“Involta” Ilmiy Jurnali

Vebsayt: https://involta.uz/

AXBOROT XAVFSIZLIGI XAVFLARINI BAHOLASH UCHUN FOYDALANILADIGAN VOSITALARNI TAHLIL QILISH

Sh.Yu. Djabbarov

R.X. Djurayev

O.A. Xasanov

Annotatsiya: Ushbu maqolada axborot xavfsizligi xavflarini baholashga yondashuvlar muhokama qilingan. Zamonaviy vositalarning (CRAMM, RiskWatch, GRIF, AvanGard) qiyosiy tahlili o‘tkazilgan. Ularning afzalliklari va kamchiliklari keltirilgan.

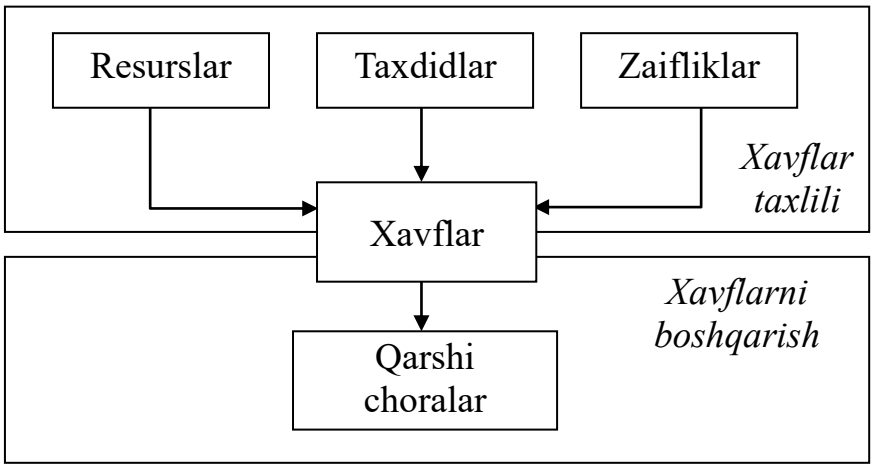
Kalit so‘zlar: axborot xavfsizligi, tahdid, zaiflik, xavf (risk), xavf tahlili, instrumental vosita.

Axborot xavfsizligi (AX) xavf (risk)larini baholash muammolarini hal qilish, axborot xavflarini tahlil va nazorat qilish uchun Britaniyaning CRAMM (Insight Consulting kompaniyasi), Amerikaning RiskWatch (RiskWatch kompaniyasi), Rossiyaning GRIF (Digital Security kompaniyasi) va Avangard (Rossiya Fanlar akademiyasining tizimli tahlil instituti) kompaniyalari tomonlaridan dasturiy vositalar ishlab chiqilgan. Kompaniyalar tomonidan

yaratilgan vositalar va ular asosida qurilgan dasturiy ta’minot tizimlarini ko‘rib chiqamiz.

CRAMM - Britaniya hukumati buyrug‘i bilan “BIS Applied Systems Limited” tomonidan ishlab chiqilgan xuddi shu nomdagi usulni amalga oshiruvchi vositadir. CRAMM usuli axborot tizimini tekshirish, BS 7799 talablariga muvofiq audit o‘tkazish, xavfsizlik siyosatini ishlab chiqish, xavflarni tahlil qilish va bir qator boshqa audit vazifalarini hal qilish imkonini beradi.

CRAMM usuli tahlilning miqdoriy va sifat usullarini birlashtirgan holda xavfni baholashga kompleks yondashuvga asoslanadi [1]. Usul universal bo‘lib, ham davlat, ham tijorat sektoridagi yirik va kichik tashkilotlar uchun javob beradi. Turli turdagi tashkilotlarga mo‘ljallangan CRAMM dasturiy ta’minotining versiyalari bilim bazalari (profillari) bo‘yicha bir-biridan farq qiladi: tijorat tashkilotlari uchun Commercial Profile va davlat tashkilotlari uchun Government profile mavjud. CRAMM so‘rovini o‘tkazish uchun kontseptual asos 1.1-rasmda keltirilgan.



1.1-rasm. CRAMM usuli yo‘rdamida tekshirish o‘tkazish sxemasi

CRAMM-dan to‘g‘ri foydalanish bilan juda yaxshi natijalarga erishish mumkin, ulardan eng muhimi, AX va biznesning uzluksizligini ta’minlash uchun tashkilot xarajatlarini iqtisodiy asoslash imkoniyatidir. Iqtisodiy asosli xavflarni boshqarish siyosati, keraksiz xarajatlardan qochish, pulni tejash imkonini beradi.

CRAMM butun protsedurani uchta ketma-ket bosqichga bo‘lishni o‘z ichiga

oladi. Birinchi bosqichning vazifasi tizimni himoya qilish uchun an’anaviy xavfsizlik funktsiyalarini amalga oshiradigan asosiy darajadagi vositalardan foydalanishning etarliligini yoki batafsilroq tahlil qilish zarurligini aniqlashdir. Ikkinchi bosqichda xavflar identifikatsiya qilinadi va ularning qiymati baholanadi. Uchinchi bosqichda tegishli qarshi choralarni tanlash masalasi hal qilinadi.

Har bir bosqich uchun CRAMM metodologiyasi dastlabki ma’lumotlar to‘plamini, harakatlar ketma-ketligini, suhbatlar uchun so‘rovnomalarni, nazorat ro‘yxatlarini va hisobot hujjatlari to‘plamini belgilaydi.

Tadqiqotning birinchi bosqichida muhofaza qilinadigan resurslarning qiymatini aniqlash va identifikatsiya amalga oshiriladi. Baholash o‘n balli shkala bo‘yicha amalga oshiriladi va bir nechta baholash mezonlari bo‘lishi mumkin - moliyaviy yo‘qotishlar, obro‘ga putur etkazish va boshqalar. CRAMM tavsiflari “Resurslarni tiklash bilan bog‘liq moliyaviy yo‘qotishlar” mezoni bo‘yicha quyidagi reyting shkalasiga misol keltiradi:

- 2 ball - 1000 $ - dan kam;
- 6 ball - 1000 $ - dan 10 000 $ - gacha;
- 8 ball - 10 000 $ - dan 100 000 $ - gacha;
- 10 ball - 100 000 $ - dan yuqori.

Amaldagi barcha mezonlar (3 ball va undan past) uchun past ball bilan ko‘rib chiqilayotgan tizim uchun himoyaning asosiy darajasi etarli deb hisoblanadi (bu daraja AX tahdidlarini batafsil baholashni talab qilmaydi), ikkinchisi o‘rganish bosqichi o‘tkazib yuboriladi.

Ikkinchi bosqichda AX sohasidagi tahdidlar identifikatsiyalanadi va baholanadi, himoyalangan tizimning zaif tomonlarini qidirish va baholash amalga oshiriladi. Tahdid darajasi quyidagi shkala bo‘yicha baholanadi: juda yuqori, yuqori, o‘rta, past, juda past. Zaifliklar darajalari yuqori, o‘rta yoki past deb baholanadi. Ushbu ma’lumotlarga asoslanib, etti ballik shkala bo‘yicha xavf darajasini baholash hisoblanadi.

Uchinchi bosqichda CRAMM aniqlangan xavflarga qarshi kurashish

variantlarini ishlab chiqadi. CRAMM quyidagi turdagi tavsiyalarni taqdim etadi:

- umumiy xarakterdagi tavsiyalar;
- aniq tavsiyalar;
- bunday vaziyatda himoyani qanday tashkil qilish mumkin.

CRAMM keng qamrovli ma'lumotlar bazasiga ega, unda turli xil kompyuter tizimlarining himoya quyi tizimlarini amalga oshirishning 1000 ga yaqin misollar tavsifi mavjud. Ushbu tavsiflardan shablon sifatida foydalanish mumkin.

Tizimga yangi xavfsizlik mexanizmlarini joriy etish va eskilarini o'zgartirish to'g'risidagi qaror tashkilot rahbariyati tomonidan tegishli xarajatlar, ularning maqbulligi va biznesning yakuniy foydasini hisobga olgan holda qabul qilinadi. Auditorning vazifasi tashkilot rahbariyatiga tavsiya etilgan chiralarni asoslab berishdan iborat.

Agar yangi qarshi choralarni joriy etish va eskilarini o'zgartirish to'g'risida qaror qabul qilinsa, auditorga amalga oshirish rejasini tayyorlash va ushbu choralarning samaradorligini baholash topshirilishi mumkin. Ushbu muammolarni hal qilish CRAMMdan tashqariga chiqadi.

CRAMMning kuchli tomonlari quyidagilardan iborat:

- CRAMM yaxshi tuzilgan va keng miqyosda sinovdan o'tgan xavflarni tahlil qilish vositasi bo'lib, haqiqiy amaliy natijalarni olish imkonini beradi;
- CRAMM vositasidan axborot tizimi xavfsizligi auditining barcha bosqichlarida foydalanish mumkin;
- dasturiy mahsulot BS 7799 standarti tavsiyalari asosida AX sohasidagi qarshi choralar bo'yicha yetarlicha hajmli bilimlar bazasiga asoslangan;
- CRAMM usulining moslashuvchanligi va ko'p qirraliligi uni har qanday murakkablik va maqsadli darajadagi axborot tizimini tekshirish uchun ishlatishga imkon beradi;
- CRAMM biznesning uzluksizligi rejasini va tashkilotning AX siyosatini ishlab chiqish vositasi sifatida ishlatilishi mumkin;
- CRAMMdan axborot tizimining xavfsizlik mexanizmlarini hujjatlashtirish

vositasi sifatida foydalanish mumkin.

CRAMM vositasining kamchiliklariga quyidagilarni keltirish mumkin:

- vosita auditorning maxsus tayyorgarligi va yuqori malakasini talab qiladi;

- CRAMM auditi - jarayon ancha mashaqqatli va auditorning bir necha oylik uzluksiz ishlashini talab qilishi mumkin;

- CRAMM ishlab chiqilayotgan axborot tizimidan ko‘ra foydalanishga topshirilgan mavjud axborot tizimlarini tekshirish uchun ko‘proq mos keladi;

- CRAMM vositasi amalda har doim ham foydali bo‘lmagan katta hajmdagi qog‘oz hujjatlarini yaratadi;

- CRAMM shaxsiy hisobot shablonlarini yaratishga yoki mavjudlarini o‘zgartirishga ruxsat bermaydi;

- CRAMM ma’lumotlar bazasiga qo‘shimchalar kiritish imkoniyati foydalanuvchilar uchun mavjud emas, bu esa ushbu usulni muayyan tashkilot ehtiyojlariga moslashtirishda ma’lum qiyinchiliklarni keltirib chiqaradi.

RiskWatch usuli - bu xavflarni tahlil qilish va boshqarish uchun kuchli vositadir [2]. RiskWatch oilasiga turli xil xavfsizlik auditlari va xavf tahlillari uchun dasturiy mahsulotlar kiradi, xususan:

- axborot tizimini himoya qilishning fizik usullari uchun;

- axborot tizimlari uchun RiskWatch;

- HIPAA standarti talablariga muvofiqligini baholash (AQSh sog‘liqni saqlash sug‘urtasi portativligi va javobgarlik to‘g‘risidagi qonun);

- ISO 17799 uchun RiskWatch RW17799.

CRAMMdan farqli o‘laroq, RiskWatch ko‘proq xavfsizlik tahdidi yo‘qotishlari va mudofaa xarajatlari o‘rtasidagi munosabatni aniq aniqlashga qaratilgan. Shuni ham ta’kidlash kerakki, ushbu usulda korxona kompyuter tarmog‘ining axborot va fizik xavfsizlik sohasidagi xavflar birgalikda ko‘rib chiqiladi.

RiskWatchda qo‘llaniladigan texnika to‘rt bosqichni o‘z ichiga oladi [3]:

- *birinchi bosqich* - tadqiqot predmetini aniqlash. Ushbu bosqichda

tashkilotning parametrlari tavsiflanadi: tashkilot turi, o‘rganilayotgan tizimning tarkibi, asosiy xavfsizlik talablari. Ta’rif bir qator kichik bandlarda rasmiylashtiriladi, ularni batafsilroq tavsiflash yoki o‘tkazib yuborish uchun tanlash mumkin. Tanlangan elementlarning har biri quyida batafsil tavsiflanadi. Tahlilchi ishini osonlashtirish uchun shablonlarda himoyalangan resurslar, yo‘qotishlar, tahdidlar, zaifliklar va himoya choralari resurslari ro‘yxati keltiriladi. Ulardan tashkilotda haqiqatda mavjud bo‘lganlarini tanlash kerak.

- *ikkinchi bosqich* - tizimning o‘ziga xos xususiyatlarini tavsiflovchi ma’lumotlarni kiritish. Ma’lumotlar qo‘lda kiritilishi yoki kompyuter tarmog‘idagi zaifliklarni o‘rganish vositalari tomonidan yaratilgan hisobotlardan import qilinishi mumkin. Ushbu bosqichda:

a) resurslar, yo‘qotishlar va hodisalar sinflari batafsil tavsiflangan. Hodisa sinflari yo‘qotish toifasi va resurs toifasini moslashtirish orqali olinadi;

b) zaifliklarni aniqlash uchun ma’lumotlar bazasi 600 dan ortiq savollarni o‘z ichiga olgan so‘rovnomadan foydalaniladi. Savollar manba resurslari bilan bog‘liq. Savollarni to‘g‘irlash, o‘chirish yoki yangilarini qo‘shishga ruxsat beriladi;

v) tanlangan tahdidlarning har birining paydo bo‘lish chastotasi, zaiflik darajasi va resurslarning qiymati belgilanadi. Bularning barchasi kelajakda AX vositalarini joriy etish samaradorligini hisoblash uchun ishlatiladi.

- *uchinchi bosqich* - xavfni baholash. Birinchidan, oldingi bosqichlarda aniqlangan resurslar, yo‘qotishlar, tahdidlar va zaifliklar o‘rtasida aloqalar o‘rnatiladi. Xavf, bir yil uchun yo‘qotishlarning matematik kutilma yordamida baholanadi:

$$m = p * v, \qquad (1)$$

bu erda: p - yil davomida tahdidning paydo bo‘lish chastotasi;

v - xavf ostida bo‘lgan resursning narxi.

Biroq, RiskWatch LAFE va SAFE [2] deb nomlangan Amerika NIST standartlari instituti tomonidan belgilangan hisob-kitoblardan foydalanganligi

sababli (1) formula ba'zi o'zgarishlarga duch keldi. LAFE (Local Annual Frequency Estimate - Mahalliy yillik chastota smetasi) - bu tahdid ma'lum bir joyda (masalan, shaharda) yiliga o'rtacha necha marta amalga oshirilishini ko'rsatadi. SAFE (Standard Annual Frequency Estimate - Standart yillik chastota smetasi) - bu "dunyoning bir qismida" (masalan, Shimoliy Amerikada) ma'lum bir tahdid yiliga o'rtacha necha marta amalga oshirilishini ko'rsatadi. Tahdidni amalga oshirish natijasida himoyalangan resurs to'liq yo'q qilinishi mumkin emas, balki qisman bo'lishi mumkinligini hisobga olish imkonini beradigan tuzatish omili ham joriy etilgan. Bundan tashqari, agar himoya choralari mavjud bo'lsa, shunga o'xshash vaziyatlarni tasvirlashga imkon beradigan "agar bo'lsa ..." stsenariylari ko'rib chiqiladi. Himoya choralari amalga oshirilgan taqdirda, ularsiz kutilayotgan yo'qotishlarni taqqoslash orqali bunday choralarning samarasini baholash mumkin.

RiskWatch LAFE va SAFE reytinglariga ega ma'lumotlar bazalarini, shuningdek, har xil turdagi himoya vositalarining umumlashtirilgan tavsiflarini o'z ichiga oladi.

Xavfsizlik choralarini amalga oshirishning ta'siri ROI (Return on Investment - investitsiyalarning daromadliligi) ko'rsatkichi yordamida miqdoriy jihatdan tavsiflanadi, bu formula bo'yicha hisoblangan ma'lum vaqt davomida kiritilgan investitsiyalar daromadliligini ko'rsatadi:

$$ROI = \sum_i NVP(Benefits_i) - \sum_i NVP(Costs_i) \qquad (2)$$

bu erda: $Costs_i$ - *i*-himoya chorasini amalga oshirish va saqlash xarajatlari;

$Benefits_i$ - berilgan himoya chorasini amalga oshirishning afzalliklarini baholash (ya'ni kutilayotgan yo'qotishlarni kamaytirish) ;

NPV (Net Present Value- Hozirgi sof qiymat) - inflyatsiyani moslashtiradi.

- *to'rtinchi bosqich* - hisobotlarni yaratish [3]. RiskWatchda quyidagi turdagi hisobotlar yaratiladi:

a) qisqacha xulosa;

b) 1 va 2-bosqichlarda tavsiflangan elementlarning to'liq va qisqacha hisobotlari;

c) himoyalangan resurslarning qiymati va tahdidlarni amalga oshirishdan kutilayotgan yo‘qotishlar to‘g‘risidagi hisobot;

d) tahdidlar va ularga qarshi choralar to‘g‘risida hisobot;

e) xavfsizlik auditi natijalari to‘g‘risidagi hisobot.

RiskWatch xususiyatlari. RiskWatch axborot tizimi modeli tavsifiga, xavfni baholashga va soddalashtirilgan yondashuvdan foydalanadi. Ushbu usul yordamida xavflarni tahlil qilish bo‘yicha ishlarning murakkabligi nisbatan kichik. Bunday vosita, agar tashkiliy va ma’muriy omillarni hisobga olmasdan, dasturiy va apparat himoyasi darajasida xavf tahlilini o‘tkazish kerak bo‘lsa, mos keladi. Shuni yodda tutish kerakki, olingan xavflarni baholash (yo‘qotishlarni matematik kutilmasi) hech qanday holatda tizim nuqtai nazardan xavf tushunchasini tugatmaydi. RiskWatchning turli xil iste’molchilar nuqtai nazaridan muhim afzalligi uning qiyosiy soddaligi, ruslashtirishning kam mehnat sarflanishi va yangi toifalarning kiritilishi, tavsiflar, savollar va boshqalarni kiritish imkoniyati bilan ta’minlangan usulning katta moslashuvchanligi va b.

GRIF usuli - bu tashkilotning axborot tizimidagi xavflarni boshqarish va tahlil qilish vositasidir. GRIF vositasi axborot oqimlari modelini tahlil qilish orqali axborot tizimining xatarlarini tahlil qilish, shuningdek, foydalanuvchi chiqishi bilan qiziqadi, foydalanuvchi qanday dastlabki ma’lumotlarga ega ekanligiga qarab tahdidlar va zaifliklar modelini tahlil qilish imkonini beradi [2].

Axborot oqimlari modeli. Axborot oqimlari modeli bilan ishlashda qimmatli ma’lumotlarga ega bo‘lgan barcha resurslar to‘g‘risidagi to‘liq ma’lumotlar, ushbu resurslarga kirish huquqiga ega bo‘lgan foydalanuvchilar tizimga kiritiladi. U har bir resurs uchun barcha himoyalarni, resurslarning tarmoq munosabatlarini va tashkilotning xavfsizlik siyosatining xususiyatlarini qayd etadi. Natijada axborot tizimining to‘liq modeli paydo bo‘ladi.

GRIF bilan ishlashning birinchi bosqichida foydalanuvchi o‘zining axborot tizimining barcha ob’ektlariga kiradi: bo‘limlar, resurslar (ushbu modelning o‘ziga xos ob’ektlari tarmoq guruhlari, tarmoq qurilmalari, ma’lumotlar turlari,

foydalanuvchilar guruhlari).

Keyinchalik, foydalanuvchi resurslar qaysi bo‘limlar va tarmoq guruhlariga tegishli ekanligini, resursda qanday ma’lumotlar saqlanganligini va qaysi foydalanuvchilar guruhlariga kirish huquqini aniqlash va ulanishlarni amalga oshirishi kerak.

Yakuniy bosqichda foydalanuvchi tizimda amalga oshirilgan xavfsizlik siyosati bo‘yicha ro‘yxatdagi savollarga javob beradi, bu tizim xavfsizligining haqiqiy darajasini baholash va xavflarni batafsil tekshirib baholash imkonini beradi.

Birinchi bosqichda qayd etilgan axborotni himoya qilish vositalarining mavjudligi, agar ular noto‘g‘ri qo‘llanilsa va axborotni himoya qilishning barcha jihatlarini, himoya qilish, fizik xavfsizlik, xodimlar xavfsizligi va boshqalar, shu jumladan axborotni himoya qilishni tashkil qilishni hisobga oladigan keng qamrovli xavfsizlik siyosati mavjud bo‘lmagan taqdirda tizimni xavfsiz qilmaydi.

Yuqoridagi bosqichlarning barcha harakatlarini bajarish natijasida chiqishda davom etish imkonini beruvchi kompleks xavfsizlik siyosati talablarining amalda bajarilishini hisobga olgan holda xavflarni har tomonlama baholash va yakuniy hisobotni yaratish uchun kiritilgan ma’lumotlarni dasturiy tahlil qilish AX nuqtai nazaridan axborot tizimining to‘liq modeli hosil bo‘ladi.

Tahdid va zaiflik modeli. Tahdid va zaiflikni tahlil qilish modeli bilan ishlash qimmatli ma’lumotlarga ega har bir resursning zaif tomonlarini va ushbu zaifliklar orqali amalga oshirilishi mumkin bo‘lgan tegishli tahdidlarni aniqlashni o‘z ichiga oladi. Natijada axborot tizimidagi zaifliklar va yetkazilishi mumkin bo‘lgan zararlar haqida to‘liq tasavvur hosil bo‘ladi.

Ushbu usul bilan ishlashning birinchi bosqichida foydalanuvchi o‘z axborot tizimining ob’ektlariga kiradi: bo‘limlar, resurslar (ushbu model uchun o‘ziga xos ob’ektlar axborot tizimiga tahdidlar, tahdidlar amalga oshiriladigan zaifliklar).

GRIF keng qamrovli o‘rnatilgan tahdidlar va zaifliklarni o‘z ichiga oladi. Ushbu kataloglarning maksimal to‘liqligi va ko‘p qirraliligiga erishish uchun

Digital Security mutaxassislari AX sohasida ko‘p yillik amaliy tajribani amalga oshiradigan DSECCT (Digital Security Classification of Threats - Tahdidlarning raqamli xavfsizlik tasnifi)ni ishlab chiqdilar [4]. Tahdidlar va zaifliklar kataloglaridan foydalanib, foydalanuvchi o‘z axborot tizimiga tegishli tahdidlar va zaifliklarni tanlashi mumkin. Kataloglarda 100 ga yaqin tahdid va 200 ta zaifliklar mavjud.

Keyinchalik, foydalanuvchi aloqani amalga oshirishi kerak, ya’ni resurslar qaysi bo‘limlarga tegishli ekanligini, resursga qanday tahdidlar ta’sir qilishini va qanday zaifliklar orqali amalga oshirilishini aniqlash.

GRIF algoritmi qurilgan modelni tahlil qiladi va har bir resurs uchun xavf qiymatlarini o‘z ichiga olgan hisobotni yaratadi. Hisobotning konfiguratsiyasi deyarli har qanday bo‘lishi mumkin, shunday qilib, foydalanuvchi boshqaruv uchun umumiy hisobotlarni va natijalar bilan keyinchalik ishlash uchun batafsil hisobotlarni yaratish imkoniyatiga ega.

GRIF instrumental vositasi xavflarni boshqarish modulini o‘z ichiga oladi, bu kiritilgan ma’lumotlarni algoritm bo‘yicha qayta ishlagandan keyin olingan xavf qiymatining barcha sabablarini tahlil qilish imkonini beradi. Shunday qilib, sabablarni bilgan holda, tashkilot qarshi choralarni amalga oshirish va shunga mos ravishda xavf darajasini pasaytirish uchun zarur bo‘lgan barcha ma’lumotlarga ega bo‘ladi. Har bir mumkin bo‘lgan qarshi chora samaradorligini hisoblash, shuningdek, qoldiq xavfning qiymatini aniqlash orqali tashkilot xavfni eng kam xarajat bilan kerakli darajaga kamaytiradigan eng maqbul qarshi choralarni tanlashi mumkin.

GRIF bilan ishlash natijasida tashkilotning axborot tizimining har bir qimmatli manbasining xavf darajasi, zaifliklarni batafsil tahlil qilish va barcha mumkin bo‘lgan qarshi choralarning iqtisodiy samaradorligini baholash bilan xavfning barcha sabablari to‘g‘risida batafsil hisobot tuziladi.

AvanGard - AXni boshqarishning instrumental vositasi. Oddiy AvanGard to‘plami ikkita vositani o‘z ichiga oladi: AvanGard - Tahlil va AvanGard - Nazorat,

ularning har biri o‘zining xavflarni baholash metodologiyasiga asoslanadi [3].

Birinchisi, baholanadigan tizim tarkibiy qismlarining xavfni shakllantirish potentsialini hisoblash asosida xavfni baholashni o‘z ichiga oladi. Bunday holda, xavfni shakllantirish potentsiali tizim bilan bog‘liq bo‘lgan umumiy xavfning ushbu komponentga tegishli bo‘lishi mumkin bo‘lgan qismi sifatida tushuniladi.

Xavflarni yuzaga keltiruvchi potentsiallarni hisoblashda, birinchi navbatda, ushbu hodisalarning iloji boricha norasmiy tavsifi va ularga olib kelishi mumkin bo‘lgan tahdidlar ro‘yxatini o‘z ichiga olgan xavf hodisalari modellari tuziladi. Bundan tashqari, xavf hodisasi ehtimolini baholash va xavf hodisasi xavflilik darajasini baholash mahsuli sifatida xavf hodisasining har bir modeli uchun xavfni baholash hisoblanadi. Shu bilan birga, daraja shkalasidan foydalangan holda xavf hodisalari ehtimoli va ushbu hodisalarning xavflilik darajasi bo‘yicha taxminlarni olish taklif etiladi. Ehtimollar shkalasi 0 dan 100 gacha (xavf hodisasi ehtimoli noldan 100 % gacha) qat’iy belgilangan o‘lchamga ega.

Xavf shkalasining pastki chegarasi 0 ga teng, yuqori chegarasi yo‘q, shuning uchun shkala quyidagi printsip bo‘yicha qurilgan. Bu xavflar birinchi navbatda unga nisbatan qo‘llaniladi, uning butun xavfi moddiy zararga kamayadi va pul birliklarida ifodalanishi mumkin. Natijada xavf hodisalari uchun asosiy xavf shkalasi xosil bo‘ladi. Bundan tashqari, foydalanuvchilarga “pul” ko‘rsatkichidan abstrakt qilish, shkalani faqat individual hodisalarning nisbiy xavflilik darajasini ifodalovchi sifatida qabul qilish va ulardagi nomaqbullik yoki yo‘l qo‘ymaslik darajasini solishtirish orqali xavf hodisalarini ko‘rsatish taklif etiladi. Bunday holda, o‘lchovning yuqori chegarasi kerak bo‘lganda ko‘tarilishi mumkin.

Metodologiya shuni ko‘rsatadiki, har qanday xavf hodisasi ma’lum bir tahdidlar to‘plamini amalga oshirish natijasida yuzaga keladi va ularning har biri baholanayotgan tizimning biron bir tarkibiy qismining xavfsizligiga tahdid sifatida belgilanishi mumkin. Shunday qilib, har bir tahdidning xavf-xatarni yuzaga keltiruvchi potentsialini, uning xavf hodisasiga qo‘shgan hissasiga, shuningdek, baholangan tizimning barcha tarkibiy qismlari va umuman tizim uchun xavflar

ushbu tahdidlar tegishli bo‘lgan tarkibiy qismlarning xavf-xatarni shakllantirish potentsialiga qarab aniqlash mumkin.

“AvanGard-Tahlil” vositasi AXni boshqarish vazifalarini hal qilishda yordamchi rol o‘ynash uchun mo‘ljallangan, xususan: xavfsizlik maqsadlari to‘plamini ifodalash, xavfsizlik siyosatini asoslash va xavfsizlikning to‘liqligini kafolatlash imkonini beruvchi to‘liq keng qamrovli tahlilni ta’minlash, bajarilishini nazorat qilish kerak bo‘lgan talablar. Shunga ko‘ra, ushbu muammolarni hal qilish uchun unda xavfni baholash amalga oshiriladi.

“AvanGard-Nazorat” xavflarni baholash metodologiyasi avtomatlashtirilgan axborot tizimining xavfsizlik darajasini monitoring qilish vazifasiga bo‘ysunadi va shuning uchun “AvanGard-Tahlil” metodologiyasidan farq qiladi. Agar “AvanGard-Tahlil” usuli baholangan tizimning mumkin bo‘lgan xavfsizlik buzilishi xavfini nazarda tutsa, “AvanGard-Nazorat” vositasining metodologiyasi baholangan tizimning xavfsizlik talablariga rioya qilmaslik natijasida yuzaga keladigan xavflarga va uning tarkibiy qismlariga bag‘ishlangan. Shu sababli, “AvanGard-Nazorat”dan foydalanish uchun baholangan tizimning har bir komponenti talablarning to‘liq to‘plamiga ega bo‘lishi kerak, ularning bajarilishi tizim xavfsizligini buzish xavfi nolga teng. Shu bilan birga, agar barcha talablar bajarilmasa, tizim xavfsizligini buzish xavfi 100% bo‘ladi deb taxmin qilinadi.

Axborot xavflarini tahlil qilish, albatta, eng qiyin amaliy vazifadir. Uni amalga oshirishga yondashuvlar juda boshqacha bo‘lishi mumkin: juda oddiy, ammo qulay va kuchli “xavf kalkulyatorlari” dan (RiskWatch) juda murakkab vositalargacha (CRAMM). CRAMM, xuddi RiskWatch kabi, tahdidlarning o‘ziga xos turlari bilan shug‘ullanadi, lekin axborot tizimining murakkab modelini yaratib, yanada uzoqroqqa boradi. Xavfsizlik tahdidlarining klassik turlari usuli qo‘llaniladigan GRIF, birinchi navbatda, o‘rganilayotgan ob’ektning xavfsizligi bilan belgilanadigan parametrlarning butun majmuasiga asoslanadi. Texnologik jihatlar ham, kompleks xavfsizlik masalalari ham tahlil qilinadi [5].

Avangard va GRIFning kamchiliklari - bu keng tarqalgan foydalanish

amaliyotining yo‘qligi va natijada ular yordamida olingan natijalarning ob’ektivligini baholashning qiyinligi [6]. 1-jadvalda xavfni baholash vositalarining xususiyatlarini taqqoslash keltirilgan [7].

1-jadval

Xatarlarni baholash vositalarining xususiyatlari

Texnik xususiyatlari	**Xatarlarni baholashning instrumental vositalari**			
	CRAMM	**RiskWatch**	**Grif**	**AvanGard - Tahlil**
Foydalanish qulayligi	+ / -	+	+	+ / -
Ma’lumotlarni qabul qilish usuli	Ehtimollikni to‘g‘ri baholash	Ehtimollikni to‘g‘ri baholash	Uchta mezon bo‘yicha ehtimollikni to‘g‘ri baholash	Ehtimollikni to‘g‘ri baholash
Usullarni sozlash imkoniyati	Ish profillari mavjud	-	-	Mutaxassis tomonidan amalga oshirilishi mumkin
AX uchun foydalaniladigan standart	ISO 17799	AQSh standartlari va ISO 17799	ISO 17799	GOST R ISO/IEC
Resurslar uchun tahdidlarini ro‘yxatga olish	+	+	+	+
Xizmatlar uchun tahdidlarini	+	+	+	+

ro‘yxatga olish				

Asosiy holatdan farqli o‘laroq, resurslar, xavflarning xususiyatlari va zaifliklari u yoki bu shaklda baholanadi. Tartib bo‘yicha, bir nechta himoya variantlarining xarajat / samaradorlik nisbatini tahlil qilish o‘tkaziladi. 2-jadvalda ba’zi xavflarni baholashning instrumental vositalarini solishtirish keltirilgan.

2-jadval

Xatarlarni baholashning instrumental vositalarini solishtirish

Usullar	**Qo‘llash sohasi**		**Afzalligi**	**Kamchiligi**
	Asosiy daraja	**To‘liq tahlil**		
CRAMM		+	Bu yaxshi tuzilgan va keng miqyosda sinovdan o‘tgan baholash vositasi bo‘lib, haqiqiy, amaliy natijalarni beradi. ISO 17799 standarti tavsiyalari asosida AX sohasidagi qarshi choralar bo‘yicha yetarlicha hajmli bilimlar bazasiga asoslangan.	Auditordan maxsus tayyorgarlik va yuqori malakani talab qiladi. Ular amaldagi mavjud axborot tizimlarini tekshirish uchun ko‘proq mos keladi. Shaxsiy hisobot shablonlarini yaratish va mavjudlarini o‘zgartirishga ruxsat bermaydi.
Risk-Watch		+	Oddiylik, kam mehnat sarflanishi, o‘z profillarini yaratish imkoniyati mavjud. Axborot tizimining	Yuqori narxdaligi.

			modelini tavsiflash va xavflarni baholashning soddalashtirilgan yondashuv.	
Grif		+	Foydalanish qulayligi, turli xil axborot resurslari uchun xavflarni baholash qobiliyati.	Amalda har doim ham foydali bo‘lmagan katta hajmdagi qog‘oz hujjatlarini yaratadi.
AvanGard		+	Xavf modelini qurish imkoniyati va qoldiq xavfni baholash.	Ko‘proq vaqt talab qiluvchi audit jarayoni.

Xavf-xatarlarni tahlil qilish usullarini taqqoslash shuni ko‘rsatadiki, barcha ko‘rib chiqilgan xavflarni tahlil qilish usullari tahdid qiymatlarini bevosita baholash usullaridan foydalanadi, bu esa ekspertlar javoblarining to‘g‘riligini tekshirish usullarini ta’minlamaydi.

AX xavflarini baholash uchun BS 7799-3, NIST 800-30 va boshqalar kabi bugungi kunda AX xavflarini tahlil qilishning eng yaxshi amaliyotlarini “CRAMM”, “Risk Watch” shuningdek, rus ishlanmalari “Grif”, “AvanGard” va boshqalar kabi xavflarni tahlil qilish vositalarini hisobga olish kerak.

Foydalanilgan adabiyotlar

1. Куканова Н. Методы и средства анализа рисков и управление ими в ИС // BYTE Россия. – 2005. - №12 (88).

2. Куканова Н. Современные методы и средства анализа и управления рисками информационных систем компаний. -

http://www.dsec.ru/about/articles/ar_compare/#top

3. Симонов С.В. Технологии и инструментарий для управления рисками // Jet Info – 2003- №2.

4. Медведовский И. Особенности алгоритмов систем анализа информационных рисков. - http://www.ixbt.com/cm/total-it-risks092004.shtml

5. Голов А. Аудит и сертификация систем безопасности. - http://www.topsbi.ru/default.asp?artID=83

6. Лысов А.С. Задача анализа информационных рисков в государственных учреждениях. // Безопасность информационных технологий. – 2008. - №3.

7. Джураев Р.Х., Джаббаров Ш.Ю., Умирзаков Б.М. Сетевая безопасность. Учебник. – Т.: “Алоқачи”, 2019, 308 с.