KIBERXAVFSIZLIK SIYOSATI HAQIDA UMUMIY MA’LUMOTLAR

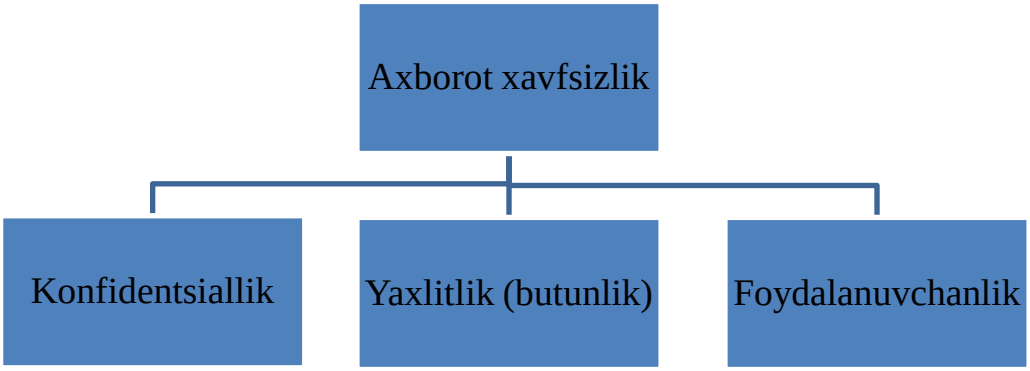
https://doi.org/10.5281/zenodo.7854358

Radjabova Madina Shavkatovna
Toshkent axborot texnologiyalari unversitetining “Kiberxavfsizlik va kriminalistika ” kafedrasi o’qituvchi-stajyor
Ikromov Nurmuhammad Ilhomjon o’g’li
Hafizov Shukurullo Fayzullo o’g’li
Mirzanazarov Mehridil Shamsiddin o'g'li
Kiberxavfsizlik fakulteti talabalari

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 (Safire 1994).[1.]

Tizimlar o‘z vazifalarini bajarishi uchun 3 ta operator belgilangan tartiblarga rioya qilishlari kerak. Xavfsizlikka tatbiq etilganda, bu triada 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 xavfsizlik

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.

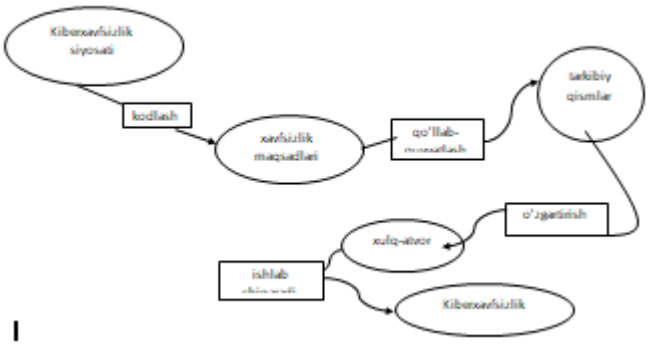
Foydalanuvchanlik – funktsional imkoniyatlarni o‘z vaqtida yetkazib berishni anglatgan holda ma’lumotni aniq va ishonchli ekanligiga ishonch hosil qilish, ma’lumot, axborot va tizimdan foydalanishning mumkinligi, ya’ni, ruxsat etilmagan “bajarish” dan himoyalashdir.

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), foydalanuvchanliligа yetkazilgan zararning oldini olish, aniqlash va tiklash uchun odamlar, jarayonlar va texnologiyalardan foydalanish usullarini anglatadi.

“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

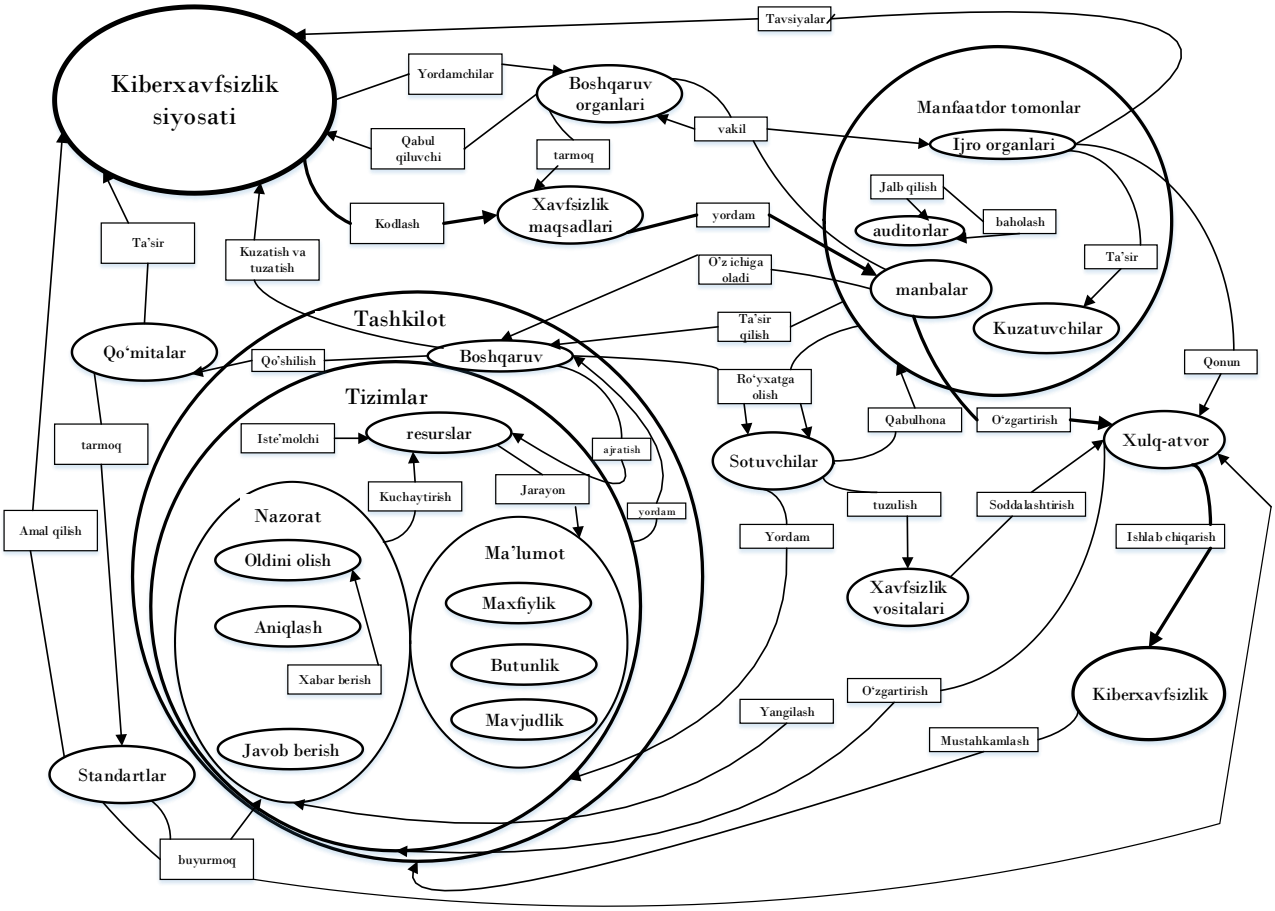
siyosati iborasini ishlatishning ko‘plab boshqa usullari mavjud. "Kibermakon" atamasida bo‘lgani kabi, yagona ta’rif mavjud emas, lekin kiberxavfsizlik atamasi siyosat sifatida qo‘llanilganda umumiy mavzu sifatida qo‘llaniladi.



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 (Bishop 2010). 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) (ISO/IEC 2005 a,b) va NIST (Ross, Katzke va boshq. 2007) 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.[3.]

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.

FOYDALANILGAN ADABIYOTLAR:

- Cyber Security Policy Guidebook

Jennifer L.

Bayuk Independent Cyber Security Governance Consultant Industry Professor at Stevens Institute of Technology, Hoboken,

NJ Jason Healey Director of the Cyber Statecraft Initiative Atlantic Council of the United States, Washington,

D.C. Paul Rohmeyer Information Systems Program Director Howe School of Technology Management Stevens Institute of Technology, Hoboken,

NJ Marcus H. Sachs

Vice President for National Security Policy Verizon Communications, Washington,

D.C. Jeffrey

Schmidt Chief Executive Officer JAS Communications LLC, Chicago, IL

Joseph Weiss

Professional Engineer Applied Control Solutions, LLC, Cupertino, CA

- İnfowatch .ru/analytics
- **Cyber Threat Intelligence in Government: A Guide for Decision Makers & Analysts**