AXBOROT XAVFSIZLIGIGA TAHDIDLAR VA ULARNING MANBALARI

Xolimtayeva Ikbol Ubaydullayevna

Annotatsiya: Ushbu maqolada axborot xavfsizligiga tahdidlar va ularning texnik, ijtimoiy hamda tabiiy manbalari tahlil qilinagan undan tashqari, tahdidlarning ichki va tashqi omillari, inson omili va texnologik xatoliklar asosida yuzaga kelish sabablari ko‘rib chiqilgan. Shuningdek, ularni aniqlash va bartaraf etish bo‘yicha zamonaviy usullar hamda xavfsizlik siyosatining ahamiyati yoritilgan.

Kalit so‘zlar: Audit jarayoni doirasida axborot xavfsizligi auditi axborot tizimlari (AT)ning himoyasini ta’minlash, xavfsizlikka tahdidlar va tahdid manbalari, ichki va tashqi tahdidlar, mavjud zaifliklar, axborot jinoyatlari va kompyuter jinoyatlari bo‘yicha tahdid tahlili va hujum modellashtirish orqali risklarni tahlil qilish, dalillar tahlili hamda axborot resurslarini himoyalash uchun himoya strategiyalarini ishlab chiqishni nazarda tutadi; bu audit dasturi va audit mezonlariga asoslanib, axborot texnologiyalari xavfsizligi bo‘yicha ISO 19011, ISO 15408 (Umumiy mezonlar)

Annotation: This article analyzes threats to information security and their technical, social, and natural sources. It also examines the internal and external factors contributing to threats, focusing on human error and technological failures. Furthermore, the article explores modern methods for identifying and mitigating threats and highlights the importance of security policies.

Keywords: Within the audit process, the concept of information security audit involves ensuring the protection of information systems (IS), analyzing threats and their sources, addressing internal and external threats, identifying existing vulnerabilities, and studying threats related to cybercrimes and computer crimes. It also includes analyzing risks through threat analysis and attack modeling, evaluating evidence, and developing protection strategies to safeguard information resources. These activities are based on audit programs and criteria aligned with information technology security standards such as ISO 19011 and ISO 15408 (Common Criteria).

ISSN 2181-

Аннотация: В данной статье проанализированы угрозы информационной безопасности и их технические, социальные и природные источники. Также рассмотрены внутренние и внешние факторы, способствующие возникновению угроз, с акцентом на человеческий фактор и технологические ошибки. Кроме того, в статье освещаются современные методы выявления и нейтрализации угроз, а также подчеркивается значимость политики безопасности.

Ключевые слова: В рамках аудиторского процесса аудит информационной безопасности включает в себя обеспечение защиты информационных систем (ИС), анализ угроз и их источников, рассмотрение внутренних и внешних угроз, выявление существующих уязвимостей, а также исследование угроз, связанных с киберпреступлениями и компьютерными преступлениями. Кроме того, он предполагает анализ рисков с помощью моделирования угроз и атак, оценку доказательств и разработку стратегий защиты для обеспечения безопасности информационных ресурсов. Деятельность осуществляется на основе программ и критериев аудита в соответствии со стандартами безопасности информационных технологий, такими как ISO 19011 и ISO 15408 (Общие критерии).

Audit - bu bozor iqtisodiyotida, ayniqsa buxgalteriya hisobi sohasida keng qo‘llaniladigan tijorat korxonasi faoliyatining har qanday sohasini mustaqil hamda neytral nazorat qilish. Korxonaning umumiy rivojlanishi nuqtai nazaridan uning xavfsizligi auditi muhim ahamiyatga ega bo‘lib, u xavfsizlikka tahdidlar ehtimoli bilan bog‘liq risklarni tahlil qilishni, ayniqsa axborot resurslariga nisbatan, axborot tizimlari (AT) xavfsizligining hozirgi darajasini baholash, ularni himoya qilish tizimidagi to‘siqlarni mahalliylashtirish, axborot tizimlarining axborot xavfsizligi sohasidagi amaldagi standartlarga muvofiqligini baholash va axborot tizimlari xavfsizligini ta’minlashning yangi mexanizmlarini joriy etish va amaldagi samaradorligini oshirish bo‘yicha tavsiyalar ishlab chiqish o‘z ichiga oladi.

Axborot xavfsizligi auditining asosiy maqsadi esa rivojlanish istiqbollarini hisobga olgan holda boshqarish uchun korxona axborot tizimining xavfsizlik darajasini baholash sifatida belgilanadi.

Zamonaviy sharoitda, axborot tizimlari korxona faoliyatining barcha sohalariga singib ketganda va ularni Internet bilan bog‘lash zarurati hisobga olinsa, shuningdek, ichki va tashqi tahdidlarga ochiq bo‘lsa, axborot xavfsizligi muammosi muhimligi jihatidan iqtisodiy yoki fizik xavfsizlikdan kam emas.

Axborot xavfsizligi bo‘yicha mutaxassislar tayyorlashda ko‘rib chiqilayotgan muammoning ahamiyatiga qaramay, u hozirgacha mavjud o‘quv dasturlariga alohida kurs sifatida kiritilmagan, darslik va o‘quv qo‘llanmalarida muhokama qilinmagan. Bu axborot xavfsizligi auditi sohasida zarur me’yoriy-huquqiy bazaning yo‘qligi, maxsus tayyorlangan mutaxassislar va amaliy tajribaning yetarli emasligi bilan bog‘liq.

Mazkur tadqiqot ishi korxonada axborot xavfsizligi auditini o‘tkazish uchun birinchi navbatda uslubiy va tashkiliy asoslarni hisobga olishga qaratilgan. Ishning maqsadi belgilangan masalalarning quyidagi ketma-ketligini o‘z ichiga oladi:

– tahdidlar, zaifliklar, risklar va ularni kamaytirish yoki oldini olish bo‘yicha ko‘rilgan qarshi choralarni hisobga olgan holda axborot xavfsizligi (AT) tizimini yaratish modelini tavsiflash;

– risklarni tahlil qilish va boshqarish usullarini ko‘rib chiqish;

– xavfsizlik auditining asosiy tushunchalarini tavsiflaydi va uni amalga oshirish maqsadlarini tavsiflash;

– axborot xavfsizligi auditini o‘tkazishda qo‘llaniladigan asosiy xalqaro va milliy standartlarni tahlil qilish;

– “umumiy mezonlar” (ISO 15408 standarti) asosida axborot texnologiyalari xavfsizligini baholash mexanizmini taqdim etish;

– axborot xavfsizligini boshqarishning ISO 17799 xalqaro standartidan foydalanish bo‘yicha aniq tavsiyalar ishlab chiqish;

– axborot xavfsizligi auditini o‘tkazish uchun dasturiy ta’minotdan foydalanish imkoniyatlarini tahlil qilish;

– korxonada axborot xavfsizligi auditini o‘tkazish bo‘yicha amaliy tavsiyalar ishlab chiqish.

Axborot xavfsizligining markaziy tushunchasi “tahdid” tushunchasidir.

Lug‘atlarga ko‘ra, «tahdid» atamasi jamoat yoki shaxsiy manfaatlarga fizik, moddiy yoki boshqa zarar yetkazish, shuningdek, mumkin bo‘lgan xavfni anglatadi.

Zamonaviy adabiyotda ko‘pgina nashrlar mualliflari axborot xavfsizligiga tahdidni axborotga beqarorlashtiruvchi ta’sirning xususiyati (turi, usuli) bilan yoki sub’ekt tomonidan huquqlarining buzilishi natijasida yetkazilgan zarar ko‘rinishidagi bunday ta’sirning oqibatlari (natijalari) bilan aniqlaydilar [2,8].

«Zarar» kategoriyasi faqat uning yetkazilgani isbotlangan taqdirdagina haqiqiy hisoblanadi. Bu shuni anglatadiki, zarar yetkazishga olib keladigan harakatlar huquqiy nuqtai nazardan jinoyat tarkibi sifatida baholanishi mumkin. Shu sababli, axborot xavfsizligiga tahdidlarni aniqlashda amaldagi jinoyat qonunchiligi, xususan, O‘zbekiston Respublikasi Jinoyat kodeksi (1994 yil) talablarini inobatga olish maqsadga muvofiqdir. Axborot jinoyatlar quyidagi toifalarga ajratiladi:

1.1-jadval

Axborot jinoyatlari toifalari

Jinoyat toifasi	Tavsifi
o‘g‘irlash	g‘arazgo‘ylik maqsadida sodir etilgan, mulk egasiga arar yetkazadigan, birovning mol-mulkini aybdor yoki boshqa shaxslar foydasiga qonunga xilof ravishda tekin egallab olish va (yoki) o‘zgartirish;
kompyuter ma’lumotlarini nusxalash	ma’lumotni mashinada yoki boshqa vositada takrorlash va doimiy ravishda bosib chiqarish;

buzish	mulkka tashqi ta’sir qilish, buning natijasida u jismonan mavjud bo‘lishni to‘xtatadi yoki o‘z maqsadiga to‘liq yaroqsiz holga keltirish;
kompyuter ma’lumotlarini yo‘q qilish	ma’lumotlarni kompyuter xotirasidan o‘chirish;
zarar yetkazish	mulkning holati sezilarli darajada yomonlashadigan, foydali xususiyatlarining muhim qismi yo‘qolgan va undan maqsadli foydalanish uchun to‘liq yoki qisman yaroqsiz holga keladigan mulk xususiyatlarini o‘zgartirish;
kompyuter ma’lumotlarini o‘zgartirish	EHM dasturi yoki ma’lumotlar bazasini moslashtirish bilan bog‘liq har qanday o‘zgartirishlar kiritish;
kompyuter ma’lumotlarini blokirovka qilish	foydalanuvchilarning uni yo‘q qilish bilan bog‘liq bo‘lmagan ma’lumotlardan foydalanishni sun’iy ravishda oldini olish;
axborotni ruxsatsiz yo‘q qilish, blokirovka qilish, o‘zgartirish, nusxa ko‘chirish	qonun hujjatlari, egasi yoki vakolatli foydalanuvchi tomonidan ruxsat etilmagan ma’lumotlarga ega bo‘lgan har qanday ko‘rsatilgan harakatlar;
aldash (haqiqatni inkor qilish yoki noto‘g‘ri ma’lumot kiritish)	bu mulkka mas’ul shaxsni noto‘g‘ri yo‘naltirish orqali undan mulkni ixtiyoriy ravishda olishga erishish yoki yolg‘on ma’lumotga ega bo‘lish maqsadida haqiqatni ataylab noto‘g‘ri ko‘rsatish yoki yashirish

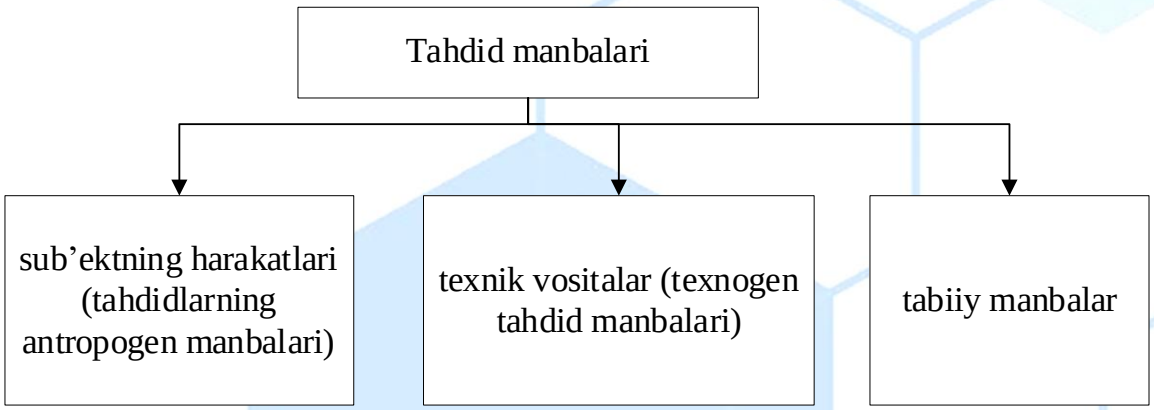
Yuqoridagilarni sarhisob qilinganda, umuman tahdidlar deganda himoya obyektiga qarshi qaratilgan, axborotni buzish, yo‘qotish yoki undan noqonuniy foydalanish xavfini keltirib chiqaruvchi, axborot resurslari egasiga (egasiga, foydalanuvchisiga) zarar yetkazishning mumkin bo‘lgan yoki haqiqiy risk (harakat yoki harakatsizlik) tushuniladi.

Tahdidlar o‘z-o‘zidan paydo bo‘lmaydi. Barcha tahdidlar axborotlashtirish obyektiga xos bo‘lgan zaifliklar mavjud bo‘lganda paydo bo‘ladi.

Zaiflik - bu avtomatlashtirilgan axborot tizimini yoki uning tarkibidagi ma’lumotlarni buzish uchun ishlatilishi mumkin bo‘lgan zaiflik. (GOST R ISO 7498-2-99 «Axborot texnologiyalari. Ochiq tizimlarning o‘zaro bog‘lanishi. Asosiy ma’lumotnoma modeli. 1-qism. Axborot xavfsizligi arxitekturasi»).

Axborot xavfsizligini baholash jarayonida tahdid manbalariga alohida e’tibor qaratish muhimdir. Tahdid manbalari sifatida subyektlar (insonlar) hamda obyektiv omillar ishtirok etishi mumkin. Shuningdek, tahdid manbalari axborot tizimining ichki qismida (ichki manbalar) yoki uning tashqarisida (tashqi manbalar) joylashgan bo‘lishi mumkin.

Tahdid manbalari 1.1-rasmda keltirilgan.



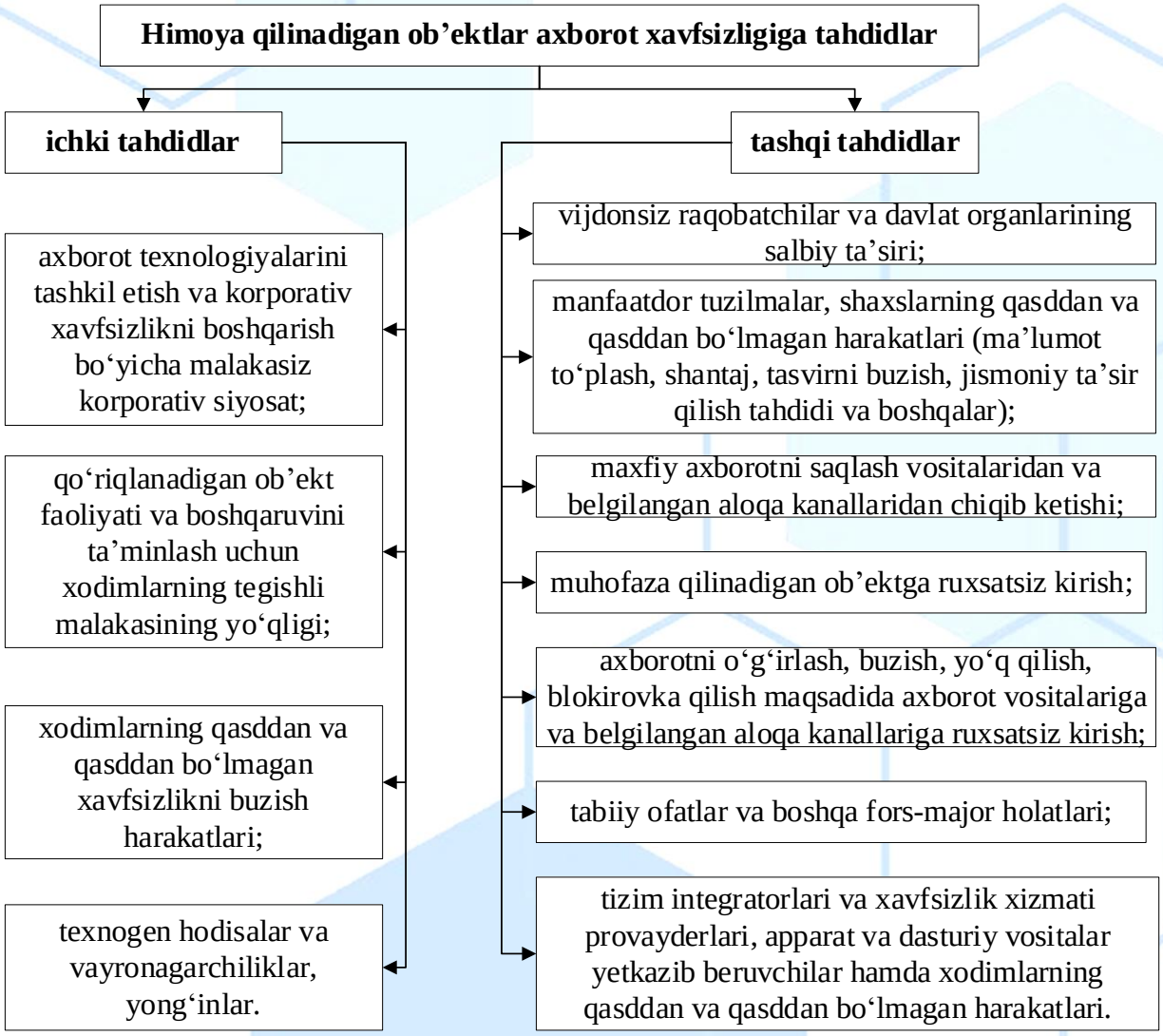
1.1-rasm. Tahdid manbalari

Tahdidlarning antropogen manbalariga xatti-harakatlari qasddan yoki tasodifiy jinoyatlar sifatida tasniflanishi mumkin bo‘lgan sub’ektlar kiradi.

Tahdidlarning texnogen manbalariga insonning texnokratik faoliyati va sivilizatsiya rivojlanishi bilan belgilanadigan manbalar kiradi.

Tabiiy manbaga ega tahdidlar qatoriga tabiiy ofatlar yoki oldindan bashorat qilib bo‘lmaydigan, shuningdek, insoniyatning mavjud bilimlari va texnologik imkoniyatlari bilan oldini olish imkoni bo‘lmagan boshqa hodisalar kiradi.

Axborot xavfsizligi tahdidlarining tahlili shuni ko‘rsatadiki, ularni ikki turga bo‘lish mumkin: ichki va tashqi (1.2-rasm).



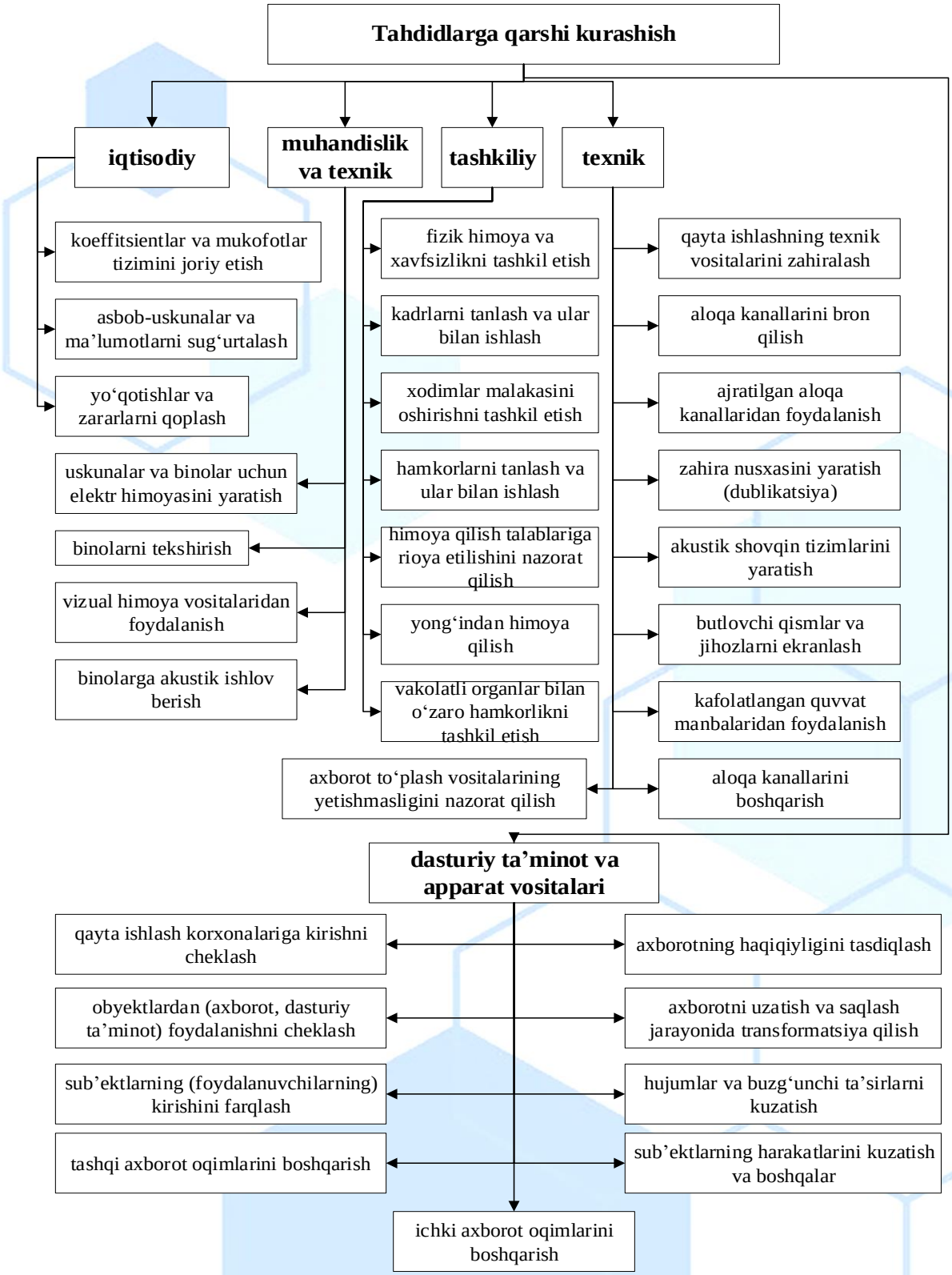
1.2-rasm. Himoya qilinadigan obyektlar xavfsizligiga nisbatan tahdidlar

Axborotlashtirish obyektiga axborot xavfsizligi tahdidlarini tahlil qilishda quyidagi kompleks yondashuvlarni amalga oshirish zarur:

– obyekt tavsifi;

– tahdid manbalarini tasniflash;
– zaifliklarni tasniflash;
– tahdidlarni amalga oshirish usullarini tasniflash;
– joriy hujumlar reytingi;
– tahdidlarni bartaraf etish usullarini tasniflash.

Axborot tizimining tipik tarkibiy qismlari hamda ular o‘rtasidagi aloqalar ko‘rinishida taqdim etilgan axborotlashtirish obyektining tizimli tavsifi matnli tushuntirishlar bilan birgalikda axborot oqimlarining aylanish yo‘nalishlari va parametrlarini tavsiflaydi, bu mumkin bo‘lgan nuqtalarni aniqlash va tahdidlarni qo‘llash yoki mavjud zaifliklarni aniqlashga imkon beradi.



1.3-rasm. Tahdidlarga qarshi kurashish usullari

Tahdidlarni amalga oshirish imkoniyatlarini tahlil qilish va baholash tahdid modelini qurish, tahdid manbalarini tasniflash, tahlil qilish va baholash, zaifliklar va amalga oshirish usullariga asoslanishi kerak. Axborot xavfsizligini buzish jarayonlarini

modellashtirish mantiqiy zanjirni hisobga olgan holda amalga oshirilishi mumkin: *tahdid - tahdid manbai - amalga oshirish usuli - zaiflik - oqibatlar.*

Ko‘rib chiqilayotgan mantiqiy zanjirning har bir komponenti kerakli tafsilotda mos ravishda tasvirlangan.

Tahdidlar axborot xavfsizligi maqsadlari buzilganda zarar yetkazish ehtimoli bo‘yicha tasniflanadi; *tahdidlar manbalari* - tahdid tashuvchining turi va joylashuvi bo‘yicha; *zaifliklar* - namoyon bo‘lishi bilan zaifliklar manbasiga mansubligi.

Hujumlarning tasnifi – bu tahdid manbai tomonidan ma’lum bir usullar yordamida amalga oshiriladigan, zaifliklardan foydalangan holda maqsadlarga erishishning ehtimoliy yo‘llari to‘plamidir. Shu bilan birga, hujumning maqsadi har doim ham tahdidni amalga oshirish maqsadi bilan mos kelmasligi mumkin. U ayrim hollarda tahdidni keyingi bosqichda amalga oshirish uchun zarur bo‘lgan oraliq natijalarni qo‘lga kiritishga qaratilgan bo‘lishi mumkin. Agar hujum maqsadlari tahdidni to‘liq amalga oshirishga mos kelmasa, bu holatda hujum tahdidga qaratilgan harakatlarga tayyorgarlik jarayoni sifatida qaraladi, ya’ni noqonuniy faoliyatni amalga oshirishga tayyorgarlik bosqichi hisoblanadi.

Mavjud tahdidlarni tasniflash, tartiblash, tahlil qilish aniqlash, tahdidlar va zaiflik manbalari, mumkin bo‘lgan hujumlarning variantlari aniqlanadi, bu esa axborot xavfsizligi holatini baholash va tahdidlarga qarshi kurashish usullarini tanlashni optimallashtirish imkonini beradi (1.6-rasm).

ISO 19011 – bu menejment tizimlari auditini rejalashtirish, o‘tkazish va boshqarish bo‘yicha xalqaro standartdir. U barcha turdagi auditlarga, jumladan, axborot xavfsizligi, sifat menejmenti, ekologik menejment va boshqa tizimlarga tegishli.

ISO 19011 standarti bo‘yicha audit jarayoni 1.2-jadvalda keltirilgan.

1.2-jadval

ISO 19011 bo‘yicha audit jarayoni

Bosqich	Asosiy faoliyatlar	Natija

Auditni rejalashtirish	- audit maqsadlarini aniqlash - audit doirasini belgilash - audit mezonlarini aniqlash - auditorlar guruhini tayinlash	Audit rejasi tayyorlanadi
Auditni tayyorlash	- audit dasturini ishlab chiqish - tekshiriladigan hujjatlarni yig‘ish - tashkilot vakillari bilan oldindan muloqot qilish	Audit dasturi va tekshirish mezonlari
Auditni o‘tkazish	- hujjatlarni tekshirish - xodimlar bilan suhbat o‘tkazish - joylarda kuzatuvlar o‘tkazish - aniqlangan muammolarni hujjatlashtirish	Dalillar to‘planadi va tekshiriladi
Audit natijalarini tahlil qilish va hisobot tayyorlash	- olingan dalillarni tahlil qilish - xulosa va tavsiyalarni ishlab chiqish - audit hisoboti tayyorlash	Audit hisoboti va tavsiyalar
Audit natijalariga javob choralarini ishlab chiqish	- kamchiliklarni bartaraf etish bo‘yicha harakat rejasini tuzish - qo‘shimcha auditlar o‘tkazish (zarur bo‘lsa) - menejment tizimini takomillashtirish	Harakat rejasi va takomillashtirish choralari

Xulosa

Axborot xavfsizligi sohasida tahdidlarning tahlili shuni ko‘rsatadiki, ularning kelib chiqish sabablari ko‘p qirrali bo‘lib, texnik, ijtimoiy, tabiiy va inson omillari bilan chambarchas bog‘liqdir. Ushbu maqolada axborot xavfsizligiga tahdidlarning tasnifi, ularning manbalari, zaifliklar bilan o‘zaro bog‘liqligi hamda hujumlarni

modellashtirish orqali risklarni aniqlash masalalari chuqur yoritilgan. Ayniqsa, ichki va tashqi tahdidlar hamda ularning zaifliklar bilan kesishuvchi nuqtalari orqali xavfsizlik holatining baholanishi axborot tizimlarining himoyasini samarali tashkil etish uchun muhim omil hisoblanadi.

Shuningdek, maqolada tahdidlarni oldindan aniqlash va bartaraf etish bo‘yicha xalqaro standartlarga asoslangan audit jarayonining bosqichlari, xususan ISO 19011 va ISO 15408 kabi hujjatlar asosida amalga oshiriladigan baholash mexanizmlari amaliy yondashuv sifatida taklif etildi. Axborot jinoyatlarining shakllari, ularning huquqiy oqibatlari, kompyuter ma’lumotlariga ruxsatsiz aralashuv turlari va ularning xavfli oqibatlari bo‘yicha keltirilgan jadval va tasniflar mavzuni yanada aniqroq ochib berdi.

Mazkur tahlillar asosida xulosa qilish mumkinki, korxona va tashkilotlarda axborot xavfsizligi auditi faqat nazorat vositasi emas, balki xavfsizlik siyosatini shakllantirish va mukammallashtirishga xizmat qiluvchi strategik vosita bo‘lishi lozim. Tahdidlarni aniqlash, risklarni baholash va samarali himoya strategiyalarini ishlab chiqish orqali tashkilotlar o‘z axborot resurslarini ishonchli tarzda himoya qilish imkoniyatiga ega bo‘ladi. Shu bilan birga, axborot xavfsizligini ta’minlash bo‘yicha mutaxassislarni tayyorlashda, o‘quv dasturlariga auditga oid maxsus kurslarni joriy etish zaruriyati ham ko‘zga tashlanadi.

Foydalanilgan adabiyotlar:

1. ISO/IEC 27001:2022 — ***Information Security, Cybersecurity and Privacy Protection – Information Security Management Systems – Requirements***. International Organization for Standardization.
2. ISO/IEC 15408:2009 — ***Information Technology – Security Techniques – Evaluation Criteria for IT Security (Common Criteria)***.
3. ISO 19011:2018 — ***Guidelines for Auditing Management Systems***. International Organization for Standardization.

4. Государственный стандарт Российской Федерации ГОСТ Р ИСО/МЭК 7498-2–99 – ***Информационные технологии. Взаимосвязь открытых систем. Основная модель безопасности***.

5. Solovev D. A. (2020). ***Information Security: Threats, Protection, Audit***. Moscow: Infra-M.

6. Shchemelinin L.S. (2022). ***Audit of Information Security: Theory and Practice***. SPb: Piter.

7. Убайдуллаев У.Т., Юсупов Ж.М. (2020). ***Axborot xavfsizligi va kriptografiya asoslari***. Toshkent: TATU.

8. Hasanov M.S., Xolmatov A.S. (2021). ***Kompyuter tizimlari va tarmoqlarda axborot xavfsizligi***. Toshkent: Fan va texnologiya nashriyoti.

9. Rasulov A.T. (2019). ***Axborot xavfsizligi auditi: nazariy va amaliy asoslari***. Toshkent: Iqtisodiyot.

10. National Institute of Standards and Technology (NIST). (2018). ***Framework for Improving Critical Infrastructure Cybersecurity***, Version 1.1.

11. Buecker A., Drobik M., Nash S. (2020). ***Security Intelligence: Protecting the Enterprise with Security Intelligence and Operational Risk Management***. IBM Redbooks.

12. Stallings, W. (2017). ***Network Security Essentials: Applications and Standards***. Pearson Education.

13. Tanenbaum, A. S., & Wetherall, D. J. (2021). ***Computer Networks***. 6th Edition. Pearson.

14. Бородин С.В., Бычков И.В. (2020). ***Комплексная информационная безопасность организации***. Москва: Юрайт.

15. Tuxmanov Sh., Sharipov A. (2023). ***Axborot xavfsizligi siyosati va boshqaruvi***. Toshkent: Iqtisodiy fanlar nashriyoti.