyosatining butun tashkilot bo'ylab bajarilishini ta'minlaydigan tashkilotning kundalik faoliyatini aniqlash uchun tegishli monitoring mexanizmlarini o'z ichiga olishi kerak. Quyidagi kichik bosqichlarni bajarish kerak: Foydalanuvchilarning xatti-harakatlarini aks ettiruvchi o'lchanadigan natijalarni ishlab chiqarish, Tizim tekshiruvlari va tekshiruvlarini o'tkazish, Bosqinlarni aniqlash va kirish testlarini o'tkazish, Foydalanuvchilar faoliyati auditini tahlil qilish, Audit siyosatiga muvofiqlik. Siyosat monitoringining asosiy maqsadi xodimlarning yangi siyosat talablariga rioya qilishlarini ta'minlashdir. Shunday qilib, taklif qilingan ISP-DLC xavfsizlik siyosatining barqarorligini ta'minlash uchun siyosat talablariga rioya qilish zarurligini ko'rsatadi. Faqatgina tuzilgan va hech qachon qo'llanilmaydigan va rioya qilinmaydigan siyosatlar tashkilotga foyda keltirmaydi.

Siyosatga xizmat ko'rsatish. Ushbu faoliyat quyidagi kichik bosqichlarni o'z ichiga oladi: Xavfsizlik hodisalari to'g'risidagi hisobotlarni ko'rib chiqish, Xavfsizlik va texnologiya infratuzilmasini ko'rib chiqish, Biznes strategiyalarini ko'rib chiqish, Trendlar va kutilmagan hodisalarni ko'rib chiqish, Qonuniy talablarni ko'rib chiqish, Siyosatni o'zgartirish uchun so'rovni tuzish, Siyosatni ishlab chiqishning hayot aylanishini takrorlash.

Yangi tahdidlarni aniqlash uchun tashkilotning xavfsizlik infratuzilmasini doimiy ravishda ko'rib chiqish muhimdir. Bu tashkilotning boshqa joylarida qo'llaniladigan texnologiyaning o'zgarishi bilan bog'liq bo'lishi mumkin. Bundan tashqari, tashkilot xavfsizligi siyosatiga kiritilishi kerak bo'lgan yangi qonunlar kiritilishi mumkin. Xulosa shuki, turli xarakterdagi o'zgarishlar axborot xavfsizligi siyosatining eskirishiga olib kelishi mumkin. Ushbu o'zgarishlar texnik xizmat ko'rsatish bosqichida siyosatlarga kiritilishi kerak. Ta'mirlash bosqichi siyosatlarga o'zgartirishlar maxsus tarzda qo'llanilmasligini

ta’minlash uchun hayot siklining 1-3 bosqichlarini qayta bajarishni talab qiladi. Albatta, noma’lum narsalar juda ko’p va bu bosqichda tashkilotlar, ehtimol, hisobga olinmagan yangi tahdidni, zarur bo’lgan yangi texnologiyani yoki unutilgan va tashkiliy siyosatda hisobga olinishi kerak bo’lgan biznes qobiliyatini aniqlaydilar.

Ushbu bosqichda menejment xodimlar amalga oshirilgan siyosat va tartiblarni tushunadimi yoki yo’qmi, siyosat va tartiblarga rioya qilinayotganligini aniqlash uchun tegishli tartib va tizimlar mavjudligini ta’minlashi kerak. Bundan tashqari, boshqaruv xavfsizlik siyosati talablariga rioya qilmaslik uchun tegishli oqibatlarga olib kelishini ta’minlashi kerak. Jazolar doimiy ravishda qo’llanilishi va barcha xodimlarga yetkazilishi kerak.

Qisqacha xulosa qilib aytadigan bo’lsak, xavfsizlik siyosatini ishlab chiqish oddiy siyosat yozish va amalga oshirishdan tashqariga chiqadi. Tashkilotlar xavfsizlik siyosatini ishlab chiqishda zarur bo’lgan turli bosqichlarni aniq tan olmasalar, ular noto’g’ri o’ylangan, to’liq bo’lmagan, ortiqcha, foydalanuvchilar tomonidan to’liq qo’llab-quvvatlanmagan, ortiqcha yoki ahamiyatsiz siyosatlarni ishlab chiqish xavfiga duch kelishadi. Xavfsizlik siyosati o’zining yaroqlilik muddati davomida o’tishi kerak bo’lgan butun hayot tsikliga ega. Ushbu mavzuning maqsadi har tomonlama va barqaror axborot xavfsizligi siyosatini ta’minlaydigan axborot xavfsizligi siyosatini ishlab chiqishning hayot aylanishini taklif qilish hisoblanadi.

Tashkilotlar bir zarbada keng qamrovli xavfsizlik siyosatini ishlab chiqa olmaydi, lekin xavfsizlik siyosatini ishlab chiqish hayotiy tsikli davomida yaxshi rejalashtirilgan, uzluksiz jarayonga rioya qilish kerak. Axborot xavfsizligi siyosatini yaratish bir martalik hodisa emas, lekin siyosatlar qo’shimcha qiymat berishini ta’minlash uchun doimiy majburiyatni talab qiladi. Bunga taklif qilingan hayot aylanishi yondashuvi orqali erishish mumkin. Bu yerda tavsiflangan keng qamrovli xavfsizlik siyosatining hayot tsiklidan foydalanish tashkilotlarga xavfsizlik siyosatini ishlab chiqish uchun zarur qadamlar siyosatning amal qilish muddati davomida izchil bajarilishini va siyosatlarga rioya etilishini ta’minlashda yordam berish uchun asos yaratadi. Shunday qilib, siyosatning o’zi rivojlanish jarayonining yagona artefakti emas, balki uning barqarorligini va siyosatga rioya etilishini kafolatlashni o’z ichiga oladi.

4.2-§. Korporatsiyalarning kiberjinoyatga munosabati

Korporatsiyalardagi kiberjinoyat tushunchasi. Korporatsiyalar katta va kichik hakerlar tomonidan muntazam ravishda hujumga uchraydi. Ba'zi hujumlar juda katta bo'lib, millionlab mijozlarning ma’lumotlarini buzilishiga olib keladi. Shu sababli korporatsiyalar kiberxavfsizlikka qanday munosabatda bo'lishi juda muhim hisoblanadi.

Haqiqat shundaki, mijozlarni va aktivlarni himoya qilish uchun katta resurslar sarflanadi, shunga qaramay korporatsiyalar har kuni qisqa yoki uzoq muddat hujum ostida bo’lishi sezilarli ta'sir va jiddiy oqibatlarga olib keladi. Shuning uchun korporatsiyaga qilingan hujumni milliy davlatga qilingan hujum sifatida qarash kerak.

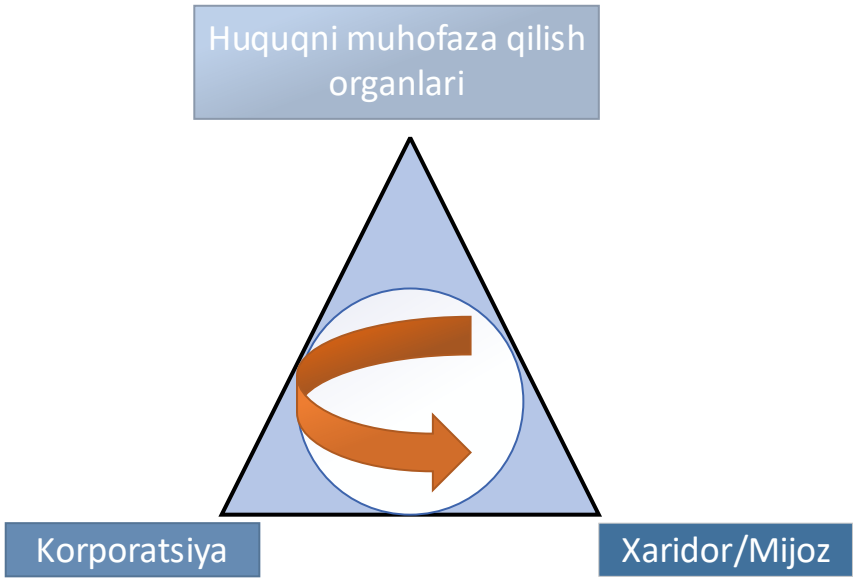
Taxminlarga ko'ra, bu muvaffaqiyatsizlik korporativ rahbarlarning aniq xavf mavjudligini tushuna olmasligi bilan bog'liq emas. Biroq, bu xavfni tushunish istagi yo'qligidan dalolat beradi. Amaliy nuqtai nazardan, tushunish birinchi holatda shunchaki gazeta o'qishni talab qiladi, ikkinchisi moliyaviy xarajatlarni, resurslarni taqsimlashni va zaiflikni oldini olish uchun keng jamoatchilik talab qiladigan aniq choralarni talab qiladi. Bularning barchasi rahbarlar nigohida ahamiyatsiz ko’rinishi mumkin. Bunday yondashuv kalta o’ylash va o’z-o’zini mag’lub qilish demakdir. Bu esa mijozlar va investorlarga salbiy ta'sir qiladi, ish huquqni muhofaza qilish organlariga yuklanadi, bu boshqa korporatsiyalar va keng jamoatchilikka ta'sir qiladi. Eng xavotirli va ahamiyatlisi - bu kiberhujumchilarning shijoatini uyg'otadi, ular korporativ rahbarlarning kiberhujumlarni yaxshi tushunisha olmasligini va qobilyatsiz ekanliklarini zaiflikka aylantiradi.

Qobiliyatsizlik - bu hujumlarning oldini olmaslik, taxmin qilingan zaiflik va tahdidlarni e’tiborsiz qoldirishdir. Bunday holatlarda artikulyatsiyani qo’llash kerak. Artikulyatsiya qo’rquvni anglatmaydi, aksincha haqiqatni tan olish va aytishga tayyorligini bildiradi, jamoatchilikni, bevosita manfaatdor tomonlarni, haqiqiy va potentsial hujumlardan xabardor qilish borasida ancha samarali siyosat.

Yana bir samarali yondashuv bu – hamkorlikdir. Bu esa tahdidni tan olishni anglatadi, tahdidni minimallashtirish choralarini ko'rishni aks ettiradi, shu bilan birga hujum ehtimolini inkor etmaydi va uning mumkin bo'lgan oqibatlarini kamaytiradi. Bundan tashqari, mijoz kiberterrorizmga qarshi kurash kontekstida hamkor bo'ladigan muhit yaratadi, chunki mijozga muhim shaxs sifatida munosabatda bo'linadi.

Mijozning kiberterrorizmga qarshi kurashda sherik sifatidagi

kontseptsiyasi korporatsiya va xaridor/mijoz o'rtasida uchburchak munosabatlar yaratiladi, bu esa huquqni muhofaza qilish organlari tahdidni keraksiz ravishda minimallashtirishdan ko'ra ancha samaralidir (4.2- rasm).



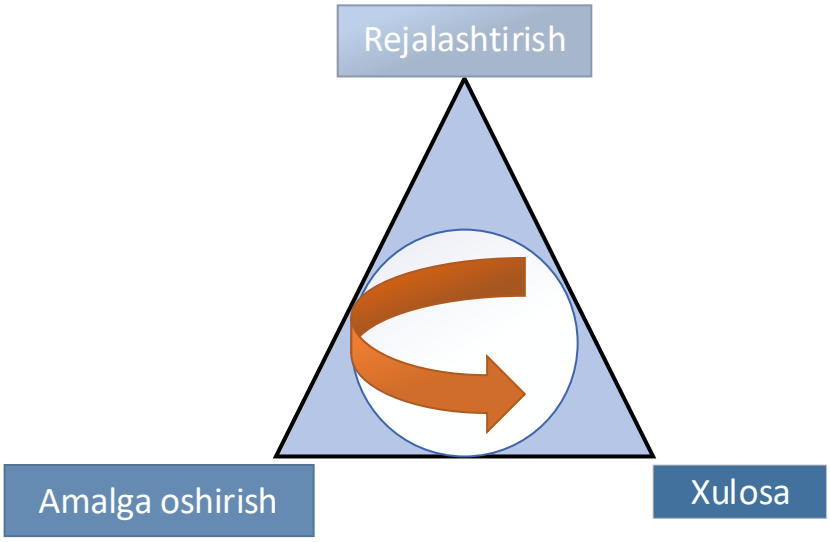
4.2-rasm. Korporatsiya bilan uchburchak munosabatlar

Xuddi shu nuqtai nazardan, kiberhujumlar tahdidi korporatsiyalardan mijozlar va huquqni muhofaza qilish organlari bilan hamkorlikni o'rnatishni talab qiladi. Tan olish kerakki bu hamkorlik birmuncha qiyin, lekin bu zarur. Chunki korporatsiyalarga kiberhujumlar tahdidini inkor etib bo'lmaydi. Buni minimallashtirish uchun tahdid to'g'ridan-to'g'ri va bilvosita ta'sir ko'rsatadigan shaxslarning birgalikdagi, to'g'ridan-to'g'ri, doimiy harakatini talab qiladi.

Kichik va katta korporatsiyalarga qilingan son-sanoqsiz hujumlar tashvishli va takrorlanadigan muhim jihat va hujumdan keyin korporatsiyalar buzg'unchilik sodir bo'lganligini anglab yetgunga qadar o'tadigan qimmatli vaqt. Bu esa ikki tomonlama zaiflikni ko'rsatadi:

— Xavfsizlik devorlari hujumning oldini olish uchun yetarlicha murakkab emas.
— Xavfsizlik devorlari hujum sodir bo'lgandan keyin uni aniqlash uchun yetarlicha murakkab emas.

Hujumning ma'lum vaqt davomida javobsiz qolishi, bitta hujumdan kelib chiqadigan zaiflikni oshiradi, zaiflik uzluksiz modeli nuqtai nazaridan, xabar qilinmagan hujum davom etayotgan zaiflikni aks ettiradi. An'anaviy terrorchilik hujumidan farqli o'laroq, uch qismli modelni aks ettiruvchi yagona hujumga asoslangan: rejalashtirish, amalga oshirish, xulosa (4.3-rasm).



4.3-rasm. Uch qismli model

Shu o’rinda bir savol tug’iladi, nega korporatsiyalar buzg'unchilik sodir bo'lganligini tan olishda ikkilanishadi? Javobi oson: bunday mashhur korporatsiyaning moliyaviy holatiga salbiy ta'sir qiladi, yangi mijozlarni to'xtatib qo'yadi, raqobatchilarga ochko to'plash imkoniyatini beradi va mavjud mijozlarni o'z biznesini boshqa joyga olib borishga turtki bo’lishi mumkin.

Korporatsiyalarning yana bir kamchiligi, hakerlik hujumidan so’ng darhol hol oldinga chiqib, “bizga hakerlik hujumi bo’ldi, ojiz qoldik, bundan saboq olaylik” deb aytadigan korporatsiyalar soni juda kam. Chunki bu ular uchun ko’pgina imkoniyat eshiklarini yopishi mumkin. Bu jarayon hakerlarga juda qo’l keladi, chunki korporatsiyalar bir – biridan tahdidlarni kamaytirish choralarini o’rgana olishmaydi.

Korporatsiyalar, shaxslar yoki davlatlar vaqti-vaqti bilan potentsial tajovuzkorlarning imkoniyatlarini yetarlicha baholamaydilar. O’zlarining tizimi yaxshiroq yoki samaraliroq deb o'ylaydilar. Buning oqibati quyida keltirilgan:

— Davomli zaiflik;
— Mijozlar uchun doimiy tahdid;
— Mijoz ma'lumotlari maxfiyligini yetarli darajada himoya qilmaslik oqibatida yuzaga kelishi mumkin bo'lgan fuqarolik javobgarligi va buzilish oqibatlari haqida xabardor qilmaslik uchun javobgarlik.

Korporatsiyaning muvaffaqiyatsizligini keltirib chiqaradigan eng muhim omillar: himoya qilmaslik va xabardor qilmaslikdir. Sabablari quyida keltirilgan:

— Potentsial mijozlar himoya qila olmagani/xabar bermasligini aniqlagandan so'ng, o'z biznesini olib kelishga ikkilanishadi.

— Mavjud mijozlar maxfiyligini himoya qilish uchun barcha oqilona choralar ko'rilmagan degan xulosaga kelishsa, o'z bizneslarini boshqa joyga olib borishlari mumkin.

— Kengroq jamoatchilik korporatsiyaga kiberhujumlarni bartaraf etish va kiberxavflarni minimallashtirish kontekstida salbiy munosabatda bo'ladi, ammo eng kuchli tanqid haqiqatni aytmaslik bo'ladi.

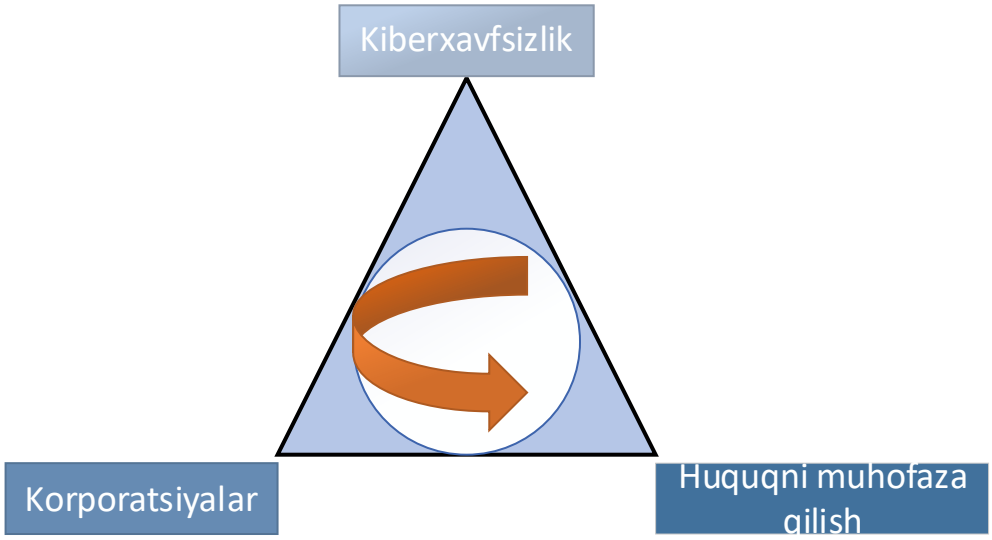
Bu kamchiliklar quyidagicha hal qilinishi kerak:

— Kirishning tan olinishi;
— Mijozlarni himoya qilish uchun kirishni darhol bartaraf etish bo'yicha ko'rilgan choralar ro'yxati;
— Kelajakda mijozlarni himoya qilishga qaratilgan chora-tadbirlar ro'yxati;
— Axborot almashish kontekstida boshqa korporatsiyalar bilan bog'lanish;
— Kiberjinoyatga qarshi tajovuzkor choralarni qo'llash.

Bunday yondashuv, korporatsiya nuqtai nazaridan, turli auditoriyalarni, xususan, mijozlarni va huquqni muhofaza qilish organlarini jalb qilishga tayyorligini ko'rsatadi.

Huquqni muhofaza qilish. Hech shubha yo'qki, kiberhujumlar huquqni muhofaza qilish organlari uchun juda qiyin va yangi muammolarni keltirib chiqaradi. Huquq-tartibot idoralari vakillari bilan suhbatlar shuni ta'kidlaydiki, kiberjinoyat ham an'anaviy politsiyachilar, ham qaroqchilar, ham an'anaviy terrorizmdan tubdan farq qiladi. Huquqni muhofaza qilish organlari uchun kiberjinoyat murakkab muammolarni keltirib chiqaradigan mutlaqo boshqacha jinoyat modelidir. Huquqni muhofaza qilish organlari xodimlari bilan o'zaro hamkorlik korporatsiyalar bilan ham faol, ham reaktiv tarzda yaqindan ishlashga katta tayyorlikdan dalolat beradi.

Asosiy yondashuv bu yerda tahdidlarni yumshatish va haqiqiy hujum ta'sirini minimallashtirishdir. Kiberxavfsizlik, korporatsiyalar va huquqni muhofaza qilish organlarining uchburchagi operativ imkoniyatlarni talab qiladi va rivojlanib boradi (4.5-rasm).

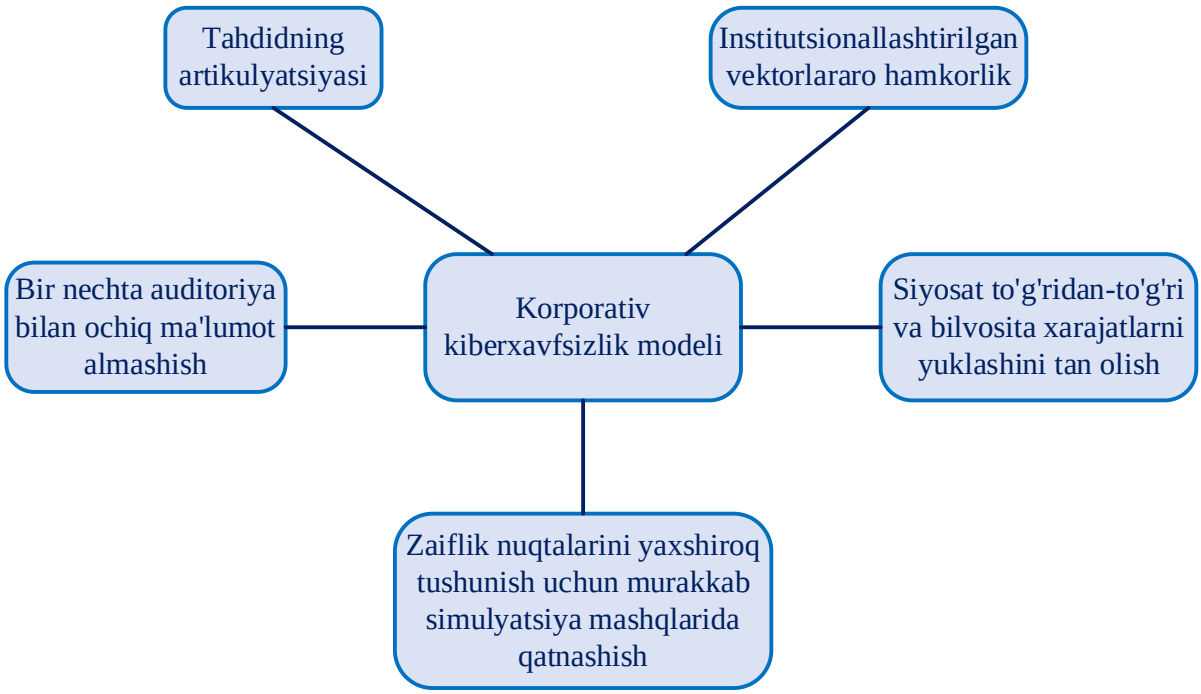


4.5-rasm. Kiberxavfsizlik uchburchagi

Sarmoya. So'nggi hujumlar shuni ko'rsatdiki, korporatsiya buzilganligini tushunish, tan olish va aniqlash uchun 243 kungacha vaqt ketishi mumkin. Bu hayratlanarli va ko’p vaqt tashvishli kechikishning sabablaridan biri shundaki, kiber-profilaktika katta sarmoyani talab qiladi. Bu sarmoya nafaqat moliyaviy, balki korporativ madaniyatda muhim o'zgarishlarni talab qiladigan xodimlarga sarmoya kiritishni ham talab qiladi, bu esa rahbariyatdan kiber zaiflikni tan olish va ifoda etishni talab qiladi.

Kiber tahdidni hisobga olgan holda, korporatsiyalar aktsiyadorga emas, balki mijoz oldidagi majburiyatning ustuvorligini tan olishlari kerak. Ushbu qayta ishlangan ustuvorlik modeli korporativ rahbariyatga aktsiyadorlar orasida tushunmovchilikka sabab bo'lsa ham, yanada ochiqroq, halol va samimiy bo'lish talabini qo'yadi . Ushbu yondashuv korporatsiyaning asosiy vazifasi mijozni himoya qilish va xabardor qilish ekanligini tan olishga asoslanadi, garchi bu majburiyat korporatsiyaga qimmatga tushsa ham.

Korporativ xavfsizlik hakerlarning narxi, ta’siri va g’arazli niyatlarini hisobga olgan holda korporativ xavfsizlik modelini tuzish mumkin (4.6-rasm).



4.6-rasm. Korporativ kiberxavfsizlik modeli

Korporatsiyalarga qarshi kiberjinoyat turlari. Korporatsiyalarga qarshi kiberjinoyatlarning bir misoli fishing hujumidir. Fishing hujumida kiberjinoyatchi ishonchli sotuvchi, bank yoki hamkasb kabi qonuniy manbadan kelgan soxta elektron pochta yoki xabar yuboradi. Elektron pochta odatda havola yoki ilovani o'z ichiga oladi, bu bosilganda, oluvchining kompyuteriga zararli dasturlarni o'rnatadi yoki qabul qiluvchidan kirish ma'lumotlari, kredit karta raqamlari yoki shaxsiy ma'lumotlar kabi maxfiy ma'lumotlarni kiritishni taklif qiladi.

Kiberjinoyatchi qabul qiluvchining kompyuteriga yoki maxfiy ma'lumotlariga kirish huquqini qo'lga kiritgandan so'ng, ular bu ma'lumotlardan maxfiy ma'lumotlarni o'g'irlash, moliyaviy firibgarlik qilish yoki tashkilot tarmog'idagi boshqa tizimlarga zararli dasturlarni tarqatish kabi turli zararli maqsadlarda foydalanishi mumkin. Kiberjinoyat natijasida kelib chiqadigan to'g'ridan-to'g'ri moliyaviy va operatsion yo'qotishlarga qo'shimcha ravishda, tashkilot o'z obro'siga putur etkazishi, mijozlar ishonchini yo'qotishi va qonuniy javobgarlikka tortilishi mumkin.

Fishing hujumlarining oldini olish uchun tashkilotlar kiberxavfsizlik bo‘yicha turli chora-tadbirlarni amalga oshirishi mumkin, masalan, xodimlarni shubhali elektron pochta xabarlarini aniqlash va hisobot berish, antifishing dasturlari va xavfsizlik devorlaridan foydalanish, ikki faktorli autentifikatsiyani amalga oshirish, dasturiy ta’minot va xavfsizlik tizimlarini muntazam yangilab turish bo‘yicha o‘rgatish. Bundan tashqari,

tashkilotlar zararni kamaytirish uchun fishing hujumlarini tezda aniqlash va ularga javob berish uchun hodisalarga javob berish rejalarini ishlab chiqishi mumkin.

Korporatsiyalarga bo’ladigan kiberhujumlar 4.1-jadvalda kengroq tahlil qilingan va tushintirilgan.

4.1-jadval

Korporatsiyalarga bo‘ladigan kiberhujumlar tavsifi

Kiberjinoyat turi	**Tavsif**
Ransomware	Tashkilot ma'lumotlarini shifrlaydigan va shifrni ochish kaliti evaziga to'lov talab qiladigan zararli dastur turi.
Fishing	Xodimlarni maxfiy ma'lumotlarni oshkor qilish yoki zararli dasturlarni yuklab olish uchun aldash uchun soxta elektron pochta, veb-saytlar yoki xabarlardan foydalanish.
Biznes elektron pochta kelishuvi	Moliyaviy ma'lumotlarga yoki to'lov tizimlariga kirish huquqiga ega bo'lgan xodimlarga qaratilgan, ularni firibgar hisoblarga pul o'tkazishda aldashga qaratilgan fishing hujumi turi.
Insayder tahdidlar	Xodimlar yoki pudratchilar tomonidan ma'lumotlarning buzilishi yoki boshqa xavfsizlik hodisalariga olib keladigan zararli yoki beparvolik harakatlari.
Taqsimlangan xizmatni rad etish (DDoS) hujumlari	Tashkilot faoliyatini buzish uchun tarmoq yoki serverni trafik bilan to'ldirish.
Ma'lumotlarning buzilishi	Maxfiy ma'lumotlarga ruxsatsiz kirish yoki o'g'irlash, shu jumladan shaxsiy identifikatsiya qilinadigan ma'lumotlar (PII), moliyaviy ma'lumotlar va intellektual mulk.
Kiber josuslik	Raqobat ustunligiga erishish yoki tashkilot faoliyatini buzish maqsadida maxfiy ma'lumotlarni yoki intellektual mulkni o'g'irlash.
Ichki tahdidlar	Xodimlar yoki pudratchilar tomonidan ma'lumotlarning buzilishi yoki boshqa xavfsizlik hodisalariga olib keladigan zararli yoki beparvolik harakatlari.

Korporatsiyalar duch keladigan kiberjinoyat turlari doimiy ravishda o'zgarib bormoqda va tashkilotlarning so'nggi tahdidlar va zaifliklardan xabardor bo'lishlari muhim ahamiyatga ega. Tegishli xavfsizlik choralarini qo'llash ularning ma'lumotlari va operatsiyalarini himoya qilishga yordam beradi.

Tashkilotlar o'zlarining ma'lumotlari va operatsiyalarini ushbu turdagi kiberjinoyatlardan himoya qilish uchun tegishli xavfsizlik choralarini amalga oshirishlari muhimdir. Ushbu chora-tadbirlar tarmoq xavfsizligi, kirishni boshqarish, xodimlarni o'qitish, ma'lumotlarni shifrlash va hodisalarga javob berishni rejalashtirishni o'z ichiga olishi mumkin.

Kiberjinoyatlarga korporativ javoblar. Korporativ kiberjinoyatlar butun dunyo bo‘ylab korxonalar uchun tobora dolzarb muammoga aylanib bormoqda. Kiberhujumlar tahdidi jiddiy bo'lib, oqibatlari moliyaviy yo'qotishlardan tortib obro'ga putur yetkazish va yuridik javobgarlikgacha bo'lgan oqibatlarga olib keladi. Yaxshiyamki, tashkilotlar o'z xavfini kamaytirish va o'zlarini kiberjinoyatlardan himoya qilish uchun ko'rishi mumkin bo'lgan bir nechta qarshi choralar mavjud (4.2-jadval).

Kiberjinoyatlarga korporativ javoblar kiberhujumlar, ma’lumotlar buzilishi va boshqa kibertahdidlarning oldini olish, aniqlash va ularga javob berish bo‘yicha tashkilotlar tomonidan ko‘riladigan strategiyalar va harakatlarni nazarda tutadi. Kiberjinoyatlarga korporativ javoblar bilan bog'liq ba'zi asosiy tushunchalar:

- Kiberxavfsizlik: kompyuter tizimlarini, tarmoqlarini va maxfiy ma'lumotlarni ruxsatsiz kirish, o'g'irlik, shikastlanish yoki buzilishdan himoya qilish amaliyoti.
- Risklarni boshqarish: tashkilotning aktivlari, obro'si yoki faoliyatiga zarar etkazishi mumkin bo'lgan xavflarni aniqlash, baholash va kamaytirish jarayoni.
- Voqealarga javob berish: Tashkilotlar ma'lumotlarning buzilishi, zararli dastur infektsiyalari yoki fishing hujumlari kabi kiber hodisalarni bartaraf etish va ularni o'z ichiga olish uchun amal qiladigan protseduralar va protokollar to'plami.
- Kriminalistika: kiber hodisa yoki jinoyat bilan bog'liq raqamli dalillarni to'plash va tahlil qilish uchun maxsus texnika va vositalardan foydalanish.

— Kiber sug'urta: kiberhujumlar yoki ma'lumotlar buzilishi natijasida kelib chiqadigan moliyaviy yo'qotishlar va majburiyatlarni qoplaydigan sug'urta polisi turi.
— Muvofiqlik: Tashkilotlar kiberxavfsizlik va ma'lumotlar maxfiyligi bilan bog'liq tegishli qonunlar, qoidalar va standartlarga rioya qilishlarini ta'minlash jarayoni.
— Kibertahdidlar bo'yicha razvedka: potentsial yoki haqiqiy kibertahdidlar, shu jumladan ularning manbasi, motivi va usullari haqida ma'lumotlarni to'plash, tahlil qilish va tarqatish.
— Uchinchi tomon risklarini boshqarish: Tashkilot tizimlari yoki ma'lumotlariga kirish huquqiga ega bo'lgan uchinchi tomon ishlab chiqaruvchilari, etkazib beruvchilari yoki hamkorlari bilan bog'liq kiberxavfsizlik risklarini baholash va boshqarish jarayoni.
— Biznesning uzluksizligi: tashkilotning kiberhujum kabi buzg'unchi hodisa paytida va undan keyin faoliyatini davom ettirish qobiliyati.
— Boshqaruv: Kiberxavfsizlik bilan bog'liq tashkilotni boshqarish va qarorlar qabul qilish jarayonlarini boshqaradigan siyosatlar, protseduralar va nazoratlar doirasi.
— Trening va xabardorlik: xodimlar va manfaatdor tomonlarni kiberxavfsizlik xatarlari, ilg'or tajribalar va tashkiliy siyosat va tartiblar bo'yicha o'qitish.
— Tahdid razvedkasi: Xatarlarni boshqarish va hodisalarga javob berish strategiyalarini xabardor qilish uchun kibertahdidlar va zaifliklarni monitoring qilish va tahlil qilish.

Tashkilotlar korporativ kiberjinoyatlardan o'zlarini himoya qilish uchun ko'rishlari mumkin bo'lgan bir qancha qarshi choralar mavjud. Xodimlarni o'qitish, kirishni boshqarish, tarmoq xavfsizligi, hodisalarga javob berishni rejalashtirish, shifrlashni o'z ichiga olgan keng qamrovli kiberxavfsizlik strategiyasini amalga oshirish orqali tashkilotlar o'z xavfini kamaytirishi va xavfsizlik hodisalariga samaraliroq javob berishi mumkin.

4.2-jadval

Kiberjinoyatlardan himoyalanish choralari

Qarshi chora	**Tavsif**
Xodimlarni tayyorlash	Xodimlarni kiberxavfsizlik bo‘yicha ilg‘or amaliyotlar haqida o‘rgatish ularni firibgarlik yoki boshqa kiberhujumlar qurboni bo‘lib qolishining oldini olishga yordam beradi.

Kirish boshqaruvlari	Maxfiy ma’lumotlar va tizimlarga vakolatli xodimlarga kirishni cheklash ruxsatsiz kirishning oldini olishga va ichki tahdidlar xavfini kamaytirishga yordam beradi.
Tarmoq xavfsizligi	Xavfsizlik devorlari, hujumlarni aniqlash tizimlari va boshqa xavfsizlik choralarini joriy qilish zararli dasturlar va DDoS hujumlari kabi tashqi tahdidlardan himoya qilishga yordam beradi.
Voqealarga javobni rejalashtirish	Xavfsizlik hodisalariga javob berish rejasini ishlab chiqish tashkilotlarga zararni minimallashtirish va hujumdan tezroq tiklanishiga yordam beradi.
Shifrlash	Maxfiy ma'lumotlarni shifrlash ma'lumotlar buzilgan taqdirda ularni ruxsatsiz kirishdan himoya qilishga yordam beradi.
Xavfsizlik bo'yicha trening	Xodimlarni kibertahdidlarni aniqlash va ularga javob berish bo‘yicha o‘rgatish fishing hujumlari, biznes elektron pochta xabarlarini buzish va boshqa turdagi kiberjinoyatlarning oldini olishga yordam beradi.
Ko'p faktorli autentifikatsiya	Xodimlardan parol va xavfsizlik tokeni kabi autentifikatsiyaning bir nechta shakllaridan foydalanishni talab qilish korporativ tarmoqlar va tizimlarga ruxsatsiz kirishning oldini olishga yordam beradi.
Tarmoq segmentatsiyasi	Korporativ tarmoqni kichikroq, ajratilgan segmentlarga bo'lish zararli dasturlarning tarqalishini oldini olishga yordam beradi va kiberhujumning zararini cheklaydi.
Voqealarga javobni rejalashtirish	Kiberhujumga javob berish rejasiga ega bo'lish voqea ta'sirini kamaytirishga yordam beradi va tezkor va samarali javobni ta'minlaydi.
Uchinchi tomon risklarini boshqarish	Uchinchi tomon sotuvchilari va pudratchilari xavfsizligini muntazam ravishda baholash va monitoring qilish ta'minot zanjiri hujumlari va kiberjinoyatlarning boshqa shakllarini oldini olishga yordam beradi.

Xodimlarni o'qitish kiberjinoyatlarga qarshi hal qiluvchi chora hisoblanadi, chunki xodimlar ko'pincha tashkilotning kiberxavfsizlik himoyasidagi eng zaif bo'g'in hisoblanadi. Parollarni boshqarish, internetni xavfsiz kezish va fishing elektron pochta xabarlarini aniqlash kabi mavzularda muntazam treninglar o‘tkazish xodimlarning zararli havolalarni beixtiyor bosish yoki maxfiy ma’lumotlarni oshkor qilishining oldini olishga yordam beradi.

Kirish nazorati, shuningdek, maxfiy ma'lumotlar va tizimlarga faqat unga muhtoj bo'lganlar uchun kirishni cheklash orqali kiberjinoyatlarning oldini olishga yordam beradi. Bu ruxsat etilgan ruxsatga ega bo'lgan xodimlar yoki pudratchilar o'z imtiyozlarini zararli maqsadlarda suiiste'mol qiladigan ichki tahdidlarning oldini olishga yordam beradi.

Xavfsizlik devori va hujumni aniqlash tizimlari kabi tarmoq xavfsizligi choralari zararli dasturlar va DDoS hujumlari kabi tashqi tahdidlarning oldini olishga yordam beradi. Bundan tashqari, hodisalarga javob berish rejasini ishlab chiqish tashkilotlarga xavfsizlik hodisalariga tezroq va samaraliroq javob berishga yordam beradi.

Shifrlash, shuningdek, kiberjinoyatlarga qarshi samarali chora bo'lishi mumkin, bu esa tajovuzkorlarga hatto tashkilotning himoyasini buzishga muvaffaq bo'lsa ham, maxfiy ma'lumotlarga kirishni qiyinlashtiradi. Dasturiy ta'minotni so'nggi xavfsizlik yamoqlari bilan yangilab turish ham muhim, chunki zaifliklar va ekspluatatsiyalar tajovuzkorlar tomonidan tezda aniqlanishi va ishlatilishi mumkin.

Shuni ta'kidlash kerakki, hech qanday qarshi chora ishonchli emas va korxonalar xavfning ko'plab sohalarini ko'rib chiqadigan kiberxavfsizlikka qatlamli yondashuvni qo'llashlari kerak. Bundan tashqari, korxonalar paydo bo'ladigan tahdidlar va zaifliklarga qarshi turish uchun kiberxavfsizlik strategiyalarini muntazam ravishda ko'rib chiqishlari va yangilashlari kerak.

4.3-§. Jismoniy shaxslarning kiberxavfsizlikni oldini olishdagi o‘rni

Ko’p hollarda korxonalarda xodimlar kiberxavfsizlik talablariga juda yengil qarashadilar, bu esa ular ishlayotgan tashkilotlar uchun keskin oqibatlarga olib kelishi mumkin. Yaqin o’tgan davrda ro’y bergan WannaCry to’lov dasturi epidemiyasida inson omili butun dunyo bo’ylab biznesni himoyasiz qilishda katta rol o’ynashi mumkinligini ko’rsatib berdi. Oshkor qilingan zaifliklar Microsoft-ning yangi o’zgarishlar(patch) yangilanishi bilan tuzatilganidan qariyb ikki oy o’tgach xam, dunyodagi ko’plab kompaniyalar hali ham o’z tizimlarini yangi o’zgarishlar bilan

yangilashmagan. Tajribalarda ko’p kuzatilgan va o’z isbotini topgan steriotiplardan biri bu IT bo’lmagan xodimlar eng zaif bo’g’in eknaligidir: masalan, mahalliy ma’mur huquqlariga ega bo’lgan xodimlar o’z kompyuterlarida xavfsizlik yechimlarini o’chirib qo’yishadi va infektsiya o’z kompyuterlaridan butun korporativ tarmoqqa tarqalishiga imkon berishadi. Natijada tarmoq xavfsizligi boy beriladi.

4.7-rasm. Xavfsizlik tizimi yoki yangilanishlarni qabul qilishni o’chirilishi

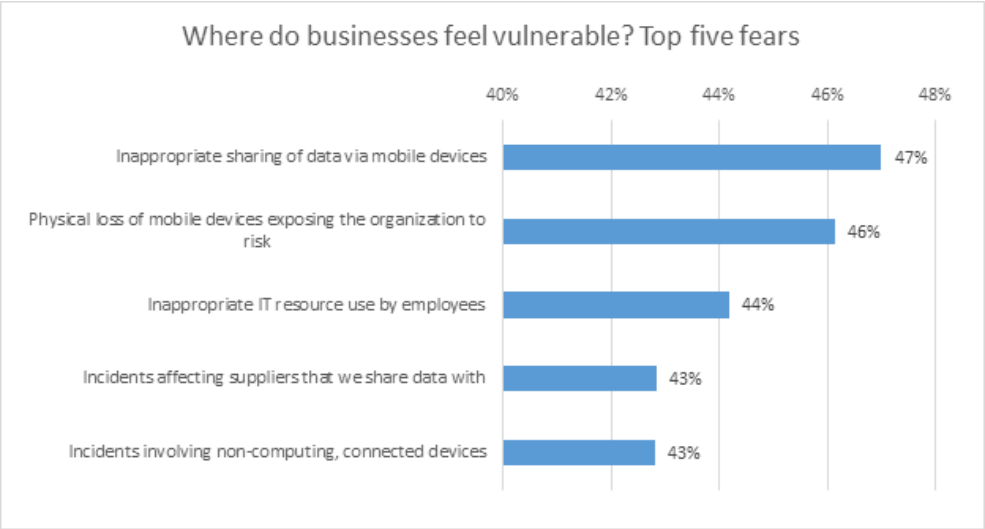
Xodimlar va umuman individuallar biznesning kiberjinoyatlarga qarshi kurashida qanday rol o’ynaydi, degan shartli savolga javob qidirsak, natijalar hayratlanarli bo’ladi. Kasperskiy laboratoriyasi tadqiqotlariga ko’ra korxonalarning yarmidan ko’pi (52%) o’zlarini ichkaridan xavf ostida deb hisoblashlarini kuzarishgan. Ularning xodimlari qasddanmi yoki o’zlarining beparvoligi yoki bilimsizligi tufayli o’zlari ishlayotgan korxonalarni xavf ostiga qo’yishadi.

Quyidagi keltirilgan Kasperskiy Laboratoriyasi hisobotida bu qanday va nima uchun sodir bo’layotgani va korxonalar o’z xodimlaridan o’zlarini himoya qilish uchun nima qilishlari mumkinligini keltirib o’tadi.

Murakkab va o’sib borayotgan kibertahdid manzarasi fonida, hozirda korxonalarning 57 foizi o’zlarining IT-xavfsizligi zaif deb o’ylashadi, korxonalar ham kiberhujumga qarshi qurol-aslahalarining eng katta chig’anoqlaridan biri bu o’z xodimlari ekanligini tushunishadi. Haqiqatan ham, korxonalarning 52 foizi xodimlarning IT xavfsizligidagi eng katta zaif tomoni ekanligini tan olishadi va ularning ehtiyotsiz harakatlari biznesning AT xavfsizligi strategiyasini xavf ostiga qo’yadi.

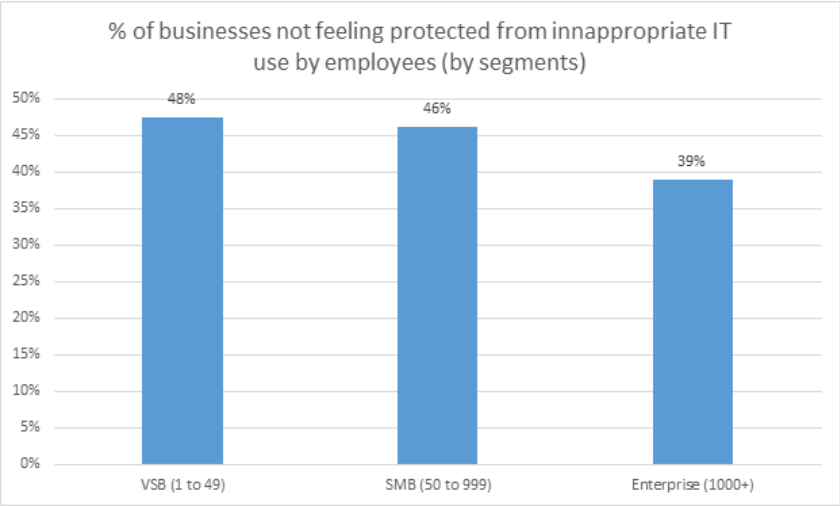
Quyidagi jadval shuni ko’rsatadiki, korxonalar xodimlar xatosi o’z

kompaniyasining xavfsizligiga juda osonligi bilan, lekin o’ta tezligi bilan ta’sir qilishini bilishadi. Ular asosan xodimlarning mobil qurilmalar orqali nomaqbul ma’lumotlarni almashishi (47%), mobil qurilmalarning jismoniy yo’qolishi, o’z kompaniyasini xavf ostiga qo’yishi (46%) va xodimlarning noto’g’ri AT resurslaridan foydalanishi (44%) haqida qayg’urishadi.



4.8-rasm. Biznesga ta’sir qiluvchi xavf-xatarlar ketma-ketligi

Ushbu topilmalarni diqqat bilan ko’rib chiqsak, xodimlarning IT-dan nomaqbul foydalanishi haqidagi xavotirlar kompaniya hajmiga qarab sezilarli darajada farq qiladi, chunki kichik korxonalar 1000 dan ortiq xodimlarga ega bo’lgan korxonalarga qaraganda ko’proq xavf ostida bo’ladi. O’rta biznes korxonalar(SMB)da xam bu ulush yirikligicha qolmoqda. Bunga bir qancha omillar sabab bo’lishi mumkin, shu jumladan korxonalarda potentsial qat’iyroq siyosatlar va xodimlarni ilg’or amaliyot bo’yicha chuqurroq o’qitishni olishimiz mumkin. Bundan tashqari, kichik korxonalar xodimlarga biznes IT resurslaridan foydalanishda yuqori darajadagi, cheklanmagan imkoniyatlarni taqdim qilishini ko’p uchratamiz. Lekin bu xavfsizlik nuqtai-nazaridan salbiy faktor sifatida qayd qilishimiz mumkin.

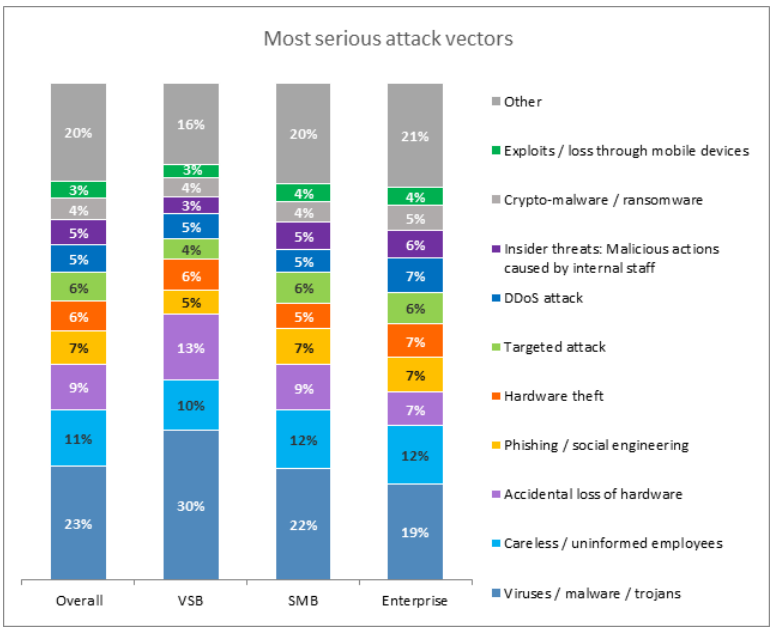


4.9-rasm. Xodimlar tomonidan kichik, o’rta va yirik biznesga salbiy ta’sir qilish darajasi

Tadqiqotlar natijalari shuni ko’rsatadiki, korxonalarda xodimlarning kiberxavfsizlik risklariga hissa qo’shayotganidan xavotirlanish uchun jiddiy sabablar bor. Xodimlar o’z kompaniyasining ma’lumotlari yoki tizimlarini risk ostiga qo’yadigan xatolarga yo’l qo’yishi mumkin.

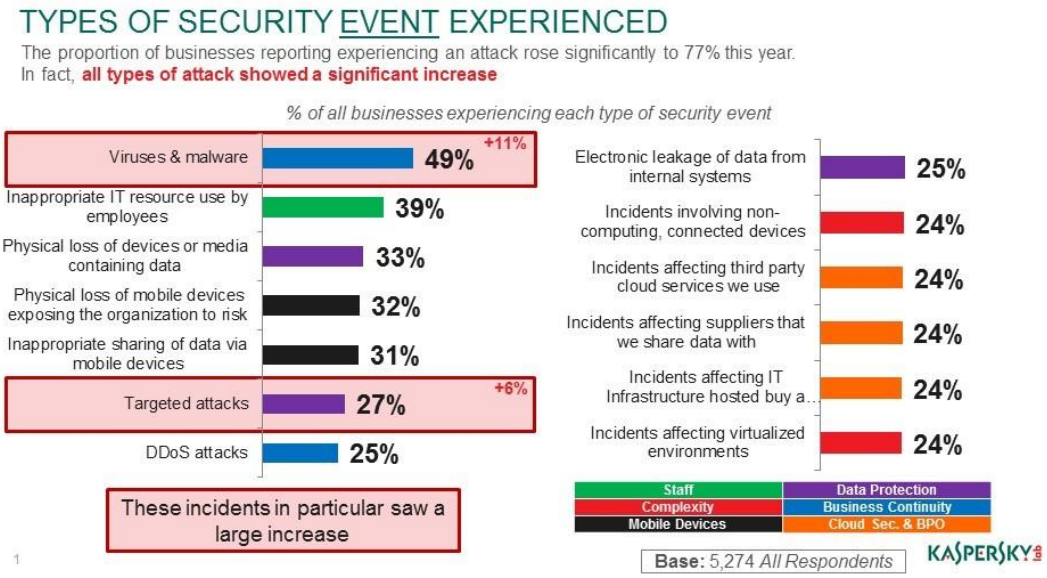
Ehtiyotsiz yoki ma’lumotga ega bo’lmagan xodimlar, masalan, jiddiy xavfsizlik buzilishining ikkinchi ehtimoliy sababi bo’lib, zararli dasturlardan keyin ikkinchi o’rinda turadi. Bundan tashqari, so’nggi yildagi kiberxavfsizlik hodisalarining 46 foizida ehtiyotsizlik oqibatida yoki yetarli ko’nikmaga ega bo’lmagan xodimlar kompaniyaga uyushtirilgan hujumlarga o’zlarining hissalarini qo’shishgan.

Xodimlarning inson xatosi korxonalar qurbon bo’ladigan yagona “hujum vektori” emas. Ya’ni, ichki xodimlar ham o’zlarining zararli harakatlari tufayli xavfsizlik muammolarini keltirib chiqargan, tadqiqotlarga ko’ra, oxirgi 12 oydagi xavfsizlik hodisalarining 30 foizi o’z ish beruvchilariga qarshi ishlaydigan xodimlar bilan bog’liq. Oxirgi 12 oy ichida kiberxavfsizlik intsidentlariga duch kelgan korxonalar orasida eng jiddiy hodisalarning o‘ndan biri (11%) ehtiyotsiz xodimlar bilan bog‘liq.



4.10-rasm. Kichik, o’rta va yirik biznesda xavfli hujum vektorlari

Xodimlarning beparvoligi va fishing (ijtimoiy muhandislik) zararli dasturlar va maqsadli hujumlar uchun asosiy omil sifatida xizmat qiladi.



4.11-rasm. Korxonalarda kuzatilayotgan hujumlarning oshish tendensiyasi

2017 yilda butun dunyo bo’ylab korxonalarning 49 foizi viruslar va zararli dasturlar tomonidan hujumga uchraganini ma’lum qilindi, bu 2016 yil natijalariga nisbatan 11 foizga ko’p. Virus va zararli dasturlar bilan bog’liq hodisalarga duch kelganlarning yarmidan sal ko’pi (53%) ehtiyotsiz yoki xabardor bo’lmagan xodimlarni asosiy omil deb hisoblashadi va uchdan bir qismidan ko’pi (36%) tahdidga fishing yoki ijtimoiy muhandislik hissa qo’shgan deb hisoblashadi.

“Berkinmachoq” yoki muammoni yashirilishi. Korxonada xavfsizlik bilan bog’liq hodisalar sodir bo’lganda, xodimlar buzilishni aniqlash yoki risklarni kamaytirish uchun tayyor bo’lishlari muhimdir. Biroq, xodimlar har doim ham kompaniya xavfsizlik hodisasiga duch kelganida chora ko’rishmaydi. Darhaqiqat, butun dunyo bo’ylab korxonalarning 40 foizida xodimlar voqea sodir bo’lganda uni yashirishadi. Hodisani yashirish dramatik oqibatlarga olib kelishi va yetkazilgan zararni oshirishi mumkin. Bitta xabar qilinmagan hodisa hatto tashkilotning butun infratuzilmasining keng miqyosda buzilishiga olib kelishi mumkin.

O’z vaqtida aniqlash, shuningdek, maqsadli hujumni muvaffaqiyatli tekshirish va kriminalistik tahlil qilish muammoning kaliti hisoblanadi. Faqat xodimlarning hushyorligiga va ular sodir bo’lgan voqealar haqida xabar berish qobiliyatiga tayanish yetarli emas, chunki inson omillari va hujumning murakkabligi bilan bog’liq xavflar ikki baravar ortib bormoqda. Shuning uchun korxonalarga tizim monitoringini avtomatlashtiradigan va xato mas’uliyatsizlik ehtimolini kamaytiradigan maxsus yechimlar va texnologiyalardan foydalanish tavsiya etiladi.

Yirik kompaniyalar uchun “berkinmachoq” muammosi eng qiyini hisoblanadi, bunda korxonalarning 45 foizi (1000 dan ortiq xodimlar) kiberxavfsizlik hodisalarini yashirayotgan xodimlarni aniqlashga qiynalishadi, kichik biznes korxonalar uchun bu ko’rsatkich atigi 29 foizni tashkil etadi (xodimlar soni 49 nafardan kam).

Hodisalarni yashirish muammosi nafaqat xodimlarga, balki butun biznesga, ya’ni yuqori boshqaruv va kadrlar bo’limiga yetkazilishi kerak. Agar xodimlar voqealarni yashirishsa, buning sababi bo’lishi kerak. Ba’zi hollarda kompaniyalar qattiq, lekin tushunarsiz qoidalarni joriy qiladi va xodimlarga qo’shimcha mas’uliyat yuklaydi, ularni u yoki bu qilmaslik haqida ogohlantiradi yoki biror narsa noto’g’ri bo’lsa, ular javobgarlikka tortiladi. Bunday siyosat faqat qo’rquvni kuchaytiradi va xodimlarga faqat bitta variantni qoldiradi, bu nima bo’lishidan qat’iy nazar jazodan qochish, ya’ni aybini yashirishga harakat qilishadi.

Mas’uliyatsiz xodimlar tomonidan zarar. Hodisalarni yashirish muammosi bilan bir qatorda, xodimlarning mas’uliyatsizligi xavfsizlik hodisasi bilan bog’liq bo’lsa, firma ma’lumotlari va tizim yaxlitligiga jiddiy ta’sir ko’rsatishi mumkin.

Misol uchun, 46% bu hodisalar ularning biznes ma’lumotlarining oshkor etilishi yoki xodimlarning xatti-harakatlari tufayli oshkor etilishiga olib kelganligini tasdiqlaydi. Bundan tashqari, chorakdan ortig’i

(28%) mas’uliyatsiz xodimlar natijasida maxfiy ma’lumotlarini yo’qotganligi, 25% esa to’lov ma’lumotlarini yo’qotganligini ko’rsatmoqda. Bularning barchasi, shubhasiz, biznesning obro’siga - ichki va tashqi miqyosda keng qamrovli va zararli ta’sir ko’rsatishi mumkin.

Biznes korxonalarda BYOD muammosi. Tadqiqot natijalari shuni ko’rsatadiki, korxonalar ham, xodimlar ham *o’z qurilmangizni olib kelish (BYOD)* tendensiyasini yaxshi bilishlariga qaramay, BYOD hali ham katta va kichik kompaniyalar uchun bosh og’rig’iga sabab bo’lmoqda. Ya’ni hali-hamon dunyo bo’ylab biznes BYOD haqida tashvishlanmoqda.

Kichik kompaniyalar uchun tashvishlar odatda xodimlarning BYOD amaliyotlari atrofida aylanadi, korxonalar esa xavfsizlikni boshqarish bilan kurashish ehtimoli ko’proq. Masalan, korxonalarning deyarli yarmi (48%) xodimlarning o’zlari ishga olib kelgan mobil qurilmalari orqali kompaniya ma’lumotlarini noo’rin almashishidan xavotirda bo’lishadi. Kichik biznes uchun bu alohida tashvish tug’diradi (57%), ehtimol, qisman, bu yirik korxonalar xarajatlarni qisqartirish va mobil ishchi kuchidan foydalanish uchun BYOD siyosatini qabul qilishga moyilligi bilan bog’liq.

Korxonalarda esa foydalanuvchilar qurilmalaridagi xavfsizlikni boshqarish qiyinroq kechadi. Yarimdan sal ko’proq (51%) qismi, kichik biznesning beshdan ikki qismi (42%) bilan solishtirganda, bu ular uchun tashvish ekanligini bildiradi.

Korxonalarning BYOD bilan bog’liq bo’lishi mumkin bo’lgan sabablarning bir qismi BYOD pirovardida xodimlarning mas’uliyatiga va ularning shaxsiy qurilmalaridagi biznes ma’lumotlariga yaxshi munosabatda bo’lish qobiliyatiga bog’liq. Bu jarayon har doim ham silliq kechmaydi - odamlar qurilmalarini yo’qotadilar va qurilmalar o’g’irlanadi. Asosan, qurilma ish muhitidan qanchalik ko’p olib ketilsa, u shunchalik xavf ostida bo’ladi.

Tadqiqotlar shuni ko’rsatadiki, korxonalarning yarmidan ko’pi (54%) xodimlar qurilmalarini yo’qotganligi sababli ma’lumotlar oshkor bo’lgan. Xodimlarning ehtiyotsizligi kiberxavfsizlik hodisalarining 48 foiziga bevosita hissa qo’shgan, bu qurilmalar o’g’irlanishidan ham ko’proq hodisalarni tashkil etgan, bu esa hodisalarning uchdan bir qismiga (37%) hissa qo’shgan.

AT xavfsizligi siyosati. AT xavfsizligi siyosati mavjud bo’lishining o’zi yetarli emas. Siyosat yolg’iz o’zi biznesni tahdidlardan himoya qila olmaydi. Ya’ni, bunda IT xavfsizlik siyosati ular uchun mo’ljallangan

xodimlar tomonidan har doim ham amal qilinmaydi, yoki xavfsizlik siyosati barcha mumkin bo'lgan risklarni to'laqonli qoplay olmaydi.

Kasperskiy Laboratoriyasi tadqiqotlari shuni ko'rsatadiki, kompaniyalarning 44 foizi xodimlarning IT xavfsizligi siyosatiga to'laqonli rioya qilmasligini aytishadi. Bundan ham qiziq tomoni shundaki, korxonalarning beshdan ikki qismi bizga xodimlar o'zlarining xavfsizlik siyosatlariga rioya qilmayotganliklarini tan olishgan bo'lsalarda, korxonalar muammoni o'zlari hal qilish uchun deyarli hech narsa qilmaydi, atigi chorak qismi (26%) o'z qoidalarini bajarishni rejalashtiradi. Bu natijalar xodimlar orasida AT xavfsizligi siyosati xar doim xam aktual emasligini ko'rsatadi.

Ko'pgina hollarda, siyosat shu qadar qiyin tarzda yozilganki, ularni xodimlar tomonidan samarali tarzda o'zlashtirib bo'lmaydi. Risklar, xavf-xatarlar va yaxshi amaliyotlarni aniq va keng qamrovli ko'rsatmalarda yetkazish o'rniga, korxonalar ko'pincha xodimlarga hamma imzolaydigan, lekin juda kam o'qiydigan va hatto kamroq tushunadigan ko'p sahifali hujjatlarni berishadi.

Lekin, aniq qiyinchiliklarga qaramay, korxonalar risk muammosini ichkaridan hal qilishga harakat qilmoqdalar. Xodimlarni o'qitish va xavfsizlik siyosatini amalga oshirishga yordam berish uchun jarayonga ko'proq maxsus xodimlarni jalb qilish xodimlarning ehtiyotsizligi muammosiga mantiqiy javobdir. Va bu butun dunyo bo'ylab ko'plab korxonalar amalga oshirishga intilayotgan javob hisoblanadi.

Yuqorida aytib o'tganimizdek, xavfsizlik siyosatining mavjudligining o'zi yetarli emas. Xodimlarning ehtiyotsizligi yoki xabardor bo'lmagan xodimlar tufayli yuzaga keladigan xavflarning oldini olish uchun siyosat va majburiyat o'rtasida to'g'ri muvozanatni saqlash kerak.

Xodimlarni o'qitish xodimlar o'rtasida xabardorlikni oshirish va ularni kibertahdidlar va ularga qarshi choralarga e'tibor berishga undashda muhim ahamiyatga ega – hattoki bu o'zlarining xos vazifalariga kirmasa ham. Yangilanishlarni o'rnatish, zararli dasturlardan himoyalanish yoqilganligini ta'minlash va shaxsiy parollarni to'g'ri boshqarish xodimning vazifalar ro'yxatining pastki qismida bo'lmasligi kerak. Xodimlarni jalb qilish va o'qitish kabi xodimlarga yo'naltirilgan xavfsizlik choralari korxonalar tomonidan kelajakdagi kibertahdidlardan o'zlarini himoya qilish uchun qo'llaniladigan eng maqbul taktikalardan biridir.

Kasperskiy laboratoriyasida biznesni kibertahdidlardan himoya

qilishning eng yaxshi usuli bu to’g’ri vositalar va amaliyotlarning kombinatsiyasi ekanligi takidlanadi. Xodimlar uchun xabardorlikni oshirish bo’yicha treningdan tashqari, himoya AT xavfsizlik guruhlari uchun korporativ tarmoqni ko’proq ko’rinadigan va boshqarish mumkin bo’lgan xavfsizlik yechimlarini o’z ichiga olishi kerak.

Spam, fishing va to’lov dasturi (Ransomware)ni o’z ichiga olgan bexabar yoki beparvo xodimlar bilan bog’liq tahdidlarning aksariyati so’nggi nuqta xavfsizligi yechimlari bilan hal qilinishi mumkin. Funktsionallik, oldindan sozlangan himoya yoki ilg’or xavfsizlik sozlamalari bo’yicha o’rta va yirik darajadagi kompaniyalarning alohida ehtiyojlarini qondira oladigan moslashtirilgan mahsulotlar mavjud.

Keltirilgan tadqiqotlarga ko’ra, xodimlar har xil shakllarda hujum vektoriga aylanishi mumkin: ular beparvo bo’lishi mumkin, ular xabardor bo’lmagan bo’lishi yoki ularning harakatlari zararli bo’lishi mumkin. Mobillik tendentsiyalari shuni anglatadiki, beparvo yoki xabardor bo’lmagan xodimlar xato qilish ehtimoli ko’proq bo’lishi mumkin va fishing va ijtimoiy muhandislik kabi tahdidlar, shuningdek, qonuniy va zararli faoliyat o’rtasidagi farqni qanday aniqlashni bilmaydigan xodimlar tomonidan biznesga xavf ortishi mumkin. Agar ular kiberxavfsizlik hodisasini keltirib chiqargan bo’lsa (yoki voqea ortida turgan omillardan biri bo’lsa), xodimlar sodir bo’lgan voqeani yashirib qo’yishi mumkin, bu esa ba’zi buzilishlarni uzoq vaqt davomida oshkor etilmasligi va biznesni yanada ko’proq xavf ostiga qo’yishi mumkin.

Xavfsizlik siyosatining mavjudligi juda muhim bo’lsa-da, korxonalar siyosat barcha risklarni qoplay olmasligini ham tan olishlari kerak. Bundan tashqari, xodimlar har doim ham o’z siyosatlariga qat’iy rioya qilmaydi. Xodimlar o’z harakatlarining ta’siridan ko’proq xabardor bo’lishlari uchun trening bilan birgalikda korporativ tarmoqlarning ko’proq ko’rinishi va markazlashtirilgan xavfsizligini boshqarishni ta’minlaydigan yechimlarga aniq ehtiyoj bor. Faqatgina xodimlarni xavfsiz ishlashning muhimligi haqida o’rgatish orqali korxonalar ushbu maxsus hujum vektori xavfini kamaytirishga yordam berishi va ular uchun eng muhim bo’lgan ma’lumotlarini himoya qilishi mumkin bo’ladi.

Nazorat savollari:

1. Tashkilotning axborot xavfsizligi siyosati qanday asosiy elementlarni o'z ichiga olishi kerak?

2. Axborot xavfsizligi siyosatini ixtiyoriy ravishda ishlab chiqish va amalga oshirishdan tashkilot qanday foyda keltirishi mumkin?

3. Qanday xalqaro axborot xavfsizligi standartlari mavjud va ular

tashkilotga o'z axborot aktivlarini himoya qilishga qanday yordam berishi mumkin?

4. Tashkilotda axborot xavfsizligi siyosati mavjud bo'lmasa yoki unga rioya qilmasa, qanday xavf va tahdidlar paydo bo'lishi mumkin?

5. Axborot xavfsizligi siyosati tashkilotga axborot xavfsizligi hodisalarini boshqarish va kamaytirishga qanday yordam berishi mumkin?

6. Tashkilotning axborot xavfsizligi siyosati qanday asosiy elementlarni o'z ichiga olishi kerak?

7. Axborot xavfsizligi siyosatini ixtiyoriy ravishda ishlab chiqish va amalga oshirishdan tashkilot qanday foyda keltirishi mumkin?

8. Qanday xalqaro axborot xavfsizligi standartlari mavjud va ular tashkilotga o'z axborot aktivlarini himoya qilishga qanday yordam berishi mumkin?

9. Tashkilotda axborot xavfsizligi siyosati mavjud bo'lmasa yoki unga rioya qilmasa, qanday xavf va tahdidlar paydo bo'lishi mumkin?

10. Axborot xavfsizligi siyosati tashkilotga axborot xavfsizligi hodisalarini boshqarish va kamaytirishga qanday yordam berishi mumkin?

V BOB. BOSHQARISH VA FOYDALANISHDAGI SIYOSATLAR

5.1-§. Huquqni muxofaza qilish organlarining kiberxavfsizlikni oldini olishdagi o‘rni

Huquqni muhofaza qilish organlari kiberxavfsizlik tahdidlarini bartaraf etishda hal qiluvchi rol o’ynaydi, chunki ular kiberjinoyatlarni tergov qilish va ta’qib qilish uchun javobgardir. Huquqni muhofaza qilish organlari xodimlari kibertahdidlarni samarali aniqlash, tahlil qilish va ularga javob berish uchun zarur bo’lgan bilim va ko’nikmalarga ega bo’lishi kerak. Ular kiberxavfsizlik bo’yicha mutaxassislar va boshqa manfaatdor tomonlar bilan hamkorlikda xavflarni yumshatish va kiberjinoyat sodir bo’lishining oldini olishlari kerak.

Har kuni jismoniy shaxslar, tashkilotlar va hukumatlar duch keladigan turli xil kibertahdidlar va xavflar mavjud. Kiberxavfsizlikning eng keng tarqalgan tahdidlaridan ba’zilari zararli dasturlar, fishing, to’lov dasturi, ijtimoiy muhandislik, xakerlik va xizmat ko’rsatishni rad etish (DoS) hujumlarini o’z ichiga oladi. Zararli dastur deganda kompyuter tizimlari yoki tarmoqlariga zarar yetkazish, o’chirish yoki ruxsatsiz kirishni qo’lga kiritish uchun mo’ljallangan dasturiy ta’minot tushuniladi. Fishing maxfiy ma’lumotlarni oshkor qilish yoki zararli dasturlarni o’rnatish uchun foydalanuvchilarni aldash uchun soxta elektron pochta xabarlari, xabarlar yoki veb-saytlardan foydalanishni o’z ichiga oladi. Ransomware - bu fayllarni shifrlaydigan yoki to’lov to’lanmaguncha foydalanuvchilarni qurilmalaridan bloklaydigan zararli dastur turi. Ijtimoiy muhandislik maxfiy ma’lumotlarni oshkor qilish uchun shaxslarni manipulyatsiya qilishni anglatadi. Xakerlik ruxsatsiz kirish uchun kompyuter tizimlaridagi zaifliklardan foydalanishni o’z ichiga oladi. DoS hujumlari server yoki tarmoqning ishdan chiqishiga yoki ishlamay qolishiga olib keladigan trafik bilan to’lib ketishini o’z ichiga oladi.

Kibertahdidlarning tabiati doimiy ravishda o’zgarib turadi va muntazam ravishda yangi xavflar paydo bo’ladi. Xakerlar va kiberjinoyatchilar hujumlarni amalga oshirish uchun sun’iy intellekt (AI) va mashinali o’rganish (ML) kabi ilg’or usullardan foydalangan holda o’z usullarida tobora murakkablashmoqda. Bulutli hisoblash va buyumlar internetining (IoT) keng qo’llanilishi ham hujum maydonini kengaytirib, kiberjinoyatchilarga jismoniy shaxslar va tashkilotlarni nishonga olishni osonlashtirdi. Ijtimoiy tarmoqlar va onlayn platformalarning ko’payishi,

shuningdek, yovuz niyatli shaxslarning yolg'on ma'lumotlarni tarqatish va jamoatchilik fikriga ta'sir qilishini osonlashtirdi.

Kiberjinoyat shaxslar, tashkilotlar va hukumatlarga jiddiy ta'sir ko'rsatadi. Jismoniy shaxslar moliyaviy yo'qotishlarga, shaxsiy ma'lumotlarning o'g'irlanishiga yoki shaxsiy ma'lumotlarining buzilishi natijasida yuzaga keladigan zararning boshqa shakllariga duch kelishi mumkin. Tashkilotlar kiberhujumlar tufayli obro'siga putur etkazishi, moliyaviy yo'qotishlar yoki intellektual mulkni yo'qotishi mumkin. Hukumatlar milliy xavfsizlikka tahdidlar yoki kiber josuslik yoki kiberhujumlar natijasida maxfiy ma'lumotlarni yo'qotishi mumkin.

Huquqni muhofaza qilish organlari va kiberxavfsizlik bo'yicha ekspertlar o'rtasidagi hamkorlik. Bugungi raqamli asrda huquq-tartibot idoralari kiberjinoyatchilik xavfi ortib borayotganiga qarshi kurashishda jiddiy muammolarga duch kelmoqda. Kiberjinoyatchilar tomonidan tobora murakkablashib borayotgan taktikalar oldida jinoyatchilikka qarshi kurashning an'anaviy usullari endi yetarli emas. Shunday qilib, samarali kiberxavfsizlik huquqni muhofaza qilish organlari va kiberxavfsizlik bo'yicha mutaxassislar o'rtasida hamkorlikdagi sa'y-harakatlarni talab qiladi. Ushbu ikki guruh o'rtasidagi fanlararo hamkorlik zarurligini ortiqcha baholab bo'lmaydi.

Huquqni muhofaza qilish organlari va kiberxavfsizlik bo'yicha mutaxassislar o'rtasidagi hamkorlik kibertahdidlarni samarali aniqlash, oldini olish va tekshirishni ta'minlash uchun muhim ahamiyatga ega. Ikkala guruh ham kibertahdidlarni samarali hal qilish uchun zarur bo'lgan noyob tajriba va istiqbolga ega. Huquqni muhofaza qilish organlari qonuniy vakolat va tergov vakolatlariga ega, kiberxavfsizlik bo'yicha mutaxassislar esa maxsus texnik ko'nikmalarga va kiber tahdidlar bo'yicha bilimga ega. Shu sababli, hamkorlikdagi yondashuv kiberjinoyatning ham huquqiy, ham texnik jihatlarini ko'rib chiqishga yordam beradi.

Xususiy sektor kiberxavfsizlik firmalari kibertahdidlarni yumshatishda hal qiluvchi rol o'ynashi mumkin. Ushbu firmalar odatda eng yangi texnologiyalar va vositalarga ega bo'lib, ularni kiberhujumlarni aniqlash va oldini olish uchun yaxshi jihozlangan qiladi. Huquqni muhofaza qilish idoralari xususiy sektor kiberxavfsizlik firmalari bilan ishlashdan bir necha usulda, jumladan, ekspertizadan foydalanish, ma'lumot almashish va qo'shma tekshiruvlardan foydalanishlari mumkin.

Axborot almashish kiberxavfsizlikning muhim tarkibiy qismidir va xususiy sektor firmalari huquqni muhofaza qilish organlariga qimmatli

ma’lumotlar va razvedka ma’lumotlarini taqdim etishi mumkin. Xususiy sektor firmalari paydo bo’layotgan kibertahdidlar, hujum shakllari va yangi zararli dasturlar haqida ma’lumot almashish orqali huquqni muhofaza qilish organlariga kibertahdidlarni yaxshiroq tushunish va oldindan ko’rishda yordam berishi mumkin. Bundan tashqari, xususiy sektor firmalari huquqni muhofaza qilish organlariga potentsial gumonlanuvchilarni aniqlash va kiberjinoyatchilarni kuzatishda yordam berishi mumkin.

Samarali kiberxavfsizlik axborot almashish va razvedka ma’lumotlarini yig’ishga proaktiv yondashuvni talab qiladi. Huquqni muhofaza qilish idoralari boshqa idoralar, xususiy sektor firmalari va xalqaro hamkorlar bilan paydo bo’layotgan kibertahdidlar bo’yicha razvedka ma’lumotlarini almashish uchun hamkorlik qilishi kerak. Bunday ma’lumot almashish jinoiy faoliyat shakllarini aniqlashga yordam beradi va huquqni muhofaza qilish organlariga kiberhujumlarning oldini olish va ularga javob berish bo’yicha samarali strategiyalarni ishlab chiqish imkonini beradi.

Samarali ma’lumot almashish, shuningdek, eng yaxshi tajribalar va olingan saboqlarni almashishni o’z ichiga oladi. Huquqni muhofaza qilish organlari kelajakdagi tahdidlarga yaxshiroq tayyorgarlik ko’rish uchun oldingi voqealardan saboq olishlari kerak. Ushbu ma’lumotni boshqa agentliklar va kiberxavfsizlik bo’yicha mutaxassislar bilan baham ko’rish umumiy kiberxavfsizlikni yaxshilashga yordam beradi va huquqni muhofaza qilish organlari kiberhujumlarning oldini olish va ularga javob berish uchun yaxshi jihozlanishini ta’minlaydi.

Kiberjinoyatlarni tekshirish va raqamli kriminalistika. Kiberjinoyatlarni tergov qilish maxsus ko’nikma va bilimlarni talab qiladi. Huquq-tartibot idoralari dalillar to’plash, kiberjinoyatchilarni izlash va jinoiy javobgarlikka tortish uchun ish yaratish uchun turli texnika va vositalardan foydalanishi kerak. Ushbu texnikalar va vositalar quyidagilarni o’z ichiga oladi:

1. **Tarmoq kriminalistikasi:** Bu ruxsatsiz kirishga urinishlar yoki ma’lumotlarni o’tkazib yuborish kabi shubhali faoliyat namunalarini aniqlash uchun tarmoq trafigini tahlil qilishni o’z ichiga oladi;
2. **Zararli dasturlarni tahlil qilish:** Bu hujumning kelib chiqishi va kiberjinoyatchilar tomonidan qo’llaniladigan taktikani aniqlash uchun zararli dastur kodini tahlil qilishni o’z ichiga oladi;
3. **Ijtimoiy muhandislik:** Bu shaxslarni maxfiy ma’lumotlarni oshkor qilish yoki ularning xavfsizligiga putur etkazadigan harakatlarni

amalga oshirish uchun manipulyatsiya qilish uchun psixologik usullardan foydalanishni o’z ichiga oladi;

4. **Kriptografiya:** Bu maxfiy xabarlar yoki jinoiy faoliyat maxfiyligini ochish uchun shifrlangan ma’lumotlarni tahlil qilishni o’z ichiga oladi.

Raqamli dalillar anchagina mo’rt bo’lib, to’g’ri ishlatilmasa, osongina yo’qolishi yoki buzilishi mumkin. Huquqni muhofaza qilish idoralari raqamli dalillarni sudda qabul qilinishini ta’minlash uchun to’plash va saqlashga katta e’tibor berishlari kerak. Bu dalillar to’plangan paytdan boshlab sudga taqdim etilgunga qadar ularning ko’rib chiqilishini kuzatib boradigan zanjirini o’rnatishni o’z ichiga oladi.

Huquqni muhofaza qilish organlari raqamli dalillarni olish uchun qonuniy talablardan ham xabardor bo’lishi kerak. Bu order yoki sud qarorini olish yoki chet eldan dalillar olish uchun xalqaro hamkorlar bilan ishlashni o’z ichiga olishi mumkin. Qonuniy talablarga rioya qilmaslik dalillarni suddan chiqarib yuborishga olib kelishi mumkin.

Kiberxavfsizlikning huquqiy asoslari. Kiberxavfsizlik qonunlari va qoidalari kibertahdidlar va hujumlarni yumshatishda hal qiluvchi ahamiyatga ega. Ular huquqni muhofaza qilish organlariga kiberjinoyatchilarni tekshirish va jinoiy javobgarlikka tortish uchun asos yaratadi, shu bilan birga shaxslar va tashkilotlarning kiber tahdidlardan himoyalanishini ta’minlaydi. Misol sifatida keltiradigan bo’lsak, Amerika Qo’shma Shtatlarida kiberxavfsizlik qonunlari va qoidalari federal va shtat darajasida qo’llaniladi. Kiberxavfsizlikni tartibga soluvchi asosiy federal qonunlar qatoriga Kompyuter firibgarligi va suiiste’moli to’g’risidagi qonun (CFAA), Elektron kommunikatsiyalar maxfiyligi to’g’risidagi qonun (ECPA) va Kiberxavfsizlik ma’lumotlarini almashish to’g’risidagi qonun (CISA) kiradi.

CFAA himoyalangan kompyuter tizimlariga, jumladan, davlat va moliya institutlari tarmoqlariga ruxsatsiz kirishni taqiqlaydi. ECPA elektron xabarlarni, shu jumladan elektron pochta va telefon suhbatlarini ushlash va oshkor qilishni tartibga soladi. CISA kiberhujumlarning oldini olish va ularga javob berish uchun xususiy va davlat tashkilotlari o’rtasida ma’lumot almashishni rag’batlantiradi. Bundan tashqari, davlat darajasidagi qonunlar va qoidalar mavjud bo’lib, ular qo’shimcha yo’l-yo’riq va himoyani ta’minlaydi, masalan, ma’lumotlar buzilishi haqida xabar berish qonunlari.

Kiberxavfsizlik tekshiruvlarida yurisdiktsiya muammolari paydo bo’ladi, chunki kiberhujumlar ko’pincha dunyoning turli joylaridan kelib

chiqadi. Kiberjinoyatchilar o’z shaxsi va joylashuvini yashirishi mumkin, bu ularni kuzatish va jinoiy javobgarlikka tortishni qiyinlashtiradi. Bu huquq-tartibot idoralari uchun qiyinchilik tug’diradi, chunki ular xalqaro hamkorlar bilan kiberjinoyatchilarni tergov qilish va jinoiy javobgarlikka tortish uchun ishlashlari kerak.

Xalqaro hamkorlik kibertahdidlarni yumshatishda hal qiluvchi ahamiyatga ega, chunki kiberjinoyat global muammo bo’lib, muvofiqlashtirilgan javob choralarini talab qiladi. Yevropa Kengashining Kiberjinoyatlar to’g’risidagi konventsiyasi, shuningdek, Budapesht konventsiyasi sifatida ham tanilgan, kiberjinoyat qonunlarini uyg’unlashtirish va kiberjinoyatlarni tergov qilishda xalqaro hamkorlikni osonlashtirishga qaratilgan xalqaro shartnomadir. Konvensiya 60 dan ortiq mamlakatlar tomonidan ratifikatsiya qilingan va kiberjinoyatchilikka qarshi kurashda yetakchi xalqaro hujjat hisoblanadi.

Maxfiylik va fuqarolar erkinliklarini himoya qilish kiberxavfsizlik sohasidagi sa’y-harakatlarning muhim jihati hisoblanadi. Huquq-tartibot idoralari kiberjinoyatchilarni tergov qilishlari va jinoiy javobgarlikka tortishlari kerak bo’lsa-da, ular buni shaxslarning huquqlarini buzmaydigan tarzda amalga oshirishlari kerak. Maxfiylikni himoya qilishning bir misoli elektron qurilmalar va ma’lumotlarni qidirish va musodara qilish uchun orderlardan foydalanishdir. Garantlar ehtimoliy sabablarni talab qiladi va tintuv va olib qo’yish qonuniy va mutanosib bo’lishini ta’minlash uchun sud tomonidan tekshirilishi kerak.

Bundan tashqari, kiberxavfsizlik choralari shaxslarning shaxsiy hayoti va fuqarolik erkinliklarini buzishga emas, balki ularni himoya qilishga qaratilgan bo’lishi kerak. Masalan, shifrlash va anonimlashtirish texnologiyalari shaxslarning shaxsiy daxlsizligini himoya qilishi va ma’lumotlar buzilgan taqdirda ularning shaxsiy ma’lumotlari oshkor qilinmasligini ta’minlashi mumkin. Huquqni muhofaza qilish organlari samarali kiberxavfsizlik choralari zarurligini shaxslarning shaxsiy hayoti va fuqarolik erkinliklarini himoya qilish bilan muvozanatlashi kerak.

Huquqni muhofaza qilish organlari xodimlarining kiberxavfsizlik bo’yicha bilim va ko’nikmalarini oshirishda ta’lim va o’qitish dasturlari muhim ahamiyatga ega. Ushbu dasturlar huquqni muhofaza qilish organlari xodimlariga kiberjinoyatlarni tekshirish va kiberhujumlarning oldini olish uchun zarur ko’nikmalarni beradi. Kiberxavfsizlik bo’yicha ta’lim va o’qitish dasturlari tarmoq xavfsizligi, raqamli kriminalistika, hodisalarga javob berish va tahdidlarni razvedka kabi bir qator mavzularni qamrab oladi.

Jamoatchilikni xabardor qilish kampaniyalari kiberxavfsizlik bo'yicha ilg'or tajribalarni ilgari surish va kibertahdidlar haqida xabardorlikni oshirishda muhim ahamiyatga ega. Ushbu kampaniyalar jismoniy shaxslar va tashkilotlarni fishing va zararli dasturlar kabi kiberhujumlardan qanday himoya qilish haqida o'rgatadi. Jamoatchilikni xabardor qilish kampaniyalari, shuningdek, shaxsiy va maxfiy ma'lumotlarga ruxsatsiz kirishni oldini olish uchun kuchli parollar, ikki faktorli autentifikatsiya va boshqa xavfsizlik choralaridan foydalanishni rag'batlantirishi mumkin.

Jamoalar va korxonalar bilan hamkorlik kiberxavfsizlikni kuchaytirishda muhim ahamiyatga ega. Huquqni muhofaza qilish idoralari kiber tahdidlarni aniqlash va yumshatish uchun biznes bilan hamkorlik qilishi mumkin. Bundan tashqari, ular kibertahdidlar haqida xabardorlikni oshirish va kiberxavfsizlik bo'yicha ilg'or tajribalarni ilgari surish uchun jamoat guruhlari bilan ishlashlari mumkin. Ushbu hamkorlik zaifliklarni aniqlashga va kiberxurujlarning oldini olish uchun kiberxavfsizlik choralarini kuchaytirishga yordam beradi..

Huquq-tartibot idoralari kiber hodisalarga tez va samarali javob berishga tayyor bo'lishi kerak, xoh ular davlat idoralariga yoki xususiy sektor tashkilotlariga hujumlar bilan bog'liq. Hodisalarga samarali javob berishning asosiy tarkibiy qismlaridan biri bu hodisalarga javob berish rejalari va protokollarini ishlab chiqishdir. Ushbu rejalar va protokollar huquqni muhofaza qilish organlari xodimlariga har xil turdagi kiber hodisalarga qanday munosabatda bo'lish bo'yicha ko'rsatmalar beradi, jumladan, voqeani qanday aniqlash va ushlab turish, dalillarni qanday saqlash va boshqa idoralar va manfaatdor tomonlar bilan qanday muvofiqlashtirish.

Kiber hodisalar ko'pincha bir nechta agentliklar va manfaatdor tomonlar, jumladan, boshqa huquqni muhofaza qilish idoralari, davlat idoralari, xususiy sektor tashkilotlari va xalqaro hamkorlarni jalb qilishni talab qiladi. Hodisaga samarali javob berish, hodisaning oldini olish va ta'sirni kamaytirishni ta'minlash uchun ushbu tashkilotlar o'rtasida yaqin muvofiqlashtirish va hamkorlikni talab qiladi. Huquq-tartibot idoralari muvofiqlashtirilgan javobni ta'minlash uchun ushbu tuzilmalar bilan aniq aloqa va hamkorlikni yo'lga qo'yishlari kerak.

Hodisaga samarali javob berish uchun o'z vaqtida va samarali muloqot muhim ahamiyatga ega. Huquqni muhofaza qilish organlari kibertahdidlarni tezda aniqlash va baholash va bu ma'lumotlarni boshqa idoralar va manfaatdor tomonlarga etkazish imkoniyatiga ega bo'lishi

kerak. Buning uchun mustahkam va xavfsiz aloqa infratuzilmasi, shuningdek, kiber tahdidlarni aniqlash va ularga javob berish uchun o’qitilgan xodimlar kerak bo’ladi.

Texnologik o’zgarishlarning tez sur’ati kiberxavfsizlik tahdidlarini yumshatish vazifasi yuklangan huquqni muhofaza qilish idoralari uchun asosiy muammo hisoblanadi. Sun’iy intellekt va narsalar interneti kabi yangi texnologiyalar yangi zaifliklar va hujum vektorlarini yaratmoqda, ularni hal qilish kerak. Huquqni muhofaza qilish idoralari ushbu o’zgarishlardan xabardor bo’lishlari va kiberjinoyatchilardan oldinda qolish uchun o’z strategiyalari va taktikalarini doimiy ravishda moslashtirishlari kerak.

Kibertahdidlarning doimiy rivojlanib borayotgan tabiati huquq-tartibot idoralaridan paydo bo’layotgan tahdidlarga samarali javob berish uchun o’z malakalari va strategiyalarini doimiy ravishda moslashtirishni talab qiladi. Bu huquqni muhofaza qilish organlari xodimlarini so’nggi tahdidlar va texnologiyalardan xabardor bo’lishlari uchun doimiy o’qitish va o’qitish, shuningdek, ularning maxsus bilim va ko’nikmalariga ega bo’lish uchun kiberxavfsizlik bo’yicha mutaxassislar bilan hamkorlikni rivojlantirishni o’z ichiga oladi.

Huquqni muhofaza qilish organlari kibertahdidlardan himoya qilish zarurati bilan shaxslar va tashkilotlarning shaxsiy hayoti va fuqarolik erkinliklarini himoya qilish zaruratini muvozanatlashi kerak. Bu fuqarolik erkinliklari va shaxsiy daxlsizlikka potentsial ta’sirni hisobga oladigan kiberxavfsizlik sa’y-harakatlariga puxta va nozik yondashuvni talab qiladi.

So’nggi yillarda kiberjinoyatlar bo’yicha ko’plab shov-shuvli tekshiruvlar o’tkazildi, natijada sud jarayoni muvaffaqiyatli yakunlandi. Ushbu holatlar kiberjinoyatchilarni aniqlash, kuzatish va ushlashda huquqni muhofaza qilish idoralari va kiberxavfsizlik bo’yicha ekspertlar o’rtasidagi samarali hamkorlik muhimligini ko’rsatadi.

Huquqni muhofaza qilish idoralari va kiberxavfsizlik bo’yicha mutaxassislar o’rtasidagi hamkorlik ko’plab kiberxavfsizlik tekshiruvlarining muvaffaqiyati uchun muhim ahamiyatga ega. Huquqni muhofaza qilish organlari va kiberxavfsizlik bo’yicha mutaxassislar birgalikda ishlash orqali kibertahdidlarni yanada samarali aniqlash va ularga javob berish uchun o’z resurslari va tajribalarini birlashtirishlari mumkin.

Muvaffaqiyatli hamkorlikning bir misoli Federal, shtat va mahalliy huquq-tartibot idoralari hamda xususiy sektor hamkorlarini

kibertahdidlarni tekshirish uchun birlashtirgan FQBning Kiber-ishchi guruhidir. Ishchi guruh ko’plab nufuzli kiberjinoyatchilarni muvaffaqiyatli tergov qilish va jinoiy javobgarlikka tortishda muhim rol o’ynadi.

Yana bir misol, AQSh Kiberqo’mondonligining kiberxavfsizliklarni aniqlash va ularni yumshatish uchun xususiy sektor kiberxavfsizlik firmalari bilan hamkorligi. Hamkorlik natijasida kiber tahdidlarni aniqlash va ularga javob berish uchun innovatsion yangi texnologiyalar va strategiyalar ishlab chiqildi.

5.2-§. Ma’lumotlarni boshqarishdagi siyosatlar

Zaxiralash va qayta tiklash siyosati. Bugungi biznes dunyosida axborot kuchdir. Ma'lumotlar 21 - asrning yangi neftidir. Raqobat ustunligingizni saqlab qolish uchun siz apparat va dasturiy ilovalar uchun ishonchli zaxira va tiklash siyosatiga ega bo'lishingiz kerak. Ogohlantirishsiz ma'lumotlaringiz yo'qolishi yoki buzilishini oldini olishda zaxiralash va qayta tiklash siyosati muhim ro’l o'ynaydi.

Zaxiralash va tiklash siyosati ma'lumotlarning qanday zaxiralanishi, falokatdan keyin tiklash uchun qanday choralar ko'rilishi va zahira nusxalariga kimlar kirishi mumkinligini ko'rsatadigan hujjatdir. Ushbu hujjat sizning qimmatli ma'lumotlaringizni yo’qolishi, buzilishini oldini olishga yordam beradi. “Zaxiralash” atamasi fayllar yoki tizimlar yo'qolgan, o'chirilgan yoki buzilgan taqdirda ularni qayta tiklash uchun ishlatiladigan ma'lumotlarning nusxasi sifatida ta'riflanishi mumkin. Ushbu nusxa asl manbaning jismoniy shikastlanishidan himoya qilish uchun boshqa qurilma yoki vositada bo'lishi mumkin. Har bir korxona zaxira va tiklash siyosatiga ega bo'lishi kerak. Tabiiy ofatlar, apparatdagi nosozlik, inson xatosi kabi ma’lumotlaringiz yo‘qolishi yoki unga kirish imkoni bo‘lmasligiga olib keladigan ko‘plab sabablar mavjud.

Ma’lumotlarni saqlashning ikkita eng yaxshi amalyoti mavjud, ulardan biri tezkor tiklash uchun mahalliy serverda, ikkinchisi esa uzilish holatlarida ma’lumotlar saqlanib qoladigan bulutda. Zaxiralangan ma'lumotlar turli xil ma'lumotlar to'plamlarini o'z ichiga olishi mumkin, ular elektron pochta ilovalari tomonidan yaratilgan yoki keng doiradagi ilovalar, jumladan ma'lumotlar bazalari tomonidan ishlatiladigan tuzilgan va tuzilmagan ma'lumotlarni o'z ichiga oladi. Tashkilotning ma'lumotlarni zaxiralash siyosati va ma'lumotlarni saqlash siyosati odatda bir-birini to'ldiradi.

Samarali zaxira siyosati nusxalanadigan ma'lumotni va zaxira

nusxasini amalga oshirish chastotasini, shuningdek, zaxiralangan ma'lumotlar yuboriladigan saqlash joyini aniqlaydi. Zaxiralash bo'yicha ko'rsatmalar, shuningdek, AT dastlabki to'liq zahiradan keyin amalga oshiradigan qo'shimcha zahiralash chastotasini belgilaydi. Tashkilotning zaxira siyosati, shuningdek, zaxiralash uchun mas'ul bo'lgan AT guruhi a'zolarining, jumladan, agar bu rol ITning bir qismi bo'lsa, zaxira ma'murining rollarini ham belgilaydi.

Yaxshi zaxiralash va tiklash siyosatining ba'zi maqsadlari quyidagilardir:

— Sizning biznesingiz apparat va dasturiy ta'minot nuqtai nazaridan ma'lumotlarni himoya qilish uchun nima kerakligini aniqlang. Bunga server zahiralari, virtual mashina zahiralari, ish stoli tizimlari, mobil qurilmalar, elektron pochta serverlari va boshqalar kiradi.

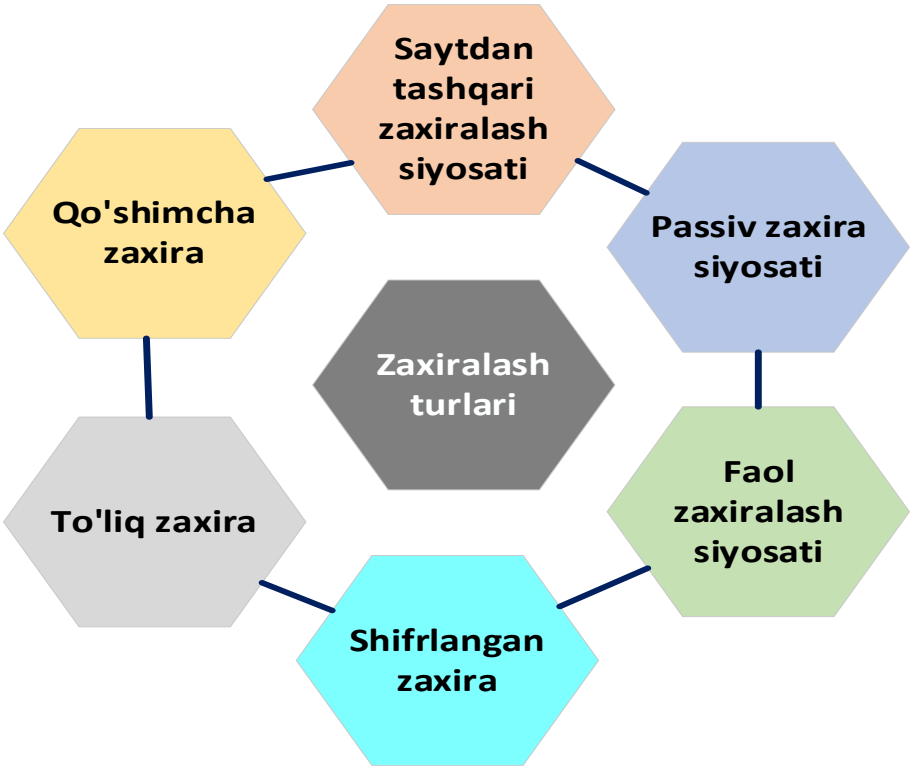
— Siz ushbu zaxira nusxalarini qanchalik tez-tez bajarishingizni va ular qachon olinishini hal qilishingiz kerak. Bu sizning kompaniyangiz talablariga, masalan, me'yoriy hujjatlarga muvofiqligi yoki buzilishlarni tiklash muddatlariga bog'liq.

— Xatolar bo'lsa, ma'lumotlar yangilangan ma'lumotlarning minimal yo'qolishi bilan izchil ravishda tiklanishi kerak.

— Ma'lumotlarning zaxira nusxasi iloji boricha real vaqtga yaqin bo'lishi kerak. Zaxira nusxalarining chastotasi himoya qilinishi kerak bo'lgan ma'lumotlar turiga bog'liq bo'lishi kerak.

— Zaxira nusxalari har doim kamida ikkita nusxaga ega bo'lishi kerak - bitta mahalliy va bitta saytdan tashqari nusxa.

Muvaffaqiyatli zaxira rejasini yaratish uchun ishlatilishi mumkin bo'lgan ko'plab zaxiralash siyosatlari mavjud (5.1-rasm):



5.1-rasm. Zaxiralash turlari

— **Saytdan tashqari zaxiralash siyosati:** Ushbu turdagi zaxira siyosatining maqsadi zaxira nusxalarini ular yaratilgan joydan farqli joyda saqlashdir. Bu yong'in yoki suv toshqini kabi mahalliy ofatdan himoya qiladi.

— **Passiv zaxiralash siyosati:** Passiv strategiya ortidagi maqsad sizning asosiy biznes maqsadlaringizga e'tibor qaratganingizda ma'lumotlaringizni zaxiralash uchun mas'ul bo'lgan boshqa shaxsga ega bo'lishdir.

— **Faol zaxiralash siyosati:** Ushbu strategiya yordamida tashkilotlar muntazam ravishda o'z nusxalarini yaratish va saqlash uchun javobgardir.

— **Shifrlangan zahira:** Agar kompaniyangiz ruxsatsiz kirishdan himoyalanishi kerak bo'lgan mijozlar ma'lumotlari yoki boshqa maxfiy ma'lumotlarga ega bo'lsa, shifrlangan zaxira nusxasi kerak bo'ladi.

— **To'liq zaxiralash** - To'liq zaxiralash butun serverning zaxira nusxasini yaratadi, ular uzoqroq vaqt davomida ishlatiladi.

— **Qo'shimcha zaxira** - Bu faqat oxirgi marta bajarilganidan beri o'zgargan narsalarni zaxiralaydi. Qo'shimcha zaxira nusxalari oxirgi to'liq zaxiradan keyin qo'shilgan yoki o'zgartirilgan har qanday faylni oladi.

Quyida esa zaxira va qayta tiklash siyosatining afzalliklari keltirilgan:

— Ushbu turdagi siyosat ma'lumotlaringizda biror narsa noto'g'ri bo'lgan taqdirda xotirjamlikni ta'minlaydi.

— Zaxira nusxalari istalgan vaqtda mavjud bo'lgani uchun siz har qanday ofatdan tezda tiklanishingiz mumkin.

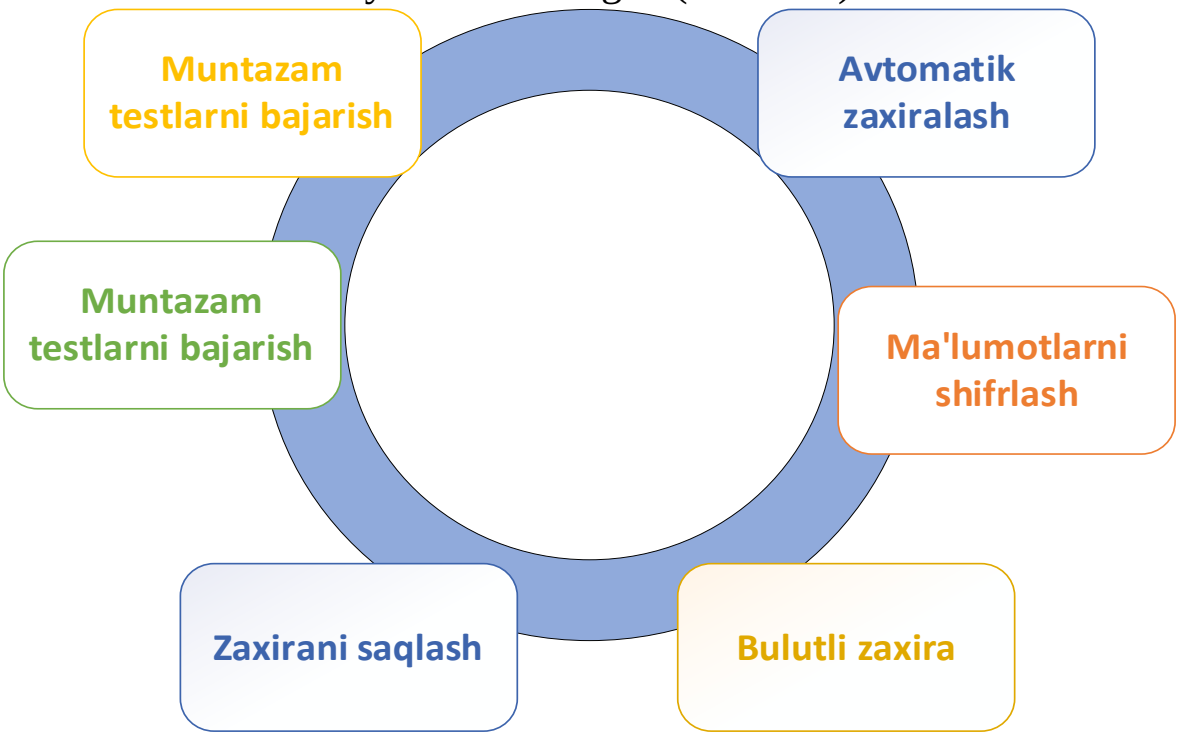
— Qattiq zaxiralash va tiklash siyosatini qo'llash, agar ish eng yuqori ish soatlarida sodir bo'lsa, soatiga minglab dollarga tushishi mumkin bo'lgan ishlamay qolishning oldini oladi.

— Zaxira nusxasi, shuningdek, tasodifiy o'chirish yoki buzilishdan himoya qiladi, agar zahiradagi bitta faylga biror narsa yuz bersa, odatda ko'proq nusxalar mavjud bo'lib, ulardan hech qanday muammosiz yo'qolgan narsalarni tiklashingiz mumkin.

— Zaxiralash siyosati zahira nusxalarini muammosiz bajarish uchun turli resurslarga tayinlangan protseduralar, jadvallar, mas'uliyatlarni aniqlaydi. Shuningdek, u zahira nusxalari qachon sodir bo'lishi mumkinligini, qanday vositalar/dasturiy ta'minotdan foydalanish kerakligini va zaxira nusxalarining joylashuvini nazorat qilish imkonini beradi.

— Ushbu siyosat zaxira nusxalarini yaratish uchun mas'ul bo'lgan resurslarni javobgar qiladi va ularning aloqa ma'lumotlarini taqdim etadi. Shuningdek, u qachon va qayerda zaxira nusxalarini amalga oshirishini aniqlaydi.

Ma’lumotlarni xavfsizligini ta’minlash uchun ham quyidagi eng yaxshi zaxiralash amaliyotlari keltirilgan (5.2-rasm):



5.2-rasm. Zaxiralash amaliyotlari.

— **Avtomatlashtirilgan zahiralash** - bu turdagi zahiralash ma'lumotlarni mahalliy tizimdan zahira nusxasiga zaxiralash va saqlash uchun kamroq yoki umuman inson aralashuvini talab qilmaydi. Avtomatik zaxiralash bilan siz hech qachon ma'lumotlaringizni qo'lda zaxiralash haqida qayg'urmasligingiz kerak. Bu jarayon inson xatosidan va fayllarning buzilishidan himoya qiladi. Bundan tashqari, tizimning umumiy ishlamay qolish xavfini kamaytiradi.

— **Ma'lumotlarni shifrlash** - bu internet orqali uzatilayotgan yoki kompyuterning qattiq diskida saqlangan shaxsiy ma'lumotlar yoki intellektual mulkni tarmog'ingizdan o'g'irlashga urinishlari mumkin bo'lgan xakerlar yoki boshqa zararli tajovuzkorlar tomonidan ma'lumotlarga ruxsatsiz kirishdan himoya qiladi.

— **Bulutli zaxira** - Bulutli saqlash barcha fayllaringiz va hujjatlaringizning zaxira nusxasini yaratish uchun internet aloqasi kuchidan foydalanadi, shunda ularga internetga ulangan istalgan joydan kirish mumkin. Bu hatto kutilmagan falokat yuz bergan taqdirda ham biznesingizni muammosiz davom ettirishning ajoyib usuli.

— **Zaxirani saqlash** - Har bir zaxira qancha vaqt saqlanishi yana bir muhim vazifadir. Har bir zaxira nusxasini saqlab qolish istalmagan. Saqlash muddati ma'lumotlaringizni qanchalik tez-tez zaxiralashingiz, qanday turdagi zaxiralash usuli qo'llanilishi va zaxira nusxalari qayerda saqlanganiga qarab o'zgaradi.

— **Muntazam testlarni o'tkazish** - Qayta tiklash rejasini sinab ko'rish, kutilmagan muammolar yuzaga kelganda tiklanish jarayonini yaxshilaydi. Rejani sinovdan o'tkazish tashkilotga nima noto'g'ri bo'lganini bilishga yordam beradi va ular tiklanish jarayonini yaxshilashlari mumkin, bu esa reja kutilganidek ishlashiga ishonch hosil qiladi.

— **Gibrid ma'lumotlarni zaxiralash yechimlari** - bu zahira dunyosida ro'y berayotgan eng so'nggi innovatsiya va tashkilotlar o'z ma'lumotlarini tabiiy va texnogen ofatlardan himoya qilishga intilayotgani sababli tobora ommalashib bormoqda. Gibrid zahiraviy yechim bilan siz ma’lumotlaringizni xavfsiz saqlashingiz va saytdan tashqarida ham, bulutli saqlash xizmatlari kabi katta oylik to‘lovlarni to‘lashdan tashvishlanmasdan ham saqlashingiz mumkin.

Ma’lumotlarni klassifikatsiyalash siyosati. *Ma'lumotlarni tasniflash siyosati* - bu kompaniyaning saqlangan ma'lumotlarini sezgirlik darajasiga qarab tasniflash, to'g'ri ishlashni ta'minlash va tashkiliy xavfni kamaytirish uchun keng qamrovli reja. Ma'lumotlarni tasniflash siyosati

har bir sinf uchun qoidalar, jarayonlar va protseduralar doirasi bilan nozik/maxfiy ma'lumotlarni aniqlaydi va himoya qilishga yordam beradi.

Ma'lumotlarni tasniflash siyosati kompaniyangiz ma'lumotlarini uning tashkilotingizga ta'sir qilish xavfiga qarab tasniflaydi. Ushbu siyosat orqali kompaniya ma'lumotlarining sezgirlik asosida qanday tasniflanishi kerakligini aniqlaydi va keyin har bir sinfga mos keladigan xavfsizlik siyosatini yaratadi. Ma'lumotlar tasnifi odatda uchta toifani o'z ichiga oladi: maxfiy, ichki va ommaviy ma'lumotlar. Siyosatni bir nechta oddiy turlar bilan cheklash tashkilotingiz ega bo'lgan barcha ma'lumotlarni tasniflashni osonlashtiradi, shuning uchun siz resurslarni eng muhim ma'lumotlaringizni himoya qilishga qaratishingiz mumkin.

Ma'lumotlarni tasniflash siyosatining afzalliklari:

— Ma'lumotlarni tasniflash siyosati tashkilotga qanday ma'lumotlardan foydalanish mumkinligini, ularning mavjudligi, qayerda joylashganligini, qanday kirish, yaxlitlik va xavfsizlik darajalari talab qilinishini hamda joriy ishlov berish va qayta ishlash dasturlari amaldagi qonunlar va qoidalarga mos keladimi yoki yo'qligini tushunishga yordam beradi.

— Bu ma'lumotlarni himoya qilishning eng samarali va samarali tizimidir, chunki u muhim, nozik va maxfiy ma'lumotlarni himoya qilish uchun ma'lumotlarni toifalarga ajratishga yordam beradi. Agar maxfiy ma'lumotlar noto'g'ri qo'llarga tushsa, tashkilotlar qonun va qoidalarni buzganliklari uchun jarimaga tortilishi mumkin va ular moliyaviy yo'qotish yoki obro'siga putur yetkazishi mumkin.

— Ma'lumotlarni tasniflash siyosati tashkilotlarga me'yoriy hujjatlarga, shuningdek, sanoatning ilg'or amaliyotlari va mijozlar kutganlariga javob berishga yordam beradi.

— Bu, shuningdek, tashkilotlarga himoyani talab qiladigan maxfiy ma’lumotlar miqdori, ularning joylashgan joyi va tahdidlar manzarasidan kelib chiqib, qanday xavfsizlik choralariga sarmoya kiritishni aniqlash imkonini berib, belgilangan xavfsizlik fondlarini optimallashtirishga yordam beradi.

Ma’lumotlarni klassifikatsiya qilishning uchta turi mavjud:

Maxfiy ma'lumotlar

Maxfiy ma'lumotlarni kompaniyaning qimmatbaho toshlari sifatida ko'rib chiqing. Agar u sizning qo'lingizdan chiqsa, bu ma'lumot tashkilotga jiddiy moliyaviy zarar yetkazishi mumkin. Maxfiy ma'lumotlar biznesga strategik ustunlikni ta'minlaydigan deyarli barcha narsalarni o'z ichiga oladi. Kompaniyalar ko'pincha ma'muriy, jismoniy

va texnik nazoratning qolgan qismini yaratish uchun asosiy nuqta sifatida Maxfiy ma'lumotlardan foydalanadilar.

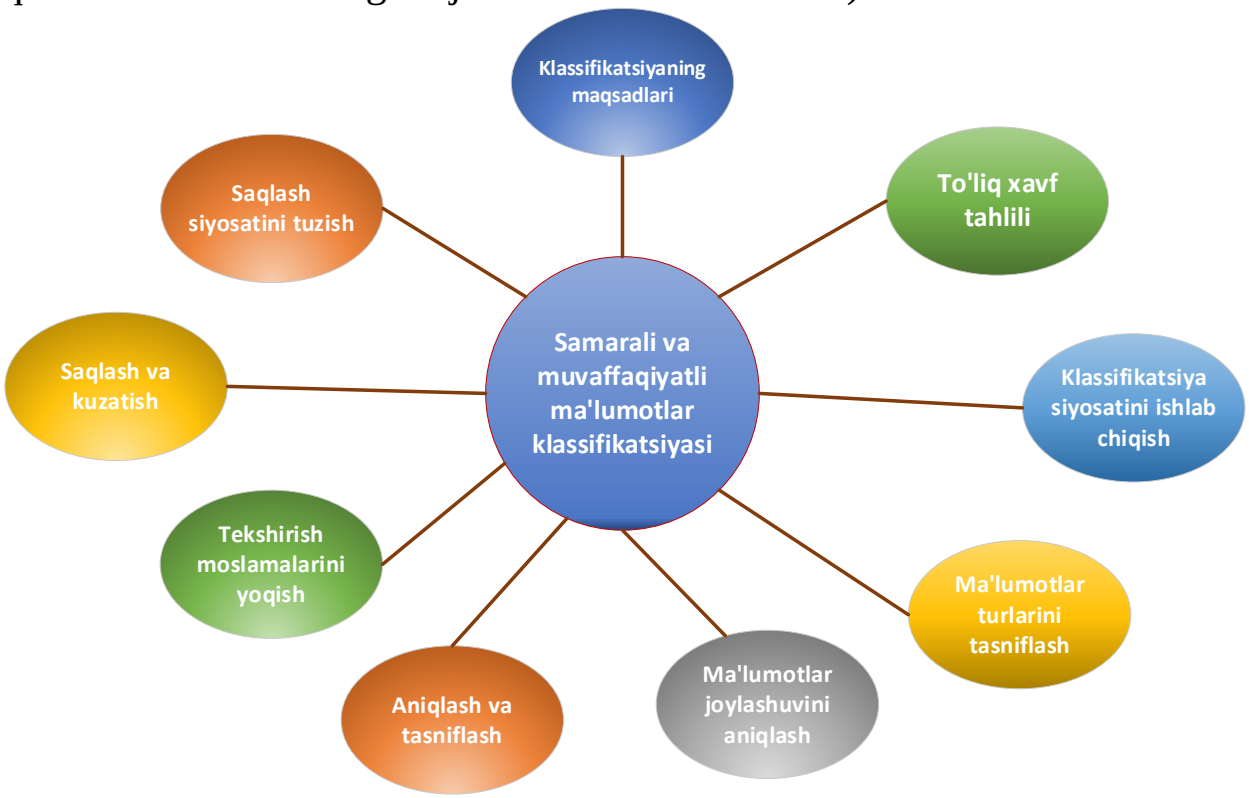
Ichki ma'lumotlar

Ichki ma'lumotlar - bu sizib chiqqan taqdirda kompaniyaga o'rtacha xavf yoki zarar keltiradigan ma'lumotlar. Bu ro‘yxatga maxfiy hisob ma’lumotlari va boshqa sirlar, shuningdek, korporativ siyosatlar va boshqa ko‘rsatmalar kiradi.

Umumiy ma'lumotlar

Umumiy ma’lumotlar korporativ veb-saytingizga kiritilgan (yoki mo‘ljallangan) har qanday ma’lumotdir. Umuman olganda, agar ommaviy ma'lumotlar oshkor qilinsa, hech qanday oqibat bo'lmaydi, chunki u allaqachon omma uchun mo'ljallangan.

Samarali va muvaffaqiyatli ma’lumotlarni tasniflash uchun quyidagi qadamlar ketma-ketligi bajarilishi kerak 5.3-rasm):



5.3-rasm. Ma’lumotlarni klassifikatsiyalash ketma-ketligi

1. Klassifikatsiyaning maqsadlarini aniqlash;
2. Maxfiy ma’lumotlarni xavf tahlilini o’tkazish;
   —kam xavf
   —o’rtacha xavf
   —yuqori xavf
3. Klassifikatsiya siyosatini ishlab chiqish;
4. Ma’lumotlar turlarini turkumlarga ajratish;

5. Ma’lumotlar joylashuvini aniqlash;
6. Ma’lumotlarni aniqlanishi va klassifikatsiyalanishi;
7. Tekshirish moslamalarini yoqish;
8. Klassifikatsiya siyosatini saqlash va kuzatib boorish;
9. Saqlash siyosatini tuzish.

Ma’lumotlarni bekor qilish va yo‘q qilish siyosati. Ma'lumotlarni bekor qilish va yo'q qilish siyosati - bu tashkilot zarur bo'lmaganda maxfiy ma'lumotlarni qanday qilib xavfsiz tarzda yo'q qilish, yo'q qilish yoki yo'q qilish kerakligini ko'rsatadigan tartib va ko'rsatmalar to'plami. Siyosat jismoniy va raqamli shakllarda saqlanadigan ma'lumotlarni, jumladan qog'oz yozuvlar, elektron fayllar va qattiq disklar, USB va mobil qurilmalar kabi saqlash qurilmalarini qamrab olishi kerak.

Ushbu siyosatning maqsadi tashkilotni ma'lumotlar buzilishi, ruxsatsiz kirish va potentsial yuridik javobgarlikdan himoya qilish uchun ma'lumotlarning to'g'ri va xavfsiz tarzda o'chirilishini ta'minlashdan iborat.

Siyosat quyidagi tarkibiy qismlarni o'z ichiga olishi kerak:

1. *Qo'llanilish doirasi:* Siyosat doirasini, jumladan, qaysi turdagi ma'lumotlar va saqlash qurilmalarini qamrab olishini aniqlang.
2. *Mas'uliyat:* Ma'lumotlarni o'chirish va yo'q qilish bilan shug'ullanadigan xodimlarning roli va mas'uliyatini aniqlang.
3. *Ma'lumotlarni o'chirish jarayoni:* Ma'lumotlarni, jumladan, foydalaniladigan dasturiy va apparat vositalarini o'chirish jarayonini belgilang.
4. *Ma'lumotlarni yo'q qilish jarayoni:* saqlash moslamalarini, shu jumladan ishlatiladigan usullar va vositalarni jismoniy yo'q qilish yoki yo'q qilish jarayonini belgilang.
5. *Tekshirish:* Ma'lumotlar muvaffaqiyatli o'chirilgan yoki yo'q qilinganligiga ishonch hosil qilish uchun tekshirish bosqichini qo'shing.
6. *Istisnolar:* Siyosat uchun har qanday istisnolarni aniqlang, masalan, qonun tomonidan ma'lum vaqt davomida saqlanishi kerak bo'lgan ma'lumotlar.
7. *Trening:* Ma'lumotlarni o'chirish va yo'q qilish bilan shug'ullanadigan xodimlarni, shu jumladan siyosatga rioya qilish muhimligini o'rgatish.
8. *Muvofiqlik:* siyosatga rioya etilishini, shu jumladan rioya qilmaslik oqibatlarini nazorat qilish tizimini yaratish.

Umuman olganda, ma’lumotlarni o‘chirish va yo‘q qilish bo‘yicha

keng qamrovli siyosat maxfiy ma’lumotlarning xavfsiz va to‘g‘ri yo‘q qilinishini ta’minlash, ma’lumotlar buzilishi xavfini va tashkilot uchun qonuniy javobgarlikni minimallashtirish uchun zarur.

Undan tashqari ma'lumotlarni yo'q qilish siyosatiga misol:

Maqsad: Ushbu siyosatning maqsadi ma'lumotlarning maxfiyligi, yaxlitligi va mavjudligini himoya qilish hamda qonuniy va tartibga soluvchi talablarga rioya qilish uchun kerak bo'lmaganda maxfiy ma'lumotlarning xavfsiz va to'g'ri yo'q qilinishini ta'minlashdan iborat.

Qo'llanish doirasi: Ushbu siyosat maxfiy ma'lumotlarni saqlash va qayta ishlashga kirish huquqiga ega bo'lgan yoki mas'ul bo'lgan barcha xodimlar, pudratchilar va uchinchi tomon sotuvchilari, shuningdek, barcha saqlash qurilmalari, shu jumladan, lekin ular bilan cheklanmagan holda, kompyuter qattiq disklari, tashqi qattiq disklar uchun amal qiladi. drayvlar, USB drayvlar, kompakt disklar, DVDlar va maxfiy ma'lumotlarni o'z ichiga olgan zahira lentalari.

Siyosat:

1. *Ma'lumotlar tasnifi:* Barcha ma'lumotlar sezgirligi va yo'qolishi yoki ta'siri bilan bog'liq xavf darajasiga qarab tasniflanishi kerak. Tasniflash tegishli himoya darajasini va yo'q qilish usulini aniqlashi kerak.

2. *Ma'lumotni saqlash:* Maxfiy ma'lumotlar faqat kerak bo'lganda saqlanishi kerak va kerak bo'lmaganda darhol yo'q qilinishi kerak.

3. *Ma'lumotlarni yo'q qilish usullari:* Ruxsatsiz kirish yoki qayta tiklashning oldini olish uchun barcha nozik ma'lumotlar tegishli usullar yordamida yo'q qilinishi kerak. Quyidagi usullardan foydalanish mumkin:

— Jismoniy yo'q qilish: saqlash qurilmalarini jismoniy yo'q qilish ma'lumotlarni yo'q qilishning eng xavfsiz usuli hisoblanadi. Bunga qattiq disklarni yoki boshqa saqlash vositalarini maydalash, gazsizlantirish yoki maydalash kiradi.

— Qayta yozish: Qayta yozish - bu saqlash qurilmasidagi mavjud ma'lumotlar ustiga yangi ma'lumotlarni yozishni o'z ichiga olgan ma'lumotlarni yo'q qilish usuli. Ushbu usul qattiq disklar, USB drayvlar va boshqa yoziladigan xotira qurilmalari uchun ishlatilishi mumkin. Tashkilot tomonidan tasdiqlangan dasturiy vosita yordamida kamida uchta qayta yozishni amalga oshirish kerak.

— Kriptografik o‘chirish: Kriptografik o‘chirish ma’lumotlarni yo‘q qilish usuli bo‘lib, u tasdiqlangan shifrlash algoritmi yordamida saqlash qurilmasidagi ma’lumotlarni shifrlashni va keyin shifrlash

kalitlarini yoʻq qilishni oʻz ichiga oladi. Ushbu usul qattiq disklar, USB drayvlar va shifrlashni qo'llab-quvvatlaydigan boshqa saqlash qurilmalari uchun ishlatilishi mumkin.

4. *Ma'lumotlarni yo'q qilish tartiblari:* Barcha xodimlar, pudratchilar va uchinchi tomon sotuvchilari maxfiy ma'lumotlar va saqlash qurilmalarini yo'q qilishda tashkilot tomonidan tasdiqlangan ma'lumotlarni yo'q qilish tartiblariga rioya qilishlari kerak. Jarayonlar nozik ma'lumotlarni aniqlash va tasniflash, tegishli yo'q qilish usulini aniqlash va yo'q qilish jarayonini hujjatlashtirish bo'yicha ko'rsatmalarni o'z ichiga olishi kerak.

5. *Tekshirish va hujjatlashtirish:* Ma'lumotlarning to'g'ri yo'q qilinganligini ta'minlash uchun barcha ma'lumotlar yo'q qilinishi tekshirilishi va hujjatlashtirilishi kerak. Hujjatlarda yo'q qilingan ma'lumotlarning turi, yo'q qilingan sana, ishlatiladigan yo'q qilish usuli va yo'q qilishni amalga oshirgan shaxsning ismi ko'rsatilishi kerak.

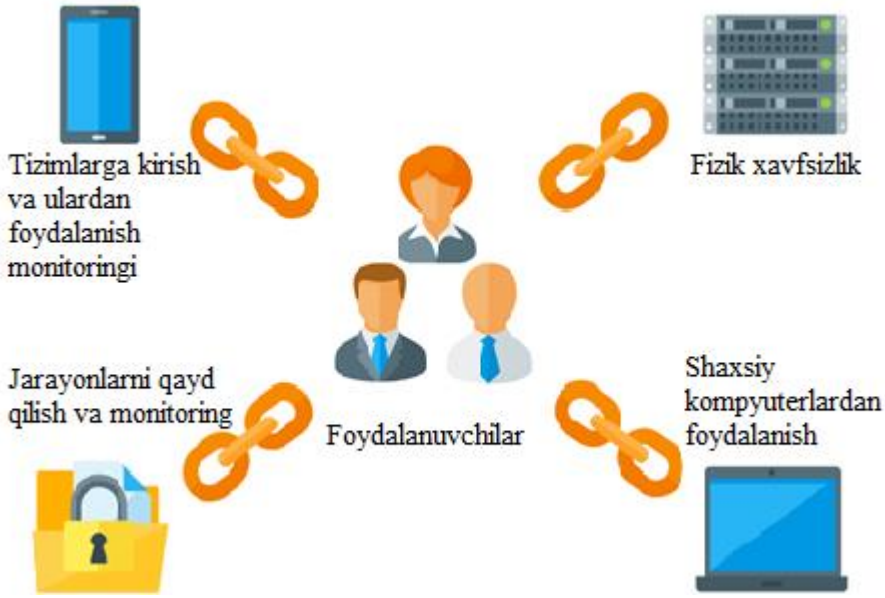
6. *Muvofiqlik:* Ushbu siyosat qonuniy va tartibga soluvchi talablarga bo'ysunadi va barcha ma'lumotlarni yo'q qilish ushbu talablarga muvofiq amalga oshirilishi kerak.

Amalga oshirish: Ushbu siyosatni buzgan har qanday xodim, pudratchi yoki uchinchi tomon sotuvchisi mehnat yoki shartnomani bekor qilishgacha bo'lgan intizomiy jazoga tortilishi mumkin.

5.3-§ Tizimlardan foydalanishdagi siyosatlar

Axborot tizimlaridan foydalanish siyosati tashkilot va uning xodimlarini zararli harakatlardan himoya qilish uchun tashkilot axborot tizimlaridan maqbul foydalanish qoidalarini belgilaydi. Ushbu siyosat axborot tizimlarining barcha foydalanuvchilariga amaldagi qonunchilikda ruxsat etilgan darajada qoʻllaniladi.

Foydalanuvchilar axborot tizimlardan quyidagi siyosatlar asosida foydalanishi kerak.



5.4-rasm. Tizimlardan foydalanishdagi siyosatlar

Jarayonlarni qayd qilish va monitoring. Xatoliklar va xavfsizlik bilan bog‘liq boshqa hodisalarni qayd qiluvchi audit jurnallari keyingi tekshiruvlar va kirish nazorati monitoringida yordam berish uchun belgilangan muddat davomida tayyorlanishi va saqlanishi kerak. Audit jurnallari quyidagilarni o‘z ichiga oladi:

(A) foydalanuvchi identifikatorlari;

(B) tizimga kirish va chiqish sanalari va vaqti, terminal identifikatori yoki joylashuvi;

(D) muvaffaqiyatli va rad etilgan tizimga kirish urinishlari yozuvlari;

(E) muvaffaqiyatli va rad etilgan ma’lumotlar va boshqa manbalarga kirish urinishlari yozuvlari.

Ba’zi audit jurnallari hujjatlarni saqlash tartib-qoidalarining bir qismi sifatida yoki dalillarni to‘plash talablari tufayli arxivga saqlanishi talab qilinadi.

Axborotni qayta ishlash vositalaridan foydalanish monitoringini o‘tkazish tartibi belgilanishi va monitoring faoliyati natijalari muntazam ravishda ko‘rib chiqilishi kerak. Bunday tartiblar foydalanuvchilarning faqat aniq ruxsat berilgan faoliyatni amalga oshirishlarini ta’minlash uchun zarur. Alohida ob’ektlar uchun zarur bo‘lgan monitoring darajasi xavfni baholash orqali aniqlanishi kerak. Ko‘rib chiqilishi kerak bo‘lgan sohalarga quyidagilar kiradi:

(A) Ruxsat berilgan kirish, shu jumladan:

(i) foydalanuvchi identifikatori;

(ii) asosiy voqealar sanasi va vaqti;

(iii) hodisalar turlari;
(iv) foydalanilgan fayllar;
(v) foydalaniladigan dastur/utilitalar.
(B) Barcha imtiyozli operatsiyalar, masalan:
(i) nazoratchi hisobidan foydalanish;
(ii) tizimni ishga tushirish va to‘xtatish;
(iii) kiritish/chiqarish qurilmasini ulash/ajratish.
(C) Ruxsatsiz kirishga urinishlar, masalan:
(i) muvaffaqiyatsiz urinishlar;
(ii) tarmoq shlyuzlari va xavfsizlik devorlari uchun kirish tartib-qoidalarining buzilishi va bildirishnomalar;
(iii) xususiy bosqinlarni aniqlash tizimlaridan ogohlantirishlar.
(D) Tizim ogohlantirishlari yoki nosozliklar, masalan:
(i) konsol ogohlantirishlari yoki xabarlari;
(ii) tizim jurnali istisnolari;
(iii) tarmoqni boshqarish signallari.

Shaxsiy kompyuterdan foydalanish. Tashkilotning kompyuterlari shu tashkilotda mehnat faoliyati bilan shug’ullanuvchi kishilar uchun taqdim etiladi. Barcha foydalanuvchilarga ish bilan bog‘liq vazifalar uchun kompyuterlardan foydalanish huquqi beriladi. Tashkilot siyosatiga, shuningdek, axborotdan foydalanish va uzatishni tartibga soluvchi qonunlarga barcha harakatlar muvofiq bo‘lishi kerak va ushbu talablarga rioya qilmaslik kirish huquqidan mahrum bo‘lishiga olib keladi va xodimlar uchun intizomiy jazoga, shu jumladan ishdan bo‘shatishga olib kelishi mumkin.

Kompyuterdan foydalanish uchun kiberxavfsizlik siyosati uning resurslaridan quyidagilar uchun foydalanishni taqiqlaydi:

(A) Birovning identifikatoridan foydalangan holda elektron pochta xabarini yuborish (Elektron pochtani qalbakilashtirish).

(B) tarmoq, uning tizimlari, periferiya qurilmalari va/yoki tashqi tarmoqlarga kirishning normal ishlashiga bila turib xalaqit beradigan har qanday harakatni amalga oshirish.

(C) Tarmoqdagi har qanday tizim yoki dasturiy ta’minotni oldindan ruxsatsiz o‘rnatish.

(D) Virus, troyan oti, qurt yoki boshqa ma’lum yoki noma’lum buzg‘unchi mexanizmni bila turib o‘rnatadigan har qanday dasturiy ta’minot tizimlari yoki apparat vositalarini o‘rnatish.

(E) IP-address ni almashtirshga urinish.

(F) mualliflik huquqi bilan himoyalangan materiallarni ruxsatsiz

yuklab olish, joylashtirish yoki tarqatishga urinish.

(G) Internetdan dasturiy ta’minotni ruxsatsiz yuklab olishga harakat qilish.

(H) Shaxsiy mulohazalar yoki bayonotlarni xato tarzda yuborish.

(I) jinsi, irqi, dini, milliy kelib chiqishi, yoshi, nogironligi asosida kamsituvchi, tuhmat qiluvchi, odobsiz, shahvoniy, haqoratli yoki bezovta qiluvchi materiallarga kirish, yaratish, uzatish (yuborish yoki qabul qilish), chop etish yoki yuklab olish , tibbiy holat, jinsiy orientatsiya yoki davlat va ichki qonunlar bilan himoyalangan va boshqalar.

Fizik xavfsizlik. Tashkilot kompyuter va telekommunikatsiya aktivlari uchun fizik xavfsizlik rejasini hujjatlashtirish, bajarish, monitoring qilish va sinovdan o‘tkazish uchun javobgardir. Ushbu fizik xavfsizlik rejasi quyidagi sabablarga ko‘ra yuzaga kelishi mumkin bo‘lgan yo‘qotishlar xavfini baholaydi:

(A) fizik boyliklarni fizik yo‘q qilish yoki o‘g‘irlash;

(B) ma’lumotlar va dastur fayllarini yo‘qotish yoki yo‘q qilish;

(C) ma’lumotlarni o‘g‘irlash;

(D) bilvosita aktivlarni o‘g‘irlash;

(E) kompyuterda ishlov berishni kechiktirish yoki to‘sqinlik qilish.

Rejaga yo‘qotish ehtimolini kamaytirish bo‘yicha chora-tadbirlar kiritiladi va quyidagilarga e’tibor qaratish kerak:

(A) ta’sirni kamaytirish uchun atrof-muhitdagi o‘zgarishlar;

(B) tahdid ta’sirini kamaytirish choralari;

(C) takomillashtirilgan nazorat tartib-qoidalari;

(D) ertaroq aniqlash;

(E) favqulodda vaziyatlar rejalari.

Tizimlarga kirish va ulardan foydalanish monitoring. Tizimlarga kirish tartib-qoidalaridan chetga chiqishni aniqlash va xavfsizlik qoidalari buzilish holatlari yuz bergan taqdirda dalillarni taqdim etish uchun tizim hodisalarini qayd etish uchun monitoring qilinishi kerak. Tizim monitoringi boshqaruv vositalarining samaradorligini tekshirish imkonini beradi.

Xatoliklar va xavfsizlik bilan bog‘liq boshqa hodisalarni qayd qiluvchi audit jurnallari kelgusidagi tekshiruvlar va kirishni nazorat qilish monitoringiga yordam berish uchun tashkilot tomonidan belgilangan muddatda hamda qonunchilik vakolatlari doirasida tayyorlanishi va saqlanishi kerak. Audit jurnallari shuningdek quyidagilarni o‘z ichiga olishi kerak:

(A) foydalanuvchi identifikatorlari;

(B) tizimga kirish va chiqish sanalari va vaqti, terminal identifikatori yoki joylashuvi;

(D) muvaffaqiyatli va rad etilgan tizimga kirish urinishlari yozuvlari;

(E) muvaffaqiyatli va rad etilgan ma’lumotlar va boshqa manbalarga kirish urinishlari yozuvlari.

Yozuvlarni saqlashning bir qismi sifatida ayrim audit jurnallarini arxivlash talab qilinishi mumkin.

Axborotni qayta ishlash vositalaridan foydalanish monitoringini o‘tkazish tartibi belgilanishi va monitoring faoliyati natijalari muntazam ravishda ko‘rib chiqilishi kerak. Bunday tartiblar foydalanuvchilar faqat aniq ruxsat berilgan faoliyatni amalga oshirishlarini ta’minlash uchun zarur. Alohida ob’ektlar uchun zarur bo‘lgan monitoring darajasi xavfni baholash orqali aniqlanishi kerak. Monitoring qilinishi kerak bo‘lgan sohalar:

(A) ruxsat berilgan kirish, shu jumladan:

(i) foydalanuvchi identifikatori;

(ii) asosiy voqealar sanasi va vaqti;

(iii) hodisalar turlari;

(iv) foydalanilgan fayllar;

(v) foydalaniladigan dastur/utilitalar.

(B) barcha imtiyozli operatsiyalar, masalan:

(i) nazoratchi hisobidan foydalanish;

(ii) tizimni ishga tushirish va to‘xtatish;

(iii) kiritish/chiqarish qurilmasini ulash/ajratish.

(C) ruxsatsiz kirishga urinishlar, masalan:

(i) muvaffaqiyatsiz urinishlar;

(ii) tarmoq shlyuzlari va xavfsizlik devorlari uchun kirish tartib-qoidalarining buzilishi va bildirishnomalar;

(iii) xususiy bosqinlarni aniqlash tizimlaridan ogohlantirishlar.

(D) tizim ogohlantirishlari yoki nosozliklar, masalan:

(i) konsol ogohlantirishlari yoki xabarlari;

(ii) tizim jurnali istisnolari;

(iii) tarmoqni boshqarish signallari.

Monitoring faoliyati natijalari muntazam ravishda ko‘rib chiqilishi kerak. Tekshiruvning chastotasi xavfga bog‘liq bo‘lishi kerak. Ko‘rib chiqilishi kerak bo‘lgan xavf omillari quyidagilardan iborat:

(A) dastur jarayonlarining muhimligi;

(B) tegishli ma’lumotlarning qiymati, sezgirligi yoki tanqidiyligi;

(C) tizimga kirish va noto‘g‘ri foydalanishning o‘tmishdagi tajribasi;

(D) tizimning o‘zaro bog‘lanish darajasi.

Jurnalni ko‘rib chiqish tizim duch keladigan tahdidlarni va ularning paydo bo‘lish holatlarini tushunishni o‘z ichiga oladi. Tizim jurnallari ko‘pincha katta hajmdagi ma’lumotlarni o‘z ichiga oladi, ularning aksariyati xavfsizlik monitoringi uchun begonadir. Xavfsizlik monitoringi maqsadlarida muhim voqealarni aniqlashga yordam berish uchun tegishli xabar turlarini avtomatik ravishda ikkinchi jurnalga nusxalash va yoki fayllarni tahlil qilish uchun mos tizim yordamchi dasturlari yoki audit vositalaridan foydalanishni hisobga olish kerak. Jurnalni ko‘rib chiqish uchun javobgar shaxs(lar) va faoliyatni nazorat qilinadigan shaxslar o‘rtasida rollarga ajratishni hisobga olinishi kerak.

Hodisalar daraxti xavfsizligiga alohida e’tibor berilishi kerak, chunki agar u o‘zgartirilsa, noto‘g‘ri xavfsizlik tizimi paydo bo‘lishi mumkin. Tekshirish vositalari ruxsatsiz o‘zgarishlar va operatsion muammolardan himoya qilishga qaratilgan bo‘lishi kerak, jumladan:

(A) ro‘yxatga olish moslamasi o‘chirilgan;

(B) yozib olingan xabar turlariga o‘zgartirishlar kiritish;

(C) tahrirlangan yoki o‘chirilayotgan jurnal fayllari va jurnal fayli tashuvchisi tugatilgan bo’lishi;

(D) jurnal fayli hodisalarni o‘zi qayta yozadigan bo‘lishi.

Operatsion dasturiy ta’minotni nazorat qilish. Operatsion tizimlarda dasturiy ta’minotni amalga oshirishda nazorat qo‘llanilishi kerak. Operatsion tizimlarda dasturiy xavflarni minimallashtirish uchun quyidagi nazorat choralarini ko‘rib chiqish kerak bo‘ladi:

(A) Operatsion dastur kutubxonalarini yangilash faqat tegishli rahbariyat ruxsati bilan tayinlangan manbalar tomonidan amalga oshirilishi kerak.

(B) Operatsion tizimlar faqat bajariladigan kodni saqlashi kerak.

(C) Muvaffaqiyatli sinovdan o‘tkazilganligi va foydalanuvchi tomonidan qabul qilinganligi to‘g‘risida dalillar olinmaguncha va tegishli dastur manbalari kutubxonalari yangilanmaguncha, bajariladigan kod operatsion tizimda amalga oshirilmasligi kerak.

(D) Operatsion dastur kutubxonalaridagi barcha yangilanishlarni tekshirish jurnali yuritilishi kerak.

(E) Dasturiy ta’minotning oldingi versiyalari favqulodda choralar sifatida saqlanishi kerak.

Operatsion tizimlarda foydalaniladigan dasturiy ta’minot yangi

versiyaga yangilash bo‘yicha har qanday qaror chiqarish xavfsizligini, ya’ni yangi xavfsizlik funksiyalarining joriy etilishini yoki ushbu versiyaga ta’sir qiluvchi xavfsizlik muammolarining soni va muximligini hisobga olishi kerak. Xavfsizlik kamchiliklarini bartaraf etish yoki kamaytirishga yordam beradigan dasturiy ta’minotlar qo‘llanilishi kerak.

Nazorat savollari.

1. Tarmoq kriminalistikasi nima va u qanday vazifalarni hal qiladi? Tarmoq dalillari va ularni tahlil qilish usullariga misollar keltiring.
2. Zararli dasturlarning asosiy turlarini bilasizmi? Zararli dasturlarni tahlil qilish uchun qanday vositalar va usullar qo'llaniladi?
3. Ijtimoiy muhandislik nima va u kiberjinoyatchilar tomonidan qanday qo'llaniladi? Ijtimoiy muhandislikdan himoya qilishning qanday usullarini taklif qila olasiz? Muvaffaqiyatli yoki muvaffaqiyatsiz ijtimoiy muhandislik hujumlariga misollar keltiring.
4. Kriptografiya nima va uning kiberjinoyat bilan qanday aloqasi bor? Shifrlashning qanday turlarini bilasiz?
5. Raqamli dalillar ashyoviy dalillarga nisbatan qanday xususiyatlarga ega?
6. Raqamli dalillarni olishda qanday qonuniy talablarga rioya qilish kerak?
7. Xalqaro kiberxavfsizlik hamkorlari bilan ishlashda qanday qiyinchiliklar yuzaga keladi?
8. Mamlakatingizda kiberxavfsizlikni qanday qonunlar va qoidalar tartibga soladi?
9. Siyosatga muvofiq ma'lumotlarni o'chirish va yo'q qilish uchun kim javobgar?
10. Saqlash qurilmalaridan ma'lumotlarni o'chirish uchun qanday dasturiy va texnik vositalardan foydalaniladi?
11. Saqlash moslamalarini yo'q qilish uchun qanday usullar va vositalar qo'llaniladi?
13. Ma'lumotlarni o'chirish yoki yo'q qilish muvaffaqiyati qanday tekshiriladi?
14. Qonun bilan saqlanishi kerak bo'lgan ma'lumotlarga nisbatan qanday siyosat istisnolari mavjud?
15. Ma'lumotlarni o'chirish va yo'q qilish bo'yicha xodimlar qanday tayyorlanadi?
16. Siyosatga rioya qilish qanday amalga oshiriladi va buzilish oqibatlari qanday?

VI BOB. XAVFSIZLIK BO‘YICHA MA’LUMOTLAR

6.1-§. Xavfsizlik texnologiyasi resurslari

Kiberxavfsizlik ham IT bo‘limlari, ham rahbarlar uchun muhim masaladir. Xavfsizlik nafaqat IT-mutaxassislari va menejerlarni, balki tashkilotdagi har bir xodimni tashvishga solishi kerak. Xodimlarni xavfsizlikning ahamiyati haqida o‘rgatishning samarali usullaridan biri bu har bir shaxsning AT tizimlari va ma’lumotlarini himoya qilish bo‘yicha mas’uliyatini tushuntiruvchi kiberxavfsizlik siyosatidir. Kiberxavfsizlik siyosati elektron pochta, ma’lumotlarni shifrlash va ijtimoiy mediadan foydalanishni cheklash kabilar uchun xatti-harakatlar standartlarini belgilaydi. Odatda, kiberxavfsizlik siyosatining birinchi qismida tashkilotdagi umumiy xavfsizlik kutilmalari, rollari va mas'uliyatlari tavsiflanadi. Katta tashkilotlar yoki tartibga solinadigan tarmoqlar uchun kiberxavfsizlik siyosati ko‘pincha o‘nlab sahifalarni tashkil qiladi. Kichik tashkilotlar uchun esa xavfsizlik siyosati bir necha sahifadan iborat bo‘lishi va asosiy xavfsizlik amaliyotlarini qamrab olishi mumkin. Bunday amaliyotlar quyidagilarni o‘z ichiga olishi mumkin:

1. Elektron pochtani shifrlashdan foydalanish qoidalari.
2. Ish ilovalariga masofadan kirish uchun qadamlar.
3. Parollarni yaratish va himoya qilish bo‘yicha ko‘rsatmalar.
4. Ijtimoiy tarmoqlardan foydalanish qoidalari.

Anti-malware siyosati. Maqsadga erishish va faoliyat uzluksizligini ta'minlash uchun aniq belgilangan va sinovdan o‘tgan rejalar va tartiblar qabul qilinadi va ularga rioya qilinadi. Bu axborot texnologiyalari aktivlarini zararli dasturlardan va virus hujumlaridan himoya qilishni ta'minlaydi. Axborot texnologiyalari aktivlari virus va zararli dasturlar hujumlariga chidamliligi ta'minlangan holda himoyalanadi. Bunday hujumlarga qarshi turish uchun barcha profilaktika va himoya choralari anti-malware siyosatida belgilanadi va u quyidagilarni o‘z ichiga oladi.

Ushbu siyosatning maqsadi virus va zararli dasturlarga qarshi vositalardan foydalanishni rag'batlantirishdir. Maqsad foydalanuvchilarni zararli dasturlarga qarshi vositalardan samarali foydalanish uchun keng qo‘llaniladigan siyosatlar bo‘yicha o‘rgatishdir. Ushbu siyosat qonun hujjatlariga rioya etilishini ta'minlash uchun yo‘nalish beradi.

Zararli dasturiy ta'minot/virus muammolarini oldini olish uchun quyidagi muayyan amaliyotlar qo‘llaniladi:

1. Tarmoqqa ulangan yoki mustaqil bo‘lgan barcha ish stantsiyalari

tasdiqlangan virusga qarshi va zararli dasturlarga qarshi dastur va konfiguratsiyadan foydalanishi kerak.

2. Virusga qarshi va zararli dasturlarga qarshi dasturlarni o‘chirib qo‘ymaslik yoki chetlab o‘tmaslik kerak.

3. Virusga qarshi va zararli dasturlarga qarshi dasturiy ta'minot sozlamalari dasturiy ta'minot samaradorligini pasaytiradigan tarzda o‘zgartirilmasligi kerak.

4. Antivirus va zararli dasturlarga qarshi dasturlarning avtomatik yangilanish chastotasi yangilanishlar chastotasini kamaytirish uchun o‘zgartirilmasligi kerak.

5. Tarmoqqa ulangan har bir fayl serveri tasdiqlangan virusga qarshi va zararli dasturlarga qarshi dasturlardan foydalanishi hamda fayl almashuvlarini yuqtirishi mumkin bo‘lgan zararli dasturlarni aniqlash va tozalashni sozlashi kerak.

6. Antivirus va zararli dasturlarga qarshi dastur tomonidan avtomatik tozalanmagan har bir virus/zararli dastur xavfsizlik hodisasini tashkil etishi kerak.

7. Tashkilot zararli kod va ruxsat etilmagan mobil kodning kiritilishining oldini olish va aniqlash uchun tegishli boshqaruv vositalarini qabul qiladi.

8. Axborot tizimi zararli kodlardan himoya mexanizmlarini avtomatik ravishda yangilaydi. Masalan, virusga qarshi va zararli dasturlarga qarshi dasturlarning avtomatik yangilanishi.

9. Har bir elektron pochta shlyuzi tasdiqlangan elektron pochta antivirus dasturidan foydalanadi va ushbu dasturiy ta'minotni sozlash va ishlatish bo‘yicha sanoatning eng yaxshi amaliyotlariga amal qiladi.

10. Zararli kod yoki dasturiy ta'minot ta'sir qilmaydi deb o‘ylangan tizimlar uchun davriy baholashlar amalga oshirilishi kerak. Bu tizimlar antivirus dasturlarini talab qilmasligini tasdiqlash uchun rivojlanayotgan zararli dasturlar tahdidlarini tushunish va baholashdir.

Ushbu siyosatni buzganligi aniqlangan har qanday xodim HR siyosatiga muvofiq intizomiy jazoga tortilishi mumkin.

Elektron pochta va xabarlar. Kompaniyaning elektron pochtada ma’lumot almashinishi har doim ochiq bo‘lgan. Ikki elektron pochta serveri o‘rtasidagi ma’lumot almashinuvi 6.1-rasmda ko‘rsatilgan. Ikki elektron pochta serveri o‘rtasidagi aloqa misolida aniq matn mazmuni mavjud va autentifikatsiya talab qilinmaydi. Protokol ma'lumotni buyruq satriga kiritish imkonini beradi, shuning uchun ushbu protokol yordamida elektron pochta serverini qalbakilashtirish uchun elektron pochta serveri

dasturiga ega bo‘lish ham shart emas. Ba'zi serverlar autentifikatsiya qilish uchun kalitni taqdim etishni talab qilishi yoki oldindan belgilangan IP-manzilga ulanishni cheklashi mumkin bo‘lsa-da, agar jo‘natuvchi va qabul qiluvchi o‘rtasidagi elektron pochta releyidagi har qanday server shaklda ko‘rsatilganidek, faqat matnga asoslangan buyruqlar qatorini qo‘llab-quvvatlasa, Internetdagi har qanday shaxs firibgarlikka qodir bo‘ladi.

```
$ telnet mail.company.com 25
Trying 192.168.142.13
Connected to mail.company.com.
Escape character is '^]'.
220 mail
SMTP/smap Ready.
helo
250 Charmed, I'm sure.
mail from:spoofvictim@anothercompany.com
250 <spoofvictim@anothercompany.com>...
Sender Ok
rcpt to: unsuspecting@company.com
250 unsuspecting@company.com
OK
Data
354 Enter mail, end with "." on a line by itself
malicious message text goes here.
250 Mail
Accepted
quit
221 Closing connection
Connection closed by foreign host.
$
```

6.1-rasm. Email server aloqa protokoli namunasi

Reklama beruvchilar elektron pochta serveri aloqalarining ochiqligidan foydalanidilar, chunki ular ushbu ochiq protokollar yordamida mijozlarni aniqlashlari mumkin. Misol uchun, agar kompaniya elektron pochta serveri 1-rasmdagi kabi buyruqlarga javob bersa, reklama beruvchining avtomatlashtirilgan dasturi elektron pochta xabarlarini jo‘natish va oxir-oqibat barcha foydalanuvchilarga uni yuborishga harakat qilishi mumkin. Xatolar yuzaga kelganda, ular shunchaki urinishni to‘xtatadilar va nom bo‘yicha keyingi taxminga o‘tadilar. Agar reklama beruvchilar potentsial xaridorlarning qaysi biri o‘z mahsulotiga qiziqish bildirishini ajratmasdan, katta miqdordagi potentsial mijozlarga elektron pochta xabarlarini yuborsa, bu “spam” deb ataladi. Internet paydo bo‘lishining dastlabki kunlarida foydalanuvchilar o‘zlari ko‘rmoqchi bo‘lmagan kontentni tasvirlash uchun “spam” so‘zidan foydalanishgan. Spam atamasi endi odatda har qanday kiruvchi elektron pochta tarkibiga ishora qiladi. Elektron pochtaga kirish fishing deb ataladi, va bu internet foydalanuvchilarini zararli veb-saytlarga olib boradigan havolalarni bosish uchun o‘lja qilish yoki jalb qilishni

anglatadi. Zararli saytlar foydalanuvchi nomlari va parollarini to‘playdigan saytlar bo‘lishi mumkin. Ular zararli dasturlarni yuklab olishlari, foydalanuvchilarning bank hisoblaridan pul o‘tkazishda aldash uchun firibgarlik qilishi mumkin. Xabar almashish texnologiyalari jo‘natuvchi va qabul qiluvchi o‘rtasidagi protokollarga tayanadi, ular kamdan-kam hollarda autentifikatsiya qilinadi, lekin shunchaki xabar oqimining bir qismi sifatida taqdim etilgan “foydalanuvchi nomi” qatori orqali jo‘natuvchini identifikatsiya qiladi. Elektron pochta va xabar almashish uchun ro‘yxatlangan kiberxavfsizlik siyosatlari elektron pochta xabarlarining umumiy talablaridan boshlanadi. Siyosatda spam va umuman javobgarlik bilan bog'liq ko‘proq tizimli muammolar etiborga olinishi kerak. (6.1-jadval).

6.1-jadval

Elektron pochta va xabar almashishga oid kiberxavfsizlik siyosati masalalari

Siyosat	Bayonot	Qarama-qarshilik sabablari
Elektron tijoratda ishtirok etuvchi barcha sub'ektlar mijozlarga standart protokollar orqali elektron pochta serverlarini tekshirish imkoniyatini taklif qilishlari kerak.	Ushbu siyosat e-tijorat kompaniyalaridan o‘zlarining elektron pochta serverlari uchun kalitlarni DNS-da chop etishlarini talab qiladi.	Iste'molchilar xizmat ko‘rsatuvchi provayderlar va boshqalardan kelgan xabarlar soxtalashtirilmaganligini tekshirish huquqiga ega. Iste'molchilar odatda elektron pochta serverini tekshirish dasturiga ega emaslar va shuning uchun elektron pochtaning haqiqiyligini tekshirish uchun o‘zlarining xosting xizmati provayderlariga tayanishi kerak bo‘ladi.
Tashkilot nomidan yoki unga tegishli barcha elektron pochta xabarlari tashkilot tomonidan qo‘llab-quvvatlanadigan	Shaxslar tashkilotning biznesini yuritishda o‘z tashkilotining elektron pochta tizimlaridan foydalanishi va	Ushbu siyosat barcha aloqalarni boshqaruv monitoringi doirasini saqlaydi. Bu ichki xodimlar ma'murlariga ma'muriy kirish huquqiga ega bo‘lgan odamlar

elektron pochta xizmatlaridan foydalanishi kerak.	ijtimoiy tarmoq saytlari, shaxsiy uyali telefonlar va boshqa davlat yoki xususiy aloqa xizmatlaridan voz kechish talabidir.	sonini minimallashtiradi. Bu siyosat uzilishlar tufayli korporativ xizmatlarga ulana olmaydigan shaxslarning muloqot qilish qobiliyatini cheklaydi.
Elektron pochta orqali jo‘natilgan va o‘qilganligi to‘g'risidagi kvitansiya elektron ma'lumotlarning yetkazilganligini tasdiqlovchi hujjat bo‘lishi kerak	Turli shartnoma va tartibga soluvchi bandlar bildirishnomalarni taqdim etuvchi tashkilotlardan xabarnoma yuborilgan shaxs uni haqiqatda olganligini isbotlashni talab qiladi.	Yetkazib berishning isboti sifatida elektron yetkazib berish va o‘qish kvitansiyasidan foydalanish imkoniyati bank va sug‘urtadan tortib huquqni muhofaza qilish organlarigacha bo‘lgan turli sohalarda jismoniy shaxslarni xabardor qilish uchun qonuniy javobgar bo‘lgan tashkilotlar uchun xarajatlarni kamaytiradi. Raqamli yozuvlarni autentifikatsiya qilishning joriy standartlari kalitlarni boshqarish, kriptografik algoritmlar va tashkiliy nazorat tartib-qoidalarini isbotlashning kombinatsiyasini talab qiladi.
Jismoniy shaxslar o‘zlarining elektron pochta manzillarini ro‘yxatga qo‘yish imkoniyatiga ega bo‘lishi kerak, bu esa sotuvchilarning	Bu elektron pochta so‘rovi uchun milliy “qo‘ng'iroq qilmang” reestrining ekvivalentidir. Ushbu turdagi	Elektron pochta manzillarini istalmagan so‘rovlardan himoya qilish uchun “elektron pochta orqali yubormang” siyosatini qo‘llash mexanizmi sezilarli

ularga keraksiz elektron pochta xabarlarini yuborishini noqonuniy qiladi.	ro‘yxat hozirda telefon raqamlari uchun ishlatiladi.	darajada kamaytiradi. Hozirda elektron pochta orqali olingan kiruvchi reklamalar soni. Bu siyosat noqonuniy spamni aniqlashni osonlashtirishi kerak. Siyosatning bajarilishi keraksiz xabarlar sonini kamaytirish orqali ham tarmoqli kengligi, ham saqlash resurslarini tejaydi..
Xabar almashish xizmatlaridan foydalanuvchi shaxslar faqat ro‘yxatdan o‘tgan Internet domen nomlaridan foydalanishlari shart.	Bu har bir potentsial elektron pochta qabul qiluvchisi uchun individual “oq ro‘yxat” ning ekvivalenti. faqat ro‘yxatdagilar qabul qiluvchiga e-pochta yoki xabar jo‘natishlari mumkin bo‘ladi.	Ushbu siyosat Internet foydalanuvchilariga o‘z resurslarini boshqarish va keraksiz xabarlar sonini kamaytirish imkonini beradi. Bu o‘tkazish qobiliyatini ham, saqlash resurslarini ham tejaydi. Elektron pochta yoki xabar almashish uchun autentifikatsiya qilishning umumiy qabul qilingan usuli yo‘qligi sababli, har kim oq ro‘yxatdagi istalgan foydalanuvchi nomini ko‘rsatish orqali bu siyosatni chetlab o‘tishi mumkin.
Ma'lum bo‘lgan fishing elektron pochta jo‘natuvchilari jinoiy javobgarlikka tortiladi va jazolar fishing oluvchilardan	Ushbu siyosat fishing elektron pochta xabarlarini yuborganlarga ma’lumot o‘g'irlash jazosini qo‘yadi	Fishing elektron pochta jo‘natuvchilari uyushgan jinoyatchilikning katta jamoasining kichik bir qismidir. Bu shaxsga qasddan qilingan kattaroq hujumning zaruriy shartidir va hujumning

potentsial ma'lumotlarni o‘g'irlash natijasida yuzaga kelgan jinoyatlarga mos kelishi kerak.		o‘zi kabi jiddiy qabul qilinishi kerak. Fishing elektron pochta jo‘natuvchisi, ehtimol, turli mijozlar uchun ommaviy elektron pochta xabarlarini yuboruvchi biznesdir. Bundan tashqari, oddiygina elektron pochta xabarini yuborish foydalanuvchining o‘ziga jalb qilinishiga kafolat bermaydi.

Shifrlash. Muhim ma'lumotlarning maxfiyligini himoya qilish uchun shifrlash qo‘llanilishi kerak. Xavfni baholash asosida foydalaniladigan shifrlash algoritmining turini hamda foydalaniladigan kriptografik kalitlarning uzunligini hisobga olgan holda zarur himoya darajasi aniqlanadi.

Tegishli himoya darajasini aniqlash, kerakli himoyani ta'minlaydigan mos mahsulotlarni tanlash va kalitlarni boshqarishning xavfsiz tizimini joriy qilish uchun mutaxassis maslahatiga murojaat qilish kerak. Bundan tashqari, tashkilot shifrlashdan maqsadli foydalanishiga taalluqli bo‘lishi mumkin bo‘lgan qonunlar va qoidalar bo‘yicha yuridik maslahat so‘rash kerak bo‘ladi.

Axborotni himoya qilishning kriptografik boshqaruv vositalaridan foydalanish tartiblari ishlab chiqilishi va ularga rioya etilishi kerak. Bunday tartib-qoidalar kriptografik usullardan maksimal foyda olish va xavflarni minimallashtirish hamda noto‘g'ri foydalanishdan qochish uchun zarurdir.

Jarayonlarni ishlab chiqishda quyidagilar e'tiborga olinishi kerak:

(A) tashkilot bo‘ylab kriptografik boshqaruv vositalaridan foydalanish bo‘yicha boshqaruv ko‘rsatmalari;

(B) biznes ma'lumotlari himoya qilinishi kerak bo‘lgan umumiy tamoyillarni o‘z ichiga oladi;

(C) kalitlarni boshqarishga yondashuv, shu jumladan kalitlar yo‘qolgan, buzilgan yoki buzilgan taqdirda shifrlangan ma'lumotlarni qayta tiklash usullari;

(D) rollar va mas'uliyatlar, masalan, kim javobgar: protseduralarni amalga oshirish; asosiy boshqaruv;

(E) kriptografik himoyaning tegishli darajasini qanday aniqlash kerakligi;

(F) butun tashkilotda samarali joriy etish uchun qabul qilinishi kerak bo‘lgan standartlar (qaysi yechim qaysi biznes jarayonlari uchun ishlatiladi).

Internet va intranet xavfsizligi. Internetni ikkita asosiy komponentga bo‘lish mumkin: Internet orqali ma'lumotni taqdim etadigan ilovalar va kirish uchun ishlatiladigan veb-brauzerlar (mijozlar) bo‘lgan veb-serverlar. Veb-server ko‘pgina tashkilotlar tarmog'ida eng ko‘p maqsadli va hujumga uchragan xost hisoblanadi. Shuning uchun veb-serverlar va ularni qo‘llab-quvvatlaydigan tarmoq infratuzilmasini himoya qilish juda muhimdir.

Veb-serverlar uchun maxsus xavfsizlik tahdidlari odatda quyidagi toifalardan biriga kiradi:

(A) Buzg’unchi shaxslar veb-serverga ruxsatsiz kirish uchun veb-server, asosiy operatsion tizim yoki faol tarkibdagi dasturiy xatolardan foydalanishi mumkin. Ruxsatsiz kirishga misollar ommaviy foydalanish uchun mo‘ljallanmagan fayl yoki papkalarga kirish yoki imtiyozli buyruqlarni bajarish va veb-serverga dasturiy ta'minotni o‘rnatishdir.

(B) Xizmat ko‘rsatishni rad etish hujumlari veb-serverga yo‘naltiriladi, bu esa haqiqiy foydalanuvchilarga hujum davomida veb-serverdan foydalanish imkoniyatini rad etadi.

(C) Veb-serverdagi maxfiy ma'lumotlar ruxsatsiz shaxslarga tarqatilishi mumkin.

(D) Veb-server va brauzer o‘rtasida uzatilganda shifrlanmagan maxfiy ma'lumotlar ushlanishi mumkin.

(E) Veb-serverdagi ma'lumotlar o‘zgartirilishi mumkin. Veb-saytni buzish bu tahdidning keng tarqalgan misolidir.

(F) Buzg’unchi shaxslar veb-serverga muvaffaqiyatli hujum qilish orqali tashkilotning boshqa kompyuter tarmog'idagi resurslarga ruxsatsiz kirishlari mumkin.

(G) Buzg’unchi shaxslar buzilgan veb-serverdan tashqi tashkilotlarga hujum qilishi, ularning haqiqiy identifikatorlarini yashirishi va hujum boshlangan tashkilotni zarar uchun javobgarlikka tortishi mumkin.

(H) Server noqonuniy nusxalarini dasturiy ta'minotga hujum qilish vositalari yoki pornografiya uchun tarqatish nuqtasi sifatida ishlatilishi

mumkin, bu esa tashkilotni zarar uchun javobgar qilishi mumkin.

Quyidagi umumiy funktsiyalarni bajarish uchun xavfsizlik devori muhitidan foydalanish kerak:

(A) paketlar va protokollarni filtrlash;

(B) ulanishlarni tekshirish;

(C) proksi-serverlar yoki tanlangan ilovalarni bajarish;

(D) xavfsizlik devori tomonidan ruxsat etilgan yoki rad etilgan trafikni kuzatish.

Tarmoq. Tarmoq xizmatlariga xavfsiz ulanishlar butun tashkilotga ta'sir qilishi mumkin. Foydalanuvchilar faqat foydalanish uchun maxsus ruxsat berilgan xizmatlardan to‘g'ridan-to‘g'ri foydalanishlari kerak. Bu nazorat, ayniqsa, muhim biznes ilovalari yoki tashkilotning xavfsizlik boshqaruvi va nazorati doirasidan tashqarida bo‘lgan jamoat yoki tashqi hududlardagi xavfli joylarda foydalanuvchilarga tarmoq ulanishlari uchun juda muhimdir.

Tarmoqlar va tarmoq xizmatlaridan foydalanishga oid tartib-qoidalar quyidagilarni qamrab olishi kerak:

(A) kirishga ruxsat berilgan tarmoqlar va tarmoq xizmatlari;

(B) kimning qaysi tarmoqlarga va tarmoq xizmatlariga kirishiga ruxsat berilganligini aniqlash uchun avtorizatsiya tartiblari;

(C) tarmoq ulanishlari va tarmoq xizmatlariga kirishni himoya qilish uchun boshqaruv nazorati va protseduralari.

Foydalanuvchi terminalidan kompyuter xizmatiga boradigan yo‘l nazorat qilinishi kerak. Tarmoqlar resurslarni almashish uchun maksimal imkoniyatlarni va marshrutlashning moslashuvchanligini ta'minlash uchun mo‘ljallangan. Bu xususiyatlar biznes ilovalariga ruxsatsiz kirish yoki axborot vositalaridan ruxsatsiz foydalanish imkoniyatlarini ham taqdim etishi mumkin. Foydalanuvchi terminali va uning foydalanuvchisi kirish huquqiga ega bo‘lgan kompyuter xizmatlari o‘rtasidagi marshrutni cheklovchi boshqaruv elementlarini kiritish, masalan, majburiy yo‘lni yaratish bunday xavflarni kamaytirishi mumkin.

Marshrutni cheklash uchun quyidagi usullarni qo‘llash kerak:

(A) ajratilgan liniyalar yoki telefon raqamlarini ajratish;

(B) portlarni belgilangan dastur tizimlari yoki xavfsizlik shlyuzlariga avtomatik ravishda ulash;

(C) individual foydalanuvchilar uchun menyu va pastki menyu imkoniyatlarini cheklash;

(D) cheksiz tarmoq roumingining oldini olish;

(E) tashqi tarmoq foydalanuvchilari uchun belgilangan dastur

tizimlari va xavfsizlik shlyuzlaridan foydalanishni ta'minlash;

(F) xavfsizlik shlyuzlari, masalan xavfsizlik devori;

(G) tashkilot ichidagi foydalanuvchilar guruhlari uchun alohida mantiqiy domenlarni, masalan, virtual xususiy tarmoqlarni o‘rnatish orqali tarmoqqa kirishni cheklash.

Tashqi ulanishlar biznes ma'lumotlariga ruxsatsiz kirish imkoniyatini ta'minlaydi, masalan, dial-up usullari bilan kirish. Shuning uchun, masofaviy foydalanuvchilar tomonidan kirish autentifikatsiya qilinishi kerak. Autentifikatsiya usullarining har xil turlari mavjud, ulardan ba'zilari boshqalarga qaraganda yuqoriroq himoya darajasini ta'minlaydi, masalan, kriptografik usullardan foydalanishga asoslangan usullar kuchli autentifikatsiyani ta'minlaydi.

(A) Masofaviy foydalanuvchilarning autentifikatsiyasiga quyidagi usullardan biri yordamida erishish kerak:

(B) kriptografiyaga asoslangan texnika;

(C) apparat tokenlari;

(D) e'tiroz/javob protokoli;

(E) ajratilgan shaxsiy liniyalar yoki tarmoq foydalanuvchisi manzilini tekshirish.

Axborotni qayta ishlash va tarmoq vositalarini o‘zaro bog'lash yoki almashishni talab qilishi mumkin bo‘lgan biznes sherikliklari shakllanar ekan, tarmoqlar an'anaviy tashkiliy chegaralardan tobora kengayib bormoqda. Bunday kengaytmalar tarmoqdan foydalanadigan mavjud axborot tizimlariga ruxsatsiz kirish xavfini oshiradi, ularning ba'zilari sezgirligi yoki muhimligi sababli boshqa tarmoq foydalanuvchilaridan himoyani talab qilishi mumkin. Bunday sharoitda tarmoqlarda axborot xizmatlari guruhlari, foydalanuvchilar va axborot tizimlarini ajratish uchun boshqaruv elementlari joriy etilishi kerak.

Katta tarmoqlarning xavfsizligi ularni alohida mantiqiy tarmoq domenlariga bo‘lish yo‘li bilan nazorat qilinishi kerak, masalan, tashkilotning ichki tarmoq domenlari va tashqi tarmoq domenlari, ularning har biri belgilangan xavfsizlik perimetri bilan himoyalangan. Bunday perimetr ikki domen o‘rtasida kirish va axborot oqimini boshqarish uchun o‘zaro bog'lanishi kerak bo‘lgan ikkita tarmoq o‘rtasida xavfsiz shlyuzni o‘rnatish orqali amalga oshirilishi kerak. Ushbu shlyuz ushbu domenlar orasidagi trafikni filtrlash va tashkilotning kirishni boshqarish tartib-qoidalariga muvofiq ruxsatsiz kirishni bloklash uchun sozlanishi kerak. Ushbu turdagi shlyuzlarga misol sifatida odatda xavfsizlik devori deb ataladi. Tarmoqlarni domenlarga ajratish mezonlari

kirishni boshqarish tartib-qoidalari va kirish talablariga asoslanishi kerak, shuningdek, tegishli tarmoq marshrutizatsiyasi yoki shlyuz texnologiyasini kiritishning nisbiy narxi va unumdorligiga ta'sirini hisobga olishi kerak.

Umumiy tarmoqlarda foydalanuvchilarning ulanish imkoniyatlari kirishni boshqarish tartib-qoidalariga muvofiq cheklanishi kerak.

Bunday boshqaruvlar oldindan belgilangan jadvallar yoki qoidalar orqali trafikni filtrlaydigan tarmoq shlyuzlari orqali amalga oshirilishi kerak. Qo‘llaniladigan cheklovlar kirish tartib-qoidalari va biznes-ilovalarning talablariga asoslanishi kerak va shunga mos ravishda saqlanishi va yangilanishi kerak. Cheklovlar qo‘llanilishi kerak bo‘lgan ilovalarga misollar:

A) elektron pochta;

(B) bir tomonlama fayllarni uzatish;

(C) fayllarni ikki tomonlama uzatish;

(D) interaktiv kirish;

(E) kun yoki sana vaqti bilan bog'langan tarmoqqa kirish.

Umumiy tarmoqlarda kompyuter ulanishlari va axborot oqimlari biznes-ilovalarning kirishni boshqarish tartib-qoidalarini buzmasligini ta'minlash uchun marshrutlashni boshqarish vositalari bo‘lishi kerak. Ushbu nazorat uchinchi tomon (tashkilot bo‘lmagan) foydalanuvchilar bilan birgalikda ishlatiladigan tarmoqlar uchun zarurdir.

Mobil hisoblash. Mobil hisoblash vositalari, xususan, himoyalanmagan muhitda ishlash xavfidan himoya qilish uchun rasmiy tartib-qoidalar mavjud bo‘lishi va tegishli boshqaruv vositalari qabul qilinishi kerak. Masalan, bunday tartiblar quyidagi talablarni o‘z ichiga olishi kerak:

(A) jismoniy himoya;

(B) kirishni boshqarish vositalari;

(C) kriptografik usullar;

(D) zaxira nusxalari;

(E) viruslardan himoyalanish.

Protseduralar, shuningdek, mobil qurilmalarni tarmoqlarga ulash bo‘yicha qoidalar va tavsiyalarni va ushbu ob'ektlardan jamoat joylarida foydalanish bo‘yicha ko‘rsatmalarni o‘z ichiga olishi kerak.

Ko‘chma hisoblash vositalaridan jamoat joylarida, yig'ilish xonalarida va tashkilot hududidan tashqaridagi boshqa himoyalanmagan joylarda foydalanishda ehtiyot bo‘lish kerak. Ushbu qurilmalar tomonidan saqlanadigan va qayta ishlanadigan ma'lumotlarga ruxsatsiz

kirish yoki oshkor etilishining oldini olish uchun himoya qilish kerak, masalan, kriptografik usullardan foydalangan holda.

Mobil hisoblash vositalaridan foydalangan holda jamoat tarmog'i bo‘ylab biznes ma'lumotlariga masofaviy kirish faqat muvaffaqiyatli identifikatsiya va autentifikatsiyadan so‘ng va tegishli kirishni boshqarish mexanizmlari mavjud bo‘lganda amalga oshirilishi kerak.

Mobil hisoblash vositalari, ayniqsa, avtomobillar va boshqa transport turlarida, mehmonxona xonalarida, konferentsiya markazlarida va yig'ilish joylarida qoldirilganda, shuningdek, o‘g'irlikdan jismonan himoyalangan bo‘lishi kerak. Muhim ma'lumotlarini tashuvchi jihozlar qarovsiz qoldirilmasligi va iloji bo‘lsa, uskunani himoya qilish uchun maxsus qulflardan foydalanishi kerak.

6.2-§. Kiberxavfsizlik vositalari

Hozirgi zamonaviy dunyoda tajovuzkorlar foydalanuvchilardan ma’lumotlarni o‘g‘irlashning an’anaviy yoki eski usullaridan emas raqamli vosita orqali ma’lumotlarni o‘g‘irlash uchun ishlatilishi mumkin bo‘lgan yangi texnologiyalar va vositalarni o‘zlashtirishmoqda. Bunda kiberhujumchilar tarmoqqa kirib, hujum qilishga harakat qiladilar, kiberhimoyachilar esa tajovuzkorlarning ma’lumotlariga kirishini bloklaydi yoki to‘xtatadi. Biroq, bu janglar jismoniy rejimda emas, ular hujum qilish va himoya qilish uchun turli xil eng yaxshi kiberxavfsizlik vositalaridan foydalanadilar. Xuddi shu vosita ham ijobiy, ham salbiy rejimda ishlatilishi mumkin. Bularning barchasi vositadan foydalanayotgan odamning fikri va maqsadiga bog‘liq. Bir necha sabablarga ko‘ra kiberbozorda juda ko‘p ochiq manbali vositalar mavjud.

Muayyan sohalarga asoslangan kiberxavfsizlikda ko‘plab vositalar mavjud.

Kiberxavfsizlik vositalarining turlari sifatida quyidagilar keltiriladi.

- Xavfsizlik ma’lumotlari va hodisalarni boshqarish vositalari;
- Zaiflikni baholash vositalari;
- Raqamli kriminalistika vositalari;
- Penetratsiyon testlash vositalari;
- Xavfsizlik devori vositalari;
- IDS/IPS vositalari;
- Imtiyozli kirishni boshqarish vositalari;
- Yakuniy nuqtani aniqlash va javob berish vositalari;
- Tarmoqni aniqlash va javob berish vositalari;

— Elektron pochta xavfsizligi vositalari;
— Ma’lumotlarni yo‘qotishning oldini olish vositalari.

Zamonaviy kiberxavfsizlik vositalari sifatida quyidagilarni keltirish mumkin.

NMAP, Wireshark, Metasploit, Aircrack, Hashcat, Burpsuite, Nessus Professional, Snort, Intruder, Kali Linux va boshqalar.

1. NMAP

6.2-rasm. NMAP kiberxavfsizlik dasturiy vositasi

NMAP, Network Mapper-ning qisqa shakli tarmoqlarni skanerlash uchun ishlatiladigan ochiq manbali vositadir. Ushbu vosita, asosan, xostlarni topish, xizmat yoki port ochiq bo‘lgan tarmoq qurilmalari haqida ma’lumot to‘plash va xavfsizlik zaifliklarini, xost qurilmasining ish vaqtini aniqlash uchun foydalidir. NMAP Windows, Linux va hatto MAC OS kabi asosiy OS platformalarini qo‘llab-quvvatlaydi. Ushbu vositaning asosiy afzalligi moslashuvchan, oson ko‘chirish, bepul va yaxshi hujjatlashtirilgandir.

NMAP vositasini https://nmap.org/download.html rasmiy portalida yuklab olish mumkin.

2. Wireshark

6.3-rasm. Wireshark kiberxavfsizlik dasturiy vositasi

Wireshark ko‘pchilik tomonidan tarmoq protokolini tahlil qilish uchun global miqyosda qo‘llaniladigan vositalardan biridir. Ushbu vosita sizga pcap yordamida suratga olishga, har bir paketni batafsil tarzda saqlashga va tahlil qilishga yordam beradi. Wireshark Windows, Linux, Solaris, macOS va boshqa OS platformalarini qo‘llab-quvvatlaydi. Wireshark shuningdek, foydalanuvchi interfeysi opsiyasiga ega tcpdumpga o‘xshash ochiq manbali vositadir. Wireshark-ning asosiy xususiyatlari shundaki, real vaqt rejimida ma’lumotlarni turli xil protokollardan tahlil qilish mumkin. Platformada paketlarni har qanday muayyan qoidaga mos kelganda ko‘rsatish uchun kodlash xususiyati ham mavjud. Ushbu vosita paketlarni faqat pcap-ni qo‘llab-quvvatlaydigan

tarmoqlardan oladi.

Vositani https://www.wireshark.org/#download rasmiy veb-saytidan yuklab olish mumkin.

3. Metasploit

6.4-rasm. Metasploit kiberxavfsizlik dasturiy vositasi

Metasploit - bu kiberxavfsizlik sanoatida qo‘llaniladigan kuchli va mashhur ochiq manbali penetratsiyani testlash vositasidir. Ushbu vosita kiberhujumchilar va shuningdek, kiber himoyachilar tomonidan qo‘llaniladi. Metasploit-da ko‘plab o‘rnatilgan modullar mavjud bo‘lib, ulardan foydalanish, foydali yuklarni bajarish, yordamchi funktsiyalar, kodlash, tinglash, qobiq kodlarini bajarish, Nops uchun foydalanish mumkin. Ushbu vositadan kompaniyaning xavfsizlik holatini yaxshilash uchun xavfsizlikni baholashni amalga oshirish uchun foydalanish mumkin.

Vositani https://www.metasploit.com/download rasmiy veb-saytidan yuklab olish mumkin

4.Aircrack-ng

6.5-rasm. Aircrack-ng kiberxavfsizlik dasturiy vositasi

Aircrack-ng Wi-Fi tarmog‘i xavfsizligini boshqarish vositalarini baholash xavfsizlik vositalari to‘plamidir. U WiFi xavfsizligini kuzatish, hujum qilish, sinovdan o‘tkazish, buzishni o‘z ichiga oladi. Ushbu vosita asosan xakerlar tomonidan WEP, WAP, WAP2 shifrlash usullarini buzish orqali WiFi-ni buzish uchun ishlatiladi. Ushbu vosita sniferlash va paketlarni in’ektsiya qilish xususiyatlariga ega. Ushbu vosita Windows, Linux, macOS, Solaris, OpenBSD, FreeBSD uchun mavjud.

Vositani ushbu rasmiy havoladan yuklab olish mumkin https://www.aircrack-ng.org/downloads.html

5. Hashcat

6.6-rasm. Hashcat kiberxavfsizlik dasturiy vositasi

Hashcat parollarni buzish uchun global miqyosda qo‘llaniladigan vositadir. Ushbu vosita deyarli 250 dan ortiq xesh algoritmlarini qo‘llab-quvvatlaydi. Ushbu vosita Windows, Linux va macOS platformalarini qo‘llab-quvvatlaydi. Ushbu vositaning asosiy xususiyatlari juda tez, moslashuvchan, ko‘p qirrali va ochiq manbali vosita bo‘lib, bir nechta xesh qiymatlari bo‘yicha qo‘pol kuch hujumlarini amalga oshirishga yordam beradi. LM, MD-family va SHA-family kabi xeshlash algoritmlari qo‘llab-quvvatlanadi. Hashcat turli kiber hujumlarni amalga oshirish uchun ishlatilishi mumkin, masalan, qo‘pol kuch hujumlari, kombinator hujumlari, lug‘at hujumlari, barmoq izlari hujumlari, niqob hujumlari, gibrid hujumlar, almashtirish hujumlari, Toggle-Case hujumlar va boshqalar.

Vositani https://hashcat.net/hashcat/ rasmiy veb-saytidan yuklab olishingiz mumkin.

6. BurpSuite

6.7-rasm. BurpSuite kiberxavfsizlik dasturiy vositasi

BurpSuite penetratsion test sohasida qo‘llaniladigan bir nechta vositalarning birlashtirilgan platformasidir. Ushbu vosita “Port Swigger” kompaniyasi tomonidan ishlab chiqilgan. Turli xil xavfsizlik sinovlari jarayonlari uchun ishlatiladigan Spider, Proksi, Intruder, Repeater, Sequencer, Dekoder, Extender, Scanner va boshqalar kabi turli xil vositalar mavjud. Ushbu vositadan loyiha darajasida ham, foydalanuvchi darajasida ham foydalanish mumkin.

Ushbu vositaning jamoat nashrini uning rasmiy veb-saytidan yuklab olish mumkin https://portswigger.net/burp/communitydownload

7. NessusProfessional

6.8-rasm. NessusProfessional kiberxavfsizlik dasturiy vositasi

Nessus Professional zaiflikni baholash uchun ishlatiladigan tijorat

vositasidir. Ushbu vosita xavfsizlik kamchiliklari, xavfsizlik zaifliklari, tizimlar, serverlar va tarmoq qurilmalarining noto‘g‘ri konfiguratsiyasi haqidagi ma’lumotlarni topishga yordam beradi. Ushbu vositadan muvofiqlik va audit maqsadlarida ham foydalanish mumkin. Ushbu vosita ilg‘or vosita bo‘lib, unda barcha xususiyatlar avtomatlashtirilgan. Asososan tarmoqni skanerlash, kengaytirilgan skanerlash, kengaytirilgan dinamik skanerlash, zararli dasturlarni skanerlash, mobil qurilmalarni skanerlash, veb-ilovalar sinovlari, hisob ma’lumotlarini tuzatish tekshiruvi, blokirovkani aniqlash, va mavjud bo‘lgan zaifliklarni skanerlash kabilarni bajaradi.

8. Snort

6.9-rasm. Snort kiberxavfsizlik dasturiy vositasi

Snort eng yaxshi ochiq manbali IPS/IDS vositalaridan biridir. Ushbu vosita zararli faoliyatni aniqlashga va foydalanuvchilarga xavfsizlik ogohlantirishlarini yaratishga yordam beradigan qoidalar to‘plamidan foydalanadi. Snort zararli manbalarni blokirovka qilish uchun tarmoqning birinchi qatlamida ham o‘rnatilishi mumkin. Snort ham shaxsiy, ham rasmiy maqsadlarda ishlashi va ishlatilishi mumkin. Sniffer uchta rejimda sozlanishi mumkin: “Sniffer rejimi, Paket jurnali rejimi, Tarmoq hujumlarini aniqlash tizimi rejimi”. Ushbu vosita Cisco Systems tomonidan ishlab chiqilgan.

Vositani https://www.snort.org/downloads rasmiy veb-saytidan yuklab olish mumkin.

9. Intruder

6.10-rasm. Intruder kiberxavfsizlik dasturiy vositasi

Intruder – kiberxavfsizlikni baholash, kompaniya tuzilmasidagi zaifliklarni skanerlash vositasidir. Ushbu vosita SQL in’ektsiyasi, saytlararo skriptlar, CSRF va boshqalar kabi veb-ilova hujumlarini, standart parollar bilan sozlangan ilovalarni va hokazolarni qidirishi mumkin. Bu “Pro, Essential, Verified” uchta versiyasiga ega vositadir.

10. Kali Linux

6.11-rasm. Kali Linux kiberxavfsizlik dasturiy vositasi

Kali Linux ochiq manbali va ilg‘or kirish test vositasidir. Ushbu vositani ishlab chiqishning asosiy maqsadi kiberhujumchilar va axloqiy xakerlar sifatida harakat qilishdir. Kali Linux Aircrac-ng, Autopsy, Burp Suite, Hashcat, Jon the ripper, Maltego, Nmap, OWASP ZAP, Sqlmap, WPScan, Nessus, Hydra, Wireshark, Nikto, Vulnhub, Metasploit kabi 600 dan ortiq vositalar to‘plamini taqdim etadi. Kali-Linux - bu Debian-ga asoslangan Linux vositasi bo‘lib, u Offensive Security tomonidan qo‘llab-quvvatlanadi va ishlab chiqiladi.

Raqamli kriminalistika vositalarini turli xil toifalarga bo‘linish mumkin, jumladan, ma’lumotlar bazasi kriminalistikai, disk va ma’lumotlarni to‘plash, elektron pochta tahlili, fayllar tahlili, fayllarni ko‘rish vositalari, internet tahlili, mobil qurilmalar tahlili, tarmoq ekspertizasi va ro‘yxatga olish kitobi tahlili. Bundan tashqari, ko‘plab vositalar bir vaqtning o‘zida bir nechta funktsiyalarni bajaradi va raqamli kriminalistikavositalarining muhim tendentsiyasi “o‘rashlar” bo‘lib, u turli funktsiyalarga ega yuzlab maxsus texnologiyalarni bitta umumiy vositalar to‘plamiga jamlaydi.

Raqamli kriminalistika vositalari kiberhujumning raqamli dalillarini tiklashga, ma’lumotlar yoki muhim tizimlarni saqlashga yordam berish uchun mo‘ljallangan apparat yoki dasturiy ta’minotdir.

Kiberxavfsizlik bo‘yicha mutaxassislar o‘zlarining tergovlarini amalga oshirish uchun texnologiyaga tayanadilar va bu ehtiyoj kriminalistika tahlili vositalari uchun katta bozorni yaratdi. Raqamli kriminalistikavositalarining asosiy turlari ro‘yxati ko‘pincha quyidagilarni o‘z ichiga oladi:

- Disk kriminalistika vositalari,
- Tarmoq kriminalistika vositalari,
- Simsiz tarmoq kriminalistika vositalari,
- Ma’lumotlar bazasi kriminalistika vositalari,
- Zararli dasturiy ta’minot kriminalistika vositalari,
- Elektron pochta kriminalistika vositalari,
- Xotiraga asoslangan kriminalistika vositalari,

- Mobil telefon uchun kriminalistika vositalari,
- Kiber kriminalistika platformalari.

Ochiq manbali kriminalistika platformalari raqamli kriminalistikaning boshlang‘ich darajadagi vositalari hisoblanadi. Quyida ba’zi ochiq manbali raqamli kriminalistika vositalari keltirilgan.

1. Paraben Korporatsiyasi.

Paraben korporatsiyasi kiberxavfsizlik bozoriga 1999-yilda kirib, raqamli kriminalistika, xavflarni baholash va xavfsizlik yechimlariga qaratilgan vositadir. Bugungi kunda, milliardlab qurilmalarga ega dunyoda Paraben elektron pochta, kompyuterlar, smartfonlar va narsalar Interneti (IoT) qurilmalari bilan bog‘liq kriminalistika tekshiruvlarni qamrab oladi .

2. Sleuth to‘plami Va Autopsy.

Sleuth Kit (TSK) va Autopsy mashhur ochiq manba raqamli tergov vositalaridir. Sleuth Kit ma’murlarga diskdagi tasvirlarni tekshirish uchun buyruq qatori vositalari kutubxonasi orqali fayl tizimi ma’lumotlarini tahlil qilish imkonini beradi. Autopsy uning grafik foydalanuvchi interfeysi (GUI) va TSKning imkoniyatlarini oshirish uchun davlat va xususiy kompyuter tizimlarini tekshirishda foydalaniladigan raqamli kriminalistika platformasi.

3. Magnit kriminalistika vositasi.

Huquqni muhofaza qilish organlari tomonidan foydalaniladigan raqamli kriminalistika vositalari yetarli emasligini payqagan kanadalik politsiyachi Jad Saliba 2011 yilda Magnet Forensics kompaniyasiga asos solgan . Kompaniya davlat va xususiy tashkilotlarga raqamli sud-tibbiy tergov vositalarini taklif etadi.

4. CAINE.

Kompyuter Tergov Muhiti (CAINE) - raqamli kriminalistika maqsadlari uchun Ubuntu va Linux-ga asoslangan ochiq manbali italyan tarqatish. CAINE mavjud Windows, Linux va Unix tizimlari xavfsizlik vositalari bilan integratsiyalashgan.

5. Kroll kompyuter kriminalistika vositasi.

Krollning kompyuter kriminalistika xizmatlari va ekspertlari hech qanday raqamli dalillar e'tibordan chetda qolmasligini ta'minlaydi va ma'lumotlar manbalarining soni yoki joylashuvidan qat'i nazar, tergov yoki sud jarayonining istalgan bosqichida yordam beradi.

6. Sanssift.

SIFT Workstation - bu raqamli sud ekspertizalarini o'tkazish uchun bepul va ochiq manbali hodisalarga javob berish va sud-tibbiy vositalar to'plami. Bepul va ochiq manbali yechimlarini taklif etuvchi SIFT Workstation foydalanish uchun turli xil variantlarni taqdim etadi, shu jumladan virtual mashina (VM), Ubuntu-da mahalliy o'rnatish yoki Linux quyi tizimi orqali Windows-ga o'rnatish mumkin.

7. Externo.

Oregon shtatining Portlend shahridan bo'lgan Exterro 2004 yilda ishga tushirilgan va ish oqimiga asoslangan dasturiy ta'minot va boshqaruv, xavf va muvofiqlik echimlariga ixtisoslashgan. Bizning barcha tanlovlarimiz tabiatan tashkilotlarning muvofiqlikni saqlash ehtiyojlarini qo'llab-quvvatlasa-da, Exterro ichki yuridik guruhlarga

yordam berish, muvofiqlik jarayonlarini soddalashtirish va xavflarni nazorat qilish uchun ayniqsa qimmatlidir.

8. X-ways.

X-Ways Forensics - bu kompyuter sud ekspertlari uchun ish muhiti. Resursga chanqoq, ammo tezkorligi bilan tanilgan, u WinHex hex va disk muharririga asoslangan bo‘lib, qo‘shimcha disk va ma’lumotlarni yozib olish dasturlari, klonlash, tasvirlash va boshqa vositalarni taklif etadi.

9. Cellebrite.

1999 yilda boshlangan Cellebrite huquqni muhofaza qilish organlari va qurilmalar ma’lumotlarini to‘plash, ko‘rib chiqish, tahlil qilish yoki boshqarishi kerak bo‘lgan korxonalar uchun mobil qurilmalar kriminalistikaiga ixtisoslashgan. Raqamli razvedka tergov platformasi tergov hayotiy siklini birlashtirishga va raqamli dalillarni saqlashga yordam beradi.

10. ProDiscover.

ProDiscover 2001 yilda davlat va xususiy tashkilotlarga raqamli jinoyatlarni ochishda yordam berish uchun ishga tushirilgan. 2021 yil holatiga ko‘ra, Hindistonda joylashgan provayder NIST, NASA va Wells Fargo kabi 400 dan ortiq mijozlari bilan 70 dan ortiq mamlakatlarda ishlaydi. ProDiscover Forensics dalillarni to‘plash, saqlash, filtrlash va tahlil qilish uchun kriminalistika vositasidir.

11. Wireshark.

Birinchi marta 1998 yilda ishlab chiqilgan Wireshark tarmoq paketlarini sud-tibbiy tekshiruvi va tahlili bilan shug‘ullanadi hamda

tarmoqlarni sinovdan o‘tkazish va nosozliklarni bartaraf etish bilan shug‘ullanadi. Bunga ma’lumotlar tuzilmalarini qamrab oluvchi uch panelli paketli brauzerda yuzlab protokollarni tekshirish kiradi.

Penetratsion test (shuningdek, pentesting deb ham ataladi) - bu tashkilotlar tomonidan xavfsizlik nazoratidagi zaifliklarni aniqlash, sinab ko‘rish va bartaraf etish uchun foydalaniladigan kiberxavfsizlik usuli.

Penetratsion test vositalari ma’lum vazifalarni avtomatlashtirish, sinov samaradorligini oshirish va faqat qo‘lda tahlil qilish usullari bilan aniqlash qiyin bo‘lgan muammolarni aniqlash uchun kirish testining bir qismi sifatida ishlatiladi. Tahdidlar va zaifliklar baholangandan so‘ng, penetratsion testerlar tashkilotga kibermudofaa tizimini yaxshilash uchun aniqlangan xavflarni bartaraf etishga yordam beradigan hisobot taqdim etadilar.

Pentesting vositalari zamonaviy, keng miqyosli AT muhitlarida xavfsizlikni tekshirish uchun muhim ahamiyatga ega. Ular murakkab, gibrid muhitda aktivlarni topishga imkon beradi va sinovchilarga tizimlarni xavfsizlik mezonlari va muvofiqlik talablariga muvofiq baholashda yordam beradi.

Penetratsiyani tekshirish to‘plami turli xil vositalarni o‘z ichiga olishi kerak. Bir nechta Penetratsiyani tekshirish vositalari mavjud:

— **Port skanerlari** - tizimdagi ochiq portlarni aniqlaydi. Bu testerlarga ular kirishga harakat qilayotgan tarmoqda ishlayotgan operatsion tizim va ilovalarni aniqlashga yordam beradi. Port skanerlari razvedkada qo‘llaniladi va potentsial hujum vektorlari uchun g‘oyalarni taqdim etishi mumkin.

— **Zaiflik skanerlari** - serverlar, operatsion tizimlar va ilovalardagi ma’lum zaifliklarni, shuningdek sinovda ishlatilishi mumkin bo‘lgan noto‘g‘ri konfiguratsiyalarni qidiradi. Zaiflik skanerlari tomonidan taqdim etilgan hisobotlar penetratsion sinovchilarga tizimga dastlabki kirish huquqini beruvchi foydalaniladigan zaiflikni tanlashda yordam beradi.

— **Tarmoq sniffer** - tarmoq trafigidagi ma’lumotlarni, shu jumladan uning manbasini, manzilini, tarmoqda aloqa qiladigan qurilmalarni, ishlatiladigan protokollar va portlarni kuzatib boradi. Bu ma’lumotlar shifrlangan yoki yo‘qligini tekshirish va penetratsiya testi paytida foydalanish mumkin bo‘lgan aloqa yo‘llarini aniqlash uchun foydali bo‘lishi mumkin.

— **Veb-proksi** - penetratsion testerlarga o‘z brauzeri va tashkilot veb-serverlari o‘rtasidagi trafikni ushlab turish va o‘zgartirish imkonini

beradi. Bu saytlararo skript (XSS) yoki saytlararo so‘rovlarni soxtalashtirish (CSRF) kabi hujumlarni faollashtirishi mumkin bo‘lgan yashirin shakl maydonlarini va boshqa HTML xususiyatlarini aniqlash imkonini beradi.

— **Parolni buzish**- parolni xeshlash maqsadli tizim yoki tarmoqdagi imtiyozlarni oshirish vositasi sifatida tajovuzkorlar uchun umumiy maqsaddir. Parolni buzish vositalari penetratsion testerlarga tashkilot xodimlariga xavf tug‘diradigan zaif parollardan foydalanayotganligini aniqlash imkonini beradi.

Penetratsion testlash bo‘yicha mutaxassislar uchun vositalar:

— **Kali Linux** - bu kirish testini, xavfsizlikni tekshirishni va tegishli faoliyatni osonlashtiradigan operatsion tizim. Bu ochiq manba sifatida taqdim etilgan va Offensive Security tomonidan qo‘llab-quvvatlanadigan Debian-ga asoslangan Linux distributividir.
— **Armitage** - tarmoq hujumlarini boshqarishning grafik vositasi.
— **Nmap** - port skaneri.
— **Wireshark** - paketlar analizatori.
— **Metasploit** - minglab ekspluatatsiya modullari bilan penetratsion test tizimi.
— **Jon Ripper** - parolni buzuvchi.
— **sqlmap** - avtomatlashtirilgan SQL in’ektsiyasi va ma’lumotlar bazasi importi.
— **Aircrack-ng** - simsiz LAN kirishini tekshirish uchun dasturiy ta’minot to‘plami.
— **OWASP ZAP** — veb-ilovalar xavfsizligi skaneri.
— **Burp suite** - dastur xavfsizligini tekshirish.

6.3-§. Xodimlarni kiberxavfsizlik bo‘yicha o‘qitish

Kiberxavfsizlikni ta’minlash bugungi kunda axborot xavfsizligini ta’minlashning umumiy tizimi doirasida har bir davlatning asosiy vazifalaridan biri bo‘lib qolmoqda. Kiberxavfsizlik bo‘yicha treninglar masofaviy ishchilarga korxona infratuzilmasidan tashqarida bo‘lganida qurilmalardan qanday foydalanishni o‘rgatadi.

Xodimlarga kiberxavfsizlik bo‘yicha bilim va ko‘nikmalarni o‘rgatish sababi oddiy: agar xodimlar xavfsizlikka tahdidini aniqlashni bilmasalar, ularni bartaraf etish, yo‘q qilishni bajara olmaydi. Masalan, 2019-yilda kiberxavfsizlik bo‘yicha o‘tkazilgan tadqiqot shuni ko‘rsatdiki, elektron pochta xavfsizligi va xodimlarni o‘qitish

kiberxavfsizlik bo‘yicha mutaxassislar duch keladigan asosiy muammolar sifatida belgilangan. Buni Wombat Security Technologies tomonidan so‘ralgan xodimlarning 30% dan ortig‘i fishing yoki zararli dastur nima ekanligini bilmasligi ham tasdiqlagan.

Bir so‘z bilan aytganda, kiberxavfsizlikning 90-95 foizi inson xatosi tufayli sodir bo‘ladi. Bundan tashqari, xalqaro tashkilotlarning atigi 38 foizi murakkab kiberhujumlarga qarshi kurashishga tayyorligini bildirgan. Kompaniyalarning yana 54 foizi so‘nggi 12 oy ichida bir yoki bir nechta hujumlarga duch kelganini va bu raqam har oy o‘sib borayotganini ma’lum qilishgan.

Bugungi kunda kiberjinoyatchilarning sevimli taktikasi ijtimoiy muhandislik - jabrlanuvchilarni shaxsiy ma’lumotlarni o‘z ixtiyori bilan yoki bilmagan holda topshirishga ishontirish uchun ularni psixologik manipulyatsiya qilishdir. Kiberhujumlarning 95% ulushi fishing firibgarliklariga to‘g‘ri keladi, shuning uchun fishing haqida ma’lumotlarni o‘qib, o‘rganish juda muhimdir.

Kiberxavfsizlikka zararli dasturlar ham doimiy tahdidni keltirib chiqaradi. Bu qurilmalarni buzish yoki xakerlarga tarmoqqa kirishni ta’minlash uchun mo‘ljallangan ilovalar yoki dasturlarni yuklab olishni o‘z ichiga oladi.

Ish jarayonlarida AT keng qo‘llanishi, raqamli texnologiyalarni joriy etish va internet tarmog‘idan foydalanish sababli xodimlar uchun kiberxavfsizlik ko‘nikmalarini o‘qitishni talab qiladi.

Internet buyumlari (IoT). Xodimlar shaxsiy qurilmalarni kompaniya tarmoqlariga ulaydi yoki hatto rasmiy ish uchun foydalanadi. Shaxsiy qurilmalarni boshqa mashinalar va tarmoqlarga ulash zaifliklarni kuchaytiradi. Mobil qurilmalar tashkilotning ichki kiberxavfsizligiga katta tahdid soladi, chunki ularning aksariyati yetarli darajada himoyalanmagan. IoT hujumlarini ish joyiga “O‘z qurilmangizni olib kelish” amaliyotini boshqarish va ehtimol minimallashtirish va xodimlar orasida xavfsizlik siyosatiga qat’iy rioya qilinishini ta’minlash orqali hal qilish mumkin.

Xodimlarni kiberxavfsizlik bo‘yicha hodimlarning malakasini oshirish

Kiberxavfsizlik bo‘yicha bilim va ko‘nikmaga ega xodimlar kiberjinoyatlarga qarshi birinchi va asosiy himoya chizig‘idir. Ish kompyuteri yoki mobil qurilmaga kirish huquqiga ega bo‘lgan har qanday xodim kiberxavfsizlik bo‘yicha treningdan o‘tishi kerak. Chunki deyarli har bir xodim kiberjinoyatchi nishoniga aylanishi mumkin. Shaxsiy

telefonlar korporativ tarmoqlarga kirish uchun ishlatilishi mumkin bo‘lgan ma’lumotlarni saqlashi mumkin, yoki xodimni shaxsiy ma’lumotlari o‘g‘irlansa kompaniya axborot tizimiga kirish uchun ishlatilishi mumkin, bu esa kiberjinoyat faoliyatini amalga oshirishga imkon beradi.

Xodimlar huquqbuzarliklarni aniqlash va oldini olishlari uchun ularga tahdidning turli shakllari haqida asosiy bilim kerak. Kibertahdidlarga spam, fishing, zararli dasturlar va tarmoq hujumlari, ijtimoiy muhandislik kiradi.

Xodimlarni o‘qitishda zararli dasturlar turlari, zararlash darajasi, ularga qarshi himoyalanish usullari haqida ma’lumot berish, hamda amaliy ko‘rsatmalar bilan tushintirish kerak. Shu bilan birga ijtimoiy muhandislik haqida batafsil ma’lumot berilishi kerak. Chunki ijtimoiy muhandislar o‘zlarini soxta, ammo ishonchli onlayn identifikator sifatida yashirib, kerakli ma’lumotlarni o‘ziga jalb qiladi.

Parollar bugungi kunda axborot tiziminingn barcha joyuda qo‘llaniladi. Xavfsizlik vositasi sifatida ishlab chiqilgan bu taktika ko‘p odamlarni eslab qolish oson va shuning uchun taxmin qilish oson bo‘lgan umumiy, takrorlanuvchi parollarni o‘rnatishiga olib keldi. Kiberxavfsizlik bo‘yicha mashg‘ulotlar parollar qanchalik muhimligini tushunishga yordam berishi va parollarni yaratishi siyosati va saqlashi mumkin bo‘lgan ishonchli dasturlar haqida tushincha berishi kerak.

Xodimlarning elektron pochtasi va ijtimoiy media odatlari kompaniyani korporativ ilovalar va ijtimoiy hisoblarga hujum qiladigan, ma’lumot va pullarni o‘g‘irlaydigan zararli dasturlarga duchor qilishi mumkin. Shuning uchun mashg‘ulotlarda elektron pochta, Internet va ijtimoiy tarmoqlardan foydalanish bo‘yicha siyosat va ko‘rsatmalarni o‘z ichiga olishi juda muhimdir.

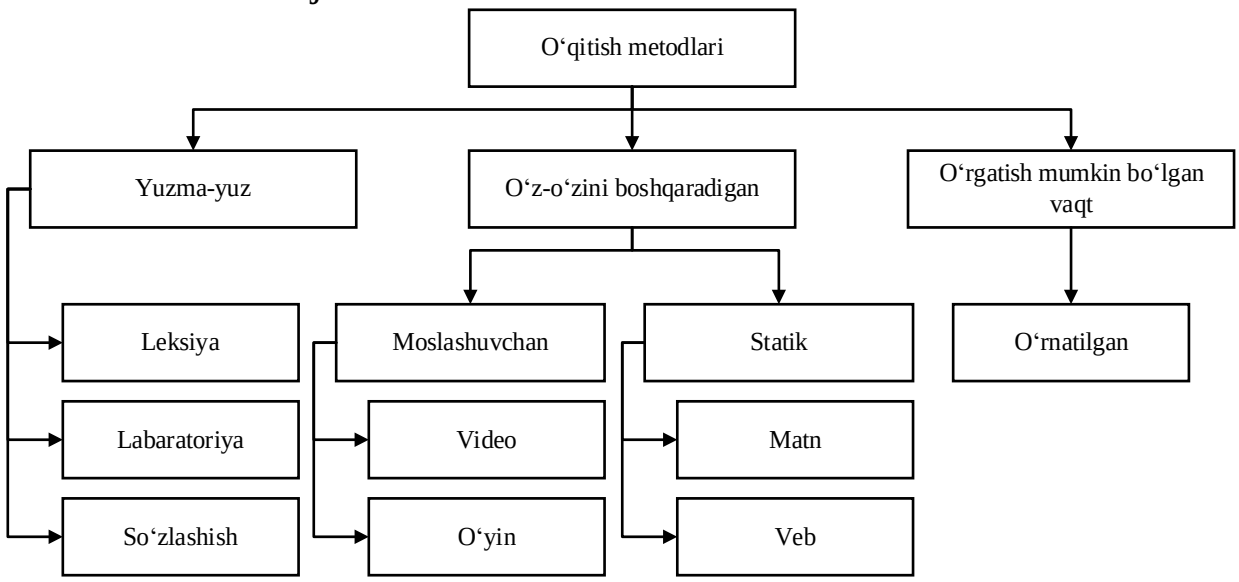
Har bir kompaniyaning o‘z ma’lumotlarini himoya qilish siyosati bor, lekin korxonaning barcha xodimlari ushbu siyosatdan xabardor bo‘lmasligi mumkin. Yangi xodimlar uchun axborot xavfsizligi bo‘yicha bilim va ko‘nikma berib, himoya qilishning qonuniy va amaliy majburiyatlarini tushuntirishi kerak. Barcha xodimlar qoidalarni eslab qolishlari va amalda qo‘llay bilishlari uchun muntazam malaka oshirib borishlari zarur.

Kiberxavfsizlik bo‘yicha o‘qitish usullari.

Hech qachon tayyor o‘quv modullari yoki online veb-kurslar bilan kifoyalanmaslik kerak. Korxona bilan bevosita ishlaydigan kiberxavfsizlik bo‘yicha professional mutaxassislar jalb etish kerak.

Professional mutaxassislar olib borgan o‘quv mashg‘uloti yangi kiberxavfsizlikni ta’minlash qoidalari, ma’lumotlar maxfiyligi va xodimlarning ehtiyojlariga moslashtirilgan to‘liq xavfsizlik strategiyasini ishlab chiqish imkonini beradi. Kiberxavfsizlik bo‘yicha o‘quv mashg‘ulotlari tez-tez o‘tkazilishi kerak, bu seanslar oralig‘ida xavfsiz xatti-harakatlarni amalga oshirish imkoniyatini beradi.

Kiberxavfsizlik bo‘yicha xabardorlikni oshirish va foydalanuvchilarni fishing hujumlari haqida o‘rgatish dasturi bir yoki bir nechta etkazib berish usullari yordamida amalga oshiriladi. Kiberxavfsizlik bo‘yicha o‘qitish va xabardorlikni oshirish usullarining bir nechta turlari mavjud.



6.5-rasm. Kiberxavfsizlik bo‘yicha treningni o‘tkazish usullari taksonomiyasi

6.5-rasmda kiberxavfsizlikdan xabardorlikni oshirish bo‘yicha o‘qitish usullarining taklif etilayotgan taksonomiyasi ko‘rsatilgan. Asosan, etkazib berish usullarini uchta asosiy sinfga ajratiladi: yuzma-yuz sinf, o‘zini o‘zi boshqaradigan sinf va o‘rnatilgan sinf. Yetkazib berish usulining o‘z-o‘zidan boshqariladigan klassi moslashuvchan va statik toifalarga bo‘linadi.

Onlayn xavfsizlik tahdidlari haqida xabardorlikni oshirish yangi xodimlarning birinchi kunidan boshlanishi kerak. Bu xodimlarning qo‘llanmasiga ma’lumotlarni himoya qilish siyosati va qoidalarini, internetdan foydalanish qoidalarini kiritishga yordam beradi.

Kiberxavfsizlik bo‘yicha trening turlari

Kiberxavfsizlikka sarmoya kiritish barcha korxonalar uchun juda muhim va xodimlar tegishli o‘quv dasturidan foydalanishlari kerak.

Kiberjinoyatchilar tomonidan yaratilgan yangi tahdidlar bilan kurashish uchun kiberxavfsizlik bo‘yicha treninglaringiz yangilanib turishi kerak. Bunga o‘quv materiallarini ko‘rib chiqish va kontentni doimiy ravishda yangilash kiradi.

Hujumlarni simulyatsiya qilish, keng tarqalgan va kam uchraydigan hujumlar haqida xabardorlikni oshirish va batafsil hisobot berishni o‘z ichiga olgan turli xil o‘qitish usullari mavjud.

Quyidagi o‘quv dasturlari ro‘yxati xodimlarga kiberxavfsizlik bo‘yicha treningni joriy etishda yordam beradi. Kiberxavfsizlik doimiy muammo bo‘lib, jamoangiz yangi hujumlarga qarshi tayyor bo‘lishini ta’minlash uchun har chorakda tez-tez yangilanishlarni talab qiladi.

1. Kiberxavfsizlikdan xabardorlik bo‘yicha trening

Kiberxavfsizlik bo‘yicha treningning asosiy shakli xodimlarning potentsial tahdidlar haqida xabardorligini oshirishga qaratilgan.

U yangi ishga qabul qilish uchun xodimlarni ishga qabul qilish jarayoniga kiritilishi va jamoa a’zolariga ham tarqatilishi mumkin.

Mijoz ma’lumotlari bilan ishlashda qonuniy majburiyatlar mavjud va bu ma’lumotlarni himoya qilish har bir xodim ishining muhim qismidir.

1. Habardorlik treningi quyidagilarni o‘z ichiga oladi:

1)Elektron pochta xavfsizligi bo‘yicha trening

2) Internet xavfsizligi bo‘yicha trening

3) Axborot almashish tartiblari bo‘yicha trening

4) Jamiyatga qarshi asosiy muhandislik ta’limi

Ijtimoiy muhandislik, fishing va internetga asoslangan xavflar kabi umumiy kiberxavfsizlik jinoyatlari aniq ko‘rinishi mumkin, ammo ularni qoplash muhim. Xodimlar potentsial tahdidni qanday aniqlashni va tashkilotingiz ichida kimga ogohlantirish kerakligini bilishlari kerak.

Xodimlaringizni so‘nggi kiberxavfsizlik muammolari bilan tezlashtirish uchun ko‘plab bepul onlayn o‘quv kurslari mavjud. Kurslar nufuzli tashkilotlar bilan bir qatorda davlat muassasalarida ham mavjud.

2. Ixtisoslashtirilgan kiberxavfsizlik dasturlari

IT guruhidagilar va xavfsizlik tahlilchilari uchun yanada rivojlangan dasturlar mavjud.

Ushbu dasturlar xodimlarga kiberxavfsizlikni chuqurroq tushunishga yordam beradi va ularga mudofaasini shakllantirish uchun zarur ko‘nikmalarni beradi.

Ushbu trening quyidagilar bilan bog‘liq bo‘lishi kerak:

1)OWASP eng yaxshi o‘ntaligi

2)CWE/SANS TOP 25 ta eng xavfli dasturiy ta’minot xatolari
3)Bulut va yetkazib berish uchun xavfsiz operatsiyalar uchun DevOps treningi.
4)CSA treningi
5)Tarmoq operatsiyalari bo‘yicha trening
6)Whitehat xakerlik va penetratsiya testi bo‘yicha trening
7)Tizim ma’murlari uchun operatsion tizim (OT) xavfsizligi bo‘yicha trening

Bootcamplar kiberxavfsizlik bo‘yicha professional ko‘nikmalarni rivojlantirishning eng keng qamrovli usuli hisoblanadi, chunki u zaiflikni baholash, ma’lumotlar xavfsizligi va kirish testlarini o‘z ichiga oladi. Ushbu dasturlar kompyuter fanlari tamoyillarini o‘rgatish uchun mo‘ljallangan va talabalar kiberhujumlarga qarshi amaliy tajribaga ega bo‘lishlari mumkin.

Kiberxavfsizlik bo‘yicha guruhlarni tayyorlash uchun ilg‘or dasturiy yechimlarni ko‘rib chiqamiz.

1. Cofense PhishMe.Cofense PhishMe keng qamrovli tadqiqotlar, tahdidlar ma’lumotlari va ilg‘or fishing himoyasi resurslari orqali foydalanuvchilarni haqiqiy fishing taktikasi haqida o‘rgatadi.

6.6-rasm. Kiberxavfsizlikni o‘qituvchi Cofense kompaniyasi

Cofense kompaniyalarni tovlamachilik, biznes elektron pochta xabarlarini buzish va fishing orqali kiberhujumlardan himoya qilish uchun bir qator bulutga asoslangan yechimlarni taklif etadi.

Cofense PhishMe - bu xavfsizlik bo‘yicha ta’lim yechimi bo‘lib, o‘z turidagi eng mashhur platformalardan biri. Bu tashkilotning ijtimoiy muhandislik hujumlariga chidamliligini oshirishga qaratilgan xodimlarni o‘qitish va fishing simulyatsiyasi vositasidir.

Cofense PhishMe foydalanuvchining mazmunli xatti-harakatlarini yaratish uchun faol fishing tahdidlarini simulyatsiya qiladi. Platforma korxonalarga har xil qiyinchilik darajasidagi ijtimoiy muhandislik hujumlarining muayyan turlari uchun sozlangan real simulyatsiyalarni taklif etadi. Trening bilan bir qatorda, Cofense qo‘shimcha ravishda

elektron pochta tarmog‘i uchun fishingga qarshi himoyani taqdim etadi.

Cofense Playbooks sizga simulyatsiya stsenariylari, multimedia va ta’lim mazmunini o‘z ichiga olgan 12 oylik to‘liq dasturni sozlash imkonini beradi.

Cofense simulyatordagi har bir kontent qismini auditoriya ehtiyojlariga javob berishiga ishonch hosil qilish uchun tekshiradi - kontent 36 tilda, shu jumladan rus tilida taqdim etiladi.

2. **Knowbe4 Enterprise Security Awareness Training.** Korxona xavfsizligi bo‘yicha xabardorlik bo‘yicha trening

KnowBe4 asosiy soxta hujum sinovlari, interaktiv treninglar va turli xil hujum shakllarining doimiy simulyatsiyalarini o‘z ichiga olgan keng qamrovli o‘rganish yondashuvini taqdim etadi.

6.7-rasm. Kiberxavfsizlikni o‘qituvchi KnowBe4 kompaniyasi

Treningni boshlashdan oldin, KnowBe4 kompaniyangizda fishing (telefon aloqasi orqali hujumlar, masalan, to‘lov kartasi egasining maxfiy ma’lumotlarini turli bahonalar bilan aldash), smishing (fishing) uchun zaif bo‘lgan foydalanuvchilar sonini baholash uchun asosiy testlarni taqdim etadi.

Kompaniya dunyodagi eng katta xavfsizlik bo‘yicha ta’lim materiallari kutubxonasini, jumladan, interaktiv modullar, videolar, o‘yinlar va axborot byulletenlarini taklif etadi.

KnowBe4 platformasi barcha funktsiyalarni bitta grafik interfeysda birlashtiradi. Trening kampaniyalari bir necha daqiqada hujumlarni boshlaydi va simulyatsiya qiladi va jamoalar minglab shablonlarni o‘z ichiga olgan to‘liq avtomatlashtirilgan fishing, vishing va smishing hujumlari orqali o‘qitiladi. Ushbu andozalar to‘liq moslashtirilgan bo‘lib, vaqt o‘tishi bilan tarqaladigan 4000 dan ortiq realistik fishing elektron pochta xabarlari mavjud.

Trening davomida KnowBe4 korxonaning kuchli va zaif tomonlari haqida hisobotlarni yuboradi. Umumiy va batafsil statistika va grafiklar mavjud va ularni boshqaruv hisobotlariga osongina kiritish mumkin. Ular butun tashkilotning xavfsizlik ko‘rsatkichlari haqida tushuncha beradi.

Nazorat savolari.

1. Tashkilotdagi har bir shaxsning kiberxavfsizlik bo'yicha qanday mas'uliyati bor?
2. Kiberxavfsizlik siyosatida elektron pochtani shifrlashdan foydalanish qoidalari qanday?
3. Parollarni yaratish va himoya qilish bo'yicha qanday ko'rsatmalarga amal qilish kerak?
4. Ijtimoiy tarmoqlardan foydalanishda qanday qoidalarga amal qilishingiz kerak?
5. Zararli dasturlarga qarshi siyosat nima va uning maqsadi nima?
6. Zararli dasturlarga qarshi siyosatda virus va zararli dasturlar hujumlariga qarshi qanday profilaktika va himoya choralari belgilangan?
7. Veb-server nima va u Internet orqali ma'lumot beruvchi ilovalar bilan qanday bog'liq?
8. Veb-serverda xavfsizlikka qanday tahdidlar yuzaga kelishi mumkin va ularni qanday tasniflash mumkin?
9. Veb-serverga ruxsatsiz kirish tashkilot uchun qanday oqibatlarga olib kelishi mumkin?
10. Xizmat ko’rsatishdan voz kechish hujumlari nima va ular veb-server va uning foydalanuvchilariga qanday ta'sir ko'rsatishi mumkin?
11. Veb-serverdagi maxfiy ma'lumotlarni ruxsatsiz shaxslar tomonidan uzatilishi yoki ushlanishidan himoya qilish uchun qanday choralar ko'rish kerak?
12. Qanday qilib veb-serverdan tajovuzkorlar boshqa tashkilotlarning resurslariga kirish yoki ularga hujum qilish uchun foydalanishlari mumkin?
13. Agar veb-server noqonuniy kontent yoki dasturiy ta'minotni tarqatish uchun foydalanilsa, qanday muammolar paydo bo'lishi mumkin?
14. Firewall nima va u veb-server va tarmoq infratuzilmasini himoya qilish uchun qanday vazifalarni bajaradi?

QISQARTMA SO‘ZLAR RO‘YXATI

ISO - International Organization for Standardization
NIST - National Institute of Standards and Technology
IO – Input/Output
LAN - Local area network
CTI - Cyberthreat Intelligence
NCSC - National Cyber Security Centre
CSOC - Cybersecurity Operations Center
CISP - Cyber Security Information Sharing Partnership
SIEM – Security information and event management
CVE - Common Vulnerabilities and Exposures
APT - Advanced Packaging Tool
MISP - Malware Information Sharing Platform
SMT - Simultaneous Multithreading
FIS - foreign intelligence services
OCG - Organized crime groups
CMDB - configuration management database
OSINT - Open source intelligence
GPMS - Global PDI Management System
ARPANET - Advanced Research Projects Agency Network
IETF - Internet Engineering Task Force
IANA - Internet Assigned Numbers Authority
ICANN - Internet Corporation for Assigned Names and Numbers
GLBA - Grahm-Leach-Bliley Act
HIPAA - Health Insurance Portability and Accountability Act
DCF - discounted cash flow
MSTI - milliy standartlar va texnologiyalar institute
MXA - Milliy xavfsizlik agentligi
DBIR - Data Breach Investigation Report
XEI - Xalqaro elektraloqa ittifoqi
EXHT - Yevropa Xavfsizlik va Hamkorlik Tashkiloti
AXBT – Axborot xavfsizligini boshqarisg tizimlari
CTRG - Computer Technology Research Group
KXSIHS - Kiberxavfsizlik siyosatini ishlab chiqish hayotiy sikli
DDOS - Distributed Denial of Service
BYOD - Bring Your Own Device
AI - artificial intelligence
ML - machine learning

IOT - internet of things
DNS - Domain Name System
GUI - graphical user interface

ATAMALARNING IZOHLI LUG‘ATI

Konfidentsiallik – Mazkur qoidalar axborotni faqat qonuniy foydalanuvchilar tomonidan “o’qilishini” ta’minlaydi va tizim ma’lumotlarining tarqalishini ruxsat etilgan foydalanish bilan cheklash qobiliyati tushuniladi.
Yaxlitlik (butunlik) – qayd etilgan va xabar qilingan ma’lumotlarning haqiqiyligi, to‘g‘riligi va manbasini saqlab qolish qobiliyatini anglatadi, ya’ni, axborotni ruxsat etilmagan o’zgartirishdan yoki “yozish” dan himoyalashdir.
Foydalanuvchanlik – funktsional imkoniyatlarni o‘z vaqtida yetkazib berishni anglatgan holda ma’lumotni aniq va ishonchli ekanligiga ishonch hosil qilish, ma’lumot, axborot va tizimdan foydalanishning mumkinligi, ya’ni, ruxsat etilmagan “bajarish” dan himoyalashdir.
Siyosat - so‘zi kiberxavfsizlik bilan bog‘liq bo‘lgan turli vaziyatlarga nisbatan qo‘llaniladi. U axborotni tarqatish, axborotni himoya qilish bo‘yicha xususiy korxona maqsadlari, texnologiyani boshqarish uchun kompyuter operatsiyalari usullari va elektron qurilmalardagi konfiguratsiya o‘zgaruvchilari bilan bog‘liq qonun va qoidalarga murojaat qilish uchun ishlatiladi.
Port skanerlari - tizimdagi ochiq portlarni aniqlaydi. Bu testerlarga ular kirishga harakat qilayotgan tarmoqda ishlayotgan operatsion tizim va ilovalarni aniqlashga yordam beradi. Port skanerlari razvedkada qo‘llaniladi va potentsial hujum vektorlari uchun g‘oyalarni taqdim etishi mumkin.
Zaiflik skanerlari - serverlar, operatsion tizimlar va ilovalardagi ma’lum zaifliklarni, shuningdek sinovda ishlatilishi mumkin bo‘lgan noto‘g‘ri konfiguratsiyalarni qidiradi. Zaiflik skanerlari tomonidan taqdim etilgan hisobotlar penetratsion sinovchilarga tizimga dastlabki kirish huquqini beruvchi foydalaniladigan zaiflikni tanlashda yordam beradi.
Tarmoq sniffer - tarmoq trafigidagi ma’lumotlarni, shu jumladan uning manbasini, manzilini, tarmoqda aloqa qiladigan qurilmalarni, ishlatiladigan protokollar va portlarni kuzatib boradi. Bu ma’lumotlar shifrlangan yoki yo‘qligini tekshirish va penetratsiya testi paytida foydalanish mumkin bo‘lgan aloqa yo‘llarini aniqlash uchun foydali

bo‘lishi mumkin.

Veb-proksi - penetratsion testerlarga o‘z brauzeri va tashkilot veb-serverlari o‘rtasidagi trafikni ushlab turish va o‘zgartirish imkonini beradi. Bu saytlararo skript (XSS) yoki saytlararo so‘rovlarni soxtalashtirish (CSRF) kabi hujumlarni faollashtirishi mumkin bo‘lgan yashirin shakl maydonlarini va boshqa HTML xususiyatlarini aniqlash imkonini beradi.

Parolni buzish - parolni xeshlash maqsadli tizim yoki tarmoqdagi imtiyozlarni oshirish vositasi sifatida tajovuzkorlar uchun umumiy maqsaddir. Parolni buzish vositalari penetratsion testerlarga tashkilot xodimlariga xavf tug‘diradigan zaif parollardan foydalanayotganligini aniqlash imkonini beradi.

Kali Linux - bu kirish testini, xavfsizlikni tekshirishni va tegishli faoliyatni osonlashtiradigan operatsion tizim. Bu ochiq manba sifatida taqdim etilgan va Offensive Security tomonidan qo‘llab-quvvatlanadigan Debian-ga asoslangan Linux distributividir.

Foydalanilgan adabiyotlar:

1. Cyber security policy guidebook. Jennifer L. Bayuk. Jason Healey. Paul Rohmeyer, et.c. Willey publisher.2018-y. 288 p. ISBN 978-1-118-02780-6.
2. Cybersecurity Curricula 2017 – Curriculum Guidelines for Post-Secondary Degree Programs in Cybersecurity (ACM, IEEE-CS, AIS SIGSEC, IFIP WG 11.8) (Crosscutting concepts).
3. Ғаниев С.К., Каримов М.М., Ташев К.А., “Ахборот хавфсизлиги”, “Фан ва технологиялар” нашриёти, Тошкент 2016.
4. Abend, V., et al. (2008). Cybersecurity for the banking and finance sector.
5. ISO/IEC 27000 Information technology. Security techniques. Information security management systems. Overview and vocabulary.
6. Шангин В.Ф., «Комплексная защита информации в корпоративных системах», Учебное пособие. М.: ИД. «ФОРУМ» - ИНФРА М. 2019, 591с.
7. Mark Stamp. Information security. Principles and Practice. Second edition. A John Wiley& Sons, Inc., publication. Printed in the United States of America. 2011y. 584p

8. CISSP Official Study Guide (Mike Chapple, James Michael Stewart, Darril Gibson) (2018, Sybex).
9. Mark Ciampa. Security+.Guide to Network Security Fundamentals. Fifth Edition. Printed in the United States of America Print Number: 01 Print Year: 2014
10. Tim Boyles. CCNA Security Study Guide. Copyright © 2010 by Wiley Publishing, Inc., Indianapolis, Indiana. Published simultaneously in Canada ISBN: 978-0-470-52767-2.
11. Joseph Migga Kizza. Computer Network Security and Cyber Ethics. Fourth edition. McFarland & Company, Inc., Publishers Jefferson, North Carolina © 2014.
12. ANSI and ISA (2010). The financial management of cyber risk. An Implementation Framework for CFOs, American National Standards Institute (ANSI) and the Internet Security Alliance (ISA).In Wiley Handbook of Science and Technology for Homeland Security, ed. J. G. Voeller. Hoboken, NJ: John Wiley & Sons, Inc.
13. Bayuk, J. (2010). Enterprise Security for the Executive: Setting the Tone at the Top. Santa Barbara, CA: Praeger.
14. Hubbard, D. W. (2009). The Failure of Risk Management. Hoboken, NJ: John Wiley & Sons, Inc., p. 6.
15. Markoff, J. (2012). Researchers find a flaw in a widely used online encryption method. The New York Times, February 15.
16. NCSC / Cabinet Office. *Minimum Cyber Security Standard.* London : publishing.service.gov.uk, 2018. Version 0.1.
17. MITRE. MITRE Cyber Attack Lifecycle. *MITRE.* [Online] attack.mitre.org/resources/enterpriseintroduction.
18. Gartner. Market Guide for Security Threat Intelligence Products and Services. *Gartner.* [Online] https://www.gartner.com/doc.3765965/market-guide-security-threat-intelligence.
19. FireEye. Threat Intelligence Use Case Series. *FireEye.* [Online]
https://www.fireeye.com/content/dam/fireeye-www/products/pdfs/pf/intel/sb-incident-responderprofile.pdf
20. Recorded Future. Threat Intelligence Use Cases. *Recorded Future.* [Online]
https://www.recordedfuture.com/threat-intelligence-use-cases.
21. OASIS. Introduction to STIX. *OASIS Open Github.* [Online] https://oasis-open.github.io/ctidocumentation/stix/intro.

22. Lockheed Martin. The Cyber Kill Chain. *Lockheed Martin.* [Online] [Cited: 27 09 2018.] https://www.lockheedmartin.com/en-us/capabilities/cyber/cyber-kill-chain.html.

23. BAE Systems. *Intelligence Led Threat Mitigation.* s.l. : BAE Systems, 2017.

24. Caltagirone, Sergio, Pendergast, Andrew and Betz, Christopher. *The Diamond Model Of Intrusion Analysis.* s.l. : Active Response, 2013.