AXBOROT XAVFSIZLIGI XAVFLARINI BAHOLASH

Amirov Akbarshox Dilshod o'g'li[1]
[1]TATU Qarshi filiali AX -11-20 guruh talabasi
Tursunov Axmadjon Akmal o'g'li[2]
[2]TATU Qarshi filiali AX -11-20 guruh talabasi
Abduraxmanov Vohid Abdumuqim o'g'li[3]
[3]TATU Qarshi filiali AX -12-20 guruh talabasi
Qurbanov Abduvohid Ismoil o'g'li[4]
[4]TATU Qarshi filiali AX -12-20 guruh talabasi
https://doi.org/10.5281/zenodo.7111640

Telekommunikatsiya tarmoqlarining axborot xavfsizligi (AX) xavflarini tahlil qilish deganda AXni ta'minlash xarajatlarini baholash bilan bog'liq qarorlar qabul qilish uchun zarur bo'lgan AXga potentsial tahdidlarni aniqlash va tahlil qilishni o'z ichiga olgan ma'lumotlarni olish jarayoni tushuniladi.

AX xavfi telekommunikatsiya operatorining tajovuzkor tomonidan AX tahdidini amalga oshirishi natijasida olingan ehtimollik va kattalik qiymatlarini o'z ichiga oladi.

Xavflarni baholash qaysi resurslar va qanday tahdidlardan himoya qilinishi kerakligini, shuningdek, ma'lum resurslarni qay darajada himoya qilish kerakligini aniqlash bo'yicha faoliyatni o'z ichiga oladi. Xavf ehtimoli va xavfsizlikka tahdid yuzaga kelgan taqdirda etkazilgan yo'qotishlar miqdori bilan belgilanadi, xavfni baholash mavjud xavflarni aniqlash va ularning hajmini baholashdan iborat.

Hozirgi vaqtda telekommunikatsiya tarmog'ining AXni baholashning ikkita asosiy yondashuvi keng tarqalgan:

AXni baholashning sifatli usuli telekommunikatsiya tarmog'ining xavfsizlik darajasining AX sohasidagi standartlar yoki standartlardan birining qat'iy belgilangan talablariga muvofiqligini tekshirishga asoslangan;

AXni baholashning miqdoriy usuli AXning raqamli xususiyatlarini aniqlashga asoslangan.

Telekommunikatsiya tarmoqlarining AXni baholashning muhim yo'nalishlaridan biri bu telekommunikatsiya texnologiyalari AXning raqamli tavsiflarini (miqdoriy mezonlarni) aniqlashga asoslangan yo'nalishdir. Xatarlarni miqdoriy baholash metodologiyasi AX tahdidlariga duchor bo'lgan taqdirda mumkin bo'lgan yo'qotishlarning aniq raqamlarini taqdim etadi. Ma'lumki, AX sohasidagi faoliyatning asosiy maqsadi axborot texnologiyalaridan foydalanish bilan bog'liq xavflarni iqtisodiy jihatdan ma'lum darajada kamaytirishdir.

Miqdoriy usul sezilarli darajada ko'proq vaqt talab qiladi, chunki har bir xavf omili (faktori)ga ma'lum bir qiymat beriladi, bu amalga oshirilgan resurslar va

ob'ektlarning tahlili bo'yicha to'liq ma'lumot beradi.

Rasmiy usul himoyaning butun telekommunikatsiya tarmog'ini qamrab olishini va quyidagilarga ishonch borligini ta'minlaydi:

barcha mumkin bo'lgan xavflar aniqlangan;

resurslarning zaif tomonlari aniqlanadi va ularning darajasi baholanadi;

tahdidlar aniqlanadi va ularning darajasi baholanadi;

samarali qarshi choralar ko'riladi;

telekommunikatsiya tarmog'ining AXni ta'minlash bilan bog'liq xarajatlar o'zini oqlaydi.

Xalqaro amaliyot shuni ko'rsatadiki, xavfni miqdoriy baholash metodologiyasi xavf tahlilining to'liq versiyasiga mos keladi, ya'ni to'liq versiya va xavfni miqdoriy baholash AXga talablar kuchaygan taqdirda qo'llaniladi. Asosiy versiyadan farqli o'laroq, resurslar, xavf va zaifliklarning xususiyatlari u yoki bu shaklda baholanadi va qoida tariqasida, bir nechta himoya variantlarining xarajat / samaradorlik nisbati tahlili amalga oshiriladi.

Shunday qilib, to'liq xavf tahlilini o'tkazishda quyidagilar zarur bo'ladi:

resurslarning qiymatini aniqlash;

standart to'plamga o'rganilayotgan axborot tizimiga tegishli bo'lgan tahdidlar ro'yxatini qo'shish;

tahdidlar ehtimolini baholash;

resurslarning zaifligini aniqlash;

AXning zarur darajasini ta'minlovchi yechimni taklif qilish.

Xatarlarni miqdoriy baholash uchun yo'qotishlar chastotasini va narxini (yo'qotishlar miqdorini taqsimlash) axborot resurslari narxiga qarab baholash kerak. Xavf hajmini baholashda nafaqat uskunani almashtirish yoki ma'lumotni tiklash bilan bog'liq to'g'ridan-to'g'ri xarajatlarni, balki telekommunikatsiya tarmoqlarining normal ishlashini to'xtatish natijasida kelib chiqadigan yo'qotishlar miqdorini ham hisobga olish kerak.

AX xavfini baholashning klassik miqdoriy algoritmiga ko'ra, kutilayotgan yo'qotishlar quyidagicha aniqlanadi

Miqdoriy xavfni baholash usulining asosiy kamchiliklari quyidagilardan iborat:

aktivlarni aniqlash va baholashdagi qiyinchiliklar;

hodisalarning sodir bo'lish chastotasini aniqlash uchun statistik ma'lumotlarning etishmasligi;

miqdoriy ko'rsatkichlar o'lchovning masshtabiga va aniqligiga bog'liq;

tahlil natijalari noto'g'ri va hatto chalg'ituvchi bo'lishi mumkin;

usullar sifat tavsifi bilan to'ldirilishi kerak (sharh, talqin shaklida);

ushbu usullar yordamida amalga oshirilgan tahlil, qoida tariqasida, katta

moliyaviy xarajatlarni, ko‘proq tajribali tahlilchilarni va qo‘shimcha vositalarni talab qiladi;

katta miqdordagi statistik ma’lumotlar kerak, masalan, hodisalar, tahdidlarning chastotasi va ehtimoli va boshqalar;

ushbu usullarni qo‘llashning yanada murakkab jarayoni, matematik vositalardan foydalanishning majburiyligidir;

ishtirokchilarning sub’ektiv fikriga asoslanib, xavflarga tayinlangan qiymatlarning ta’siri;

ishonchli natijalar va konsensusga erishish jarayoni juda uzoq davom etadi;

hisoblash murakkab va ko‘p vaqt talab qilishi mumkin;

natijalar faqat pul ko‘rinishida taqdim etiladi va ularni izohlash qiyin;

o‘tish qiyin bo‘lgan miqdoriy xavfni baholash jarayonining tajribasini talab qiladi.

Umumiy xolda xavflarni miqdoriy baholashning eng keng tarqalgan usullari ALE (Annual Loss Expected), AX xavfini tahlil qilish usuli (ISRAM - Information Security Risk Analysis Method), Monte-Karlo usuli va Noravshan kompleks baholash (Fuzzy Comprehensive Evaluation- FCE) usullari ko‘rib chiqildi.

Taxlil natijasi shuni ko‘rsatdiki xavflarni miqdoriy baholashning eng keng tarqalgan va eng ko‘p qo‘llaniladigan usuli bu ALE (Annual Loss Expected) usuli ekanligi ma’lum bo‘ldi.

Foydalanilgan adabiyotlar:

1. Зинкевич В., Штатов Д. Информационные риски: анализ и количественная оценка // «Бухгалтерия и Банки» № 2, 2007, с. 48-53.
2. Artur Rot. ITRisk Assessment: Quantitative and qualitative approach. Proceedings of the world congress on engineering and science, San Francisco, USA, 2008.
3. Mohammed A. Bashir, Nicolas Christin. Three Case Studies in Quantitative Information Risk Analysis – http://www.andrew.cmu.edu/user/ nicolasc/publications
4. Valentin P. Măzăreanu. Risk management and analysis: risk assessment (qualitative and quantitative). 2007. - http://anale.feaa.uaic.ro/anale/resurse.
5. Корченко, А. Г. Построение систем защиты информации на нечетких множествах. Теория и практические решения. / А. Г. Корченко — К.: «МК-Пресс», 2006. — 320 с.: ил.
6. Джураев Р.Х., Джаббаров Ш.Ю., Умирзаков Б.М. Сетевая безопасность. Учебник. – Т.: “Алоқачи”, 2019, 308 с.

7. R.X. Djurayev. Axborot xavfsizlıgı xavflarını baholashnıng mıqdorıy usullarını tahlil qılısh