AUDIT TADBIRLARINING TASNIFI

Xolimtayeva Ikbol Ubaydullayevna

Annotatsiya: Ushbu maqolada axborot xavfsizligi auditining umumiy tasnifi, uning turlari va tasniflash mezonlari batafsil ko‘rib chiqilgan. Jumladan, auditning maqsadi, obyekti, shakli, o‘tkazish uslubi, qonuniylik darajasi va auditorning o‘rganilayotgan tizimga nisbatan joylashuvi kabi mezonlar asosida tasniflash yondashuvlari tahlil qilingan. Shuningdek, passiv va aktiv audit farqlari, ularning metodik jihatlari, axborot tizimlariga ta’sir darajasi, shuningdek, auditning qonuniy va noqonuniy shakllari o‘rtasidagi huquqiy tafovutlar yoritilgan. Auditning ekspert, muvofiqlikni baholovchi, testlashga asoslangan va kompleks turlari amaliy misollar va mezonlar asosida tahlil qilinadi. Muvofiqlikni baholash jarayonlarida sinov, attestatsiya va sertifikatlash kabi shakllar orqali axborot xavfsizligi darajasini aniqlash mexanizmlari keltirilgan. Mazkur tadqiqotda auditorlik faoliyatining zamonaviy yondashuvlari, standartlar asosidagi baholash mezonlari va axborot xavfsizligi holatini baholashda kompleks yondashuvning zarurligi asoslab berilgan.

Kalit so‘zlar: Axborot xavfsizligi auditi, audit turlari, passiv audit, aktiv audit, ekspert auditi, muvofiqlikni baholash, sinov, attestatsiya, sertifikatlash, testlash, instrumental audit, qonuniy va noqonuniy audit, ichki va tashqi audit, tizimli tahlil, zaifliklar, tahdidlar, hujum modellashtirish, ISO 19011, ISO 15408, axborot xavfsizligini baholash, xavfsizlik siyosati.

Annotation: This article provides a detailed overview of the general classification of information security audits, including their types and classification criteria. Specifically, the study examines classifications based on audit purpose, object, form, method of execution, level of legality, and the auditor’s position relative to the system being assessed. It also explores the distinctions between passive and active audits, their methodological aspects, the degree of impact on information systems, and the legal differences between legitimate and illegitimate audit practices. Furthermore, the article analyzes expert audits, compliance assessments, testing-based and

comprehensive audits with practical examples and defined criteria. Mechanisms for determining the level of information security through processes such as testing, attestation, and certification are also presented. The study justifies the necessity of a modern, standardized, and integrated approach to auditing practices in evaluating information security.

Keywords: Information security audit, audit types, passive audit, active audit, expert audit, compliance assessment, testing, attestation, certification, instrumental audit, legal and illegal audit, internal and external audit, systematic analysis, vulnerabilities, threats, attack modeling, ISO 19011, ISO 15408, information security evaluation, security policy.

Аннотация: В данной статье представлен подробный обзор общей классификации аудита информационной безопасности, включая его типы и критерии классификации. В частности, рассматриваются классификации по цели аудита, объекту, форме, методу проведения, уровню законности и положению аудитора по отношению к анализируемой системе. Также исследуются различия между пассивным и активным аудитом, их методологические особенности, степень воздействия на информационные системы, а также правовые различия между законными и незаконными формами аудита. Дополнительно проанализированы экспертные аудиты, оценка соответствия, тестовые и комплексные виды аудита с практическими примерами и установленными критериями. Представлены механизмы определения уровня информационной безопасности посредством тестирования, аттестации и сертификации. Исследование обосновывает необходимость применения современного, стандартизированного и интегрированного подхода к аудиторской практике при оценке состояния информационной безопасности.

Ключевые слова: Аудит информационной безопасности, виды аудита, пассивный аудит, активный аудит, экспертный аудит, оценка соответствия, тестирование, аттестация, сертификация, инструментальный аудит, законный и незаконный аудит, внутренний и внешний аудит, системный анализ, уязвимости,

угрозы, моделирование атак, ISO 19011, ISO 15408, оценка информационной безопасности, политика безопасности.

Axborot xavfsizligi auditining umumiy tasnifi, ushbu faoliyat turlarining yuqoridagi parchalanishini hisobga olgan holda, 1.1-rasmda ko‘rsatilgan.

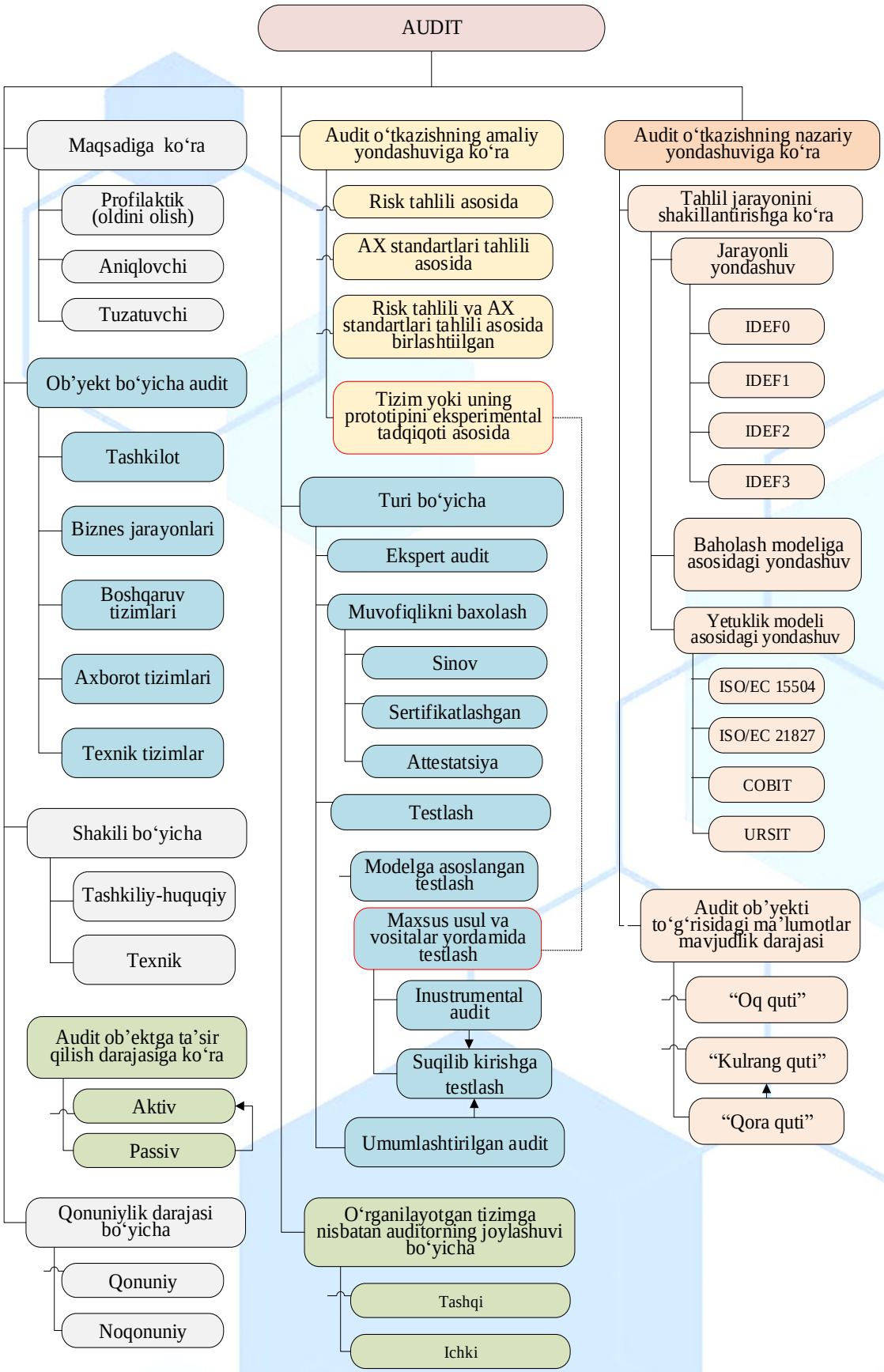
Axborot xavfsizligi auditini quyidagi asosda tasniflash mumkin:

1) audit maqsadi bo‘yicha;
2) audit obyekti bo‘yicha;
3) audit shakli bo‘yicha;
4) audit o‘tkazishga amaliy yondashuv bo‘yicha;
5) audit o‘tkazishga nazariy yondashuv bo‘yicha;
6) tekshirilayotgan obyektga ta’sir qilish darajasi bo‘yicha;
7) qonuniylik darajasi bo‘yicha;
8) o‘rganilayotgan tizimga nisbatan auditorning joylashgan joyi bo‘yicha;
9) audit turi bo‘yicha.

*Obyektga ta’sir qilish darajasiga ko‘ra audit*ni quyidagilarga bo‘lish mumkin:

– passiv;
– aktiv.

Passiv audit - bu haqiqiy audit ob’yektiga o‘zgarishlar kiritmaydigan va uni boshqa holatga o‘tkazmaydigan faoliyatni amalga oshiradi. Passiv auditga axborot xavfsizligi standartlari tahlili asosida, shuningdek, risklarni tahlil qilishning rasmiy modellari asosida o‘tkaziladigan har qanday turdagi auditni o‘z ichiga oladi. Agar auditda modellar asosida sinovlar o‘tkazilsa, bunday turdagi audit ham passiv hisoblanadi. Passiv auditga audit ob’yekti yoki uning himoya vositalari haqida ma’lumot to‘plashga qaratilgan maxsus vositalar va usullarni, ATT yoki razvedka xususiyatiga ega bo‘lgan APT qo‘llash bilan bog‘liq jarayonlarni ham kiritish mumkin.



1.1-rasm. Audit tadbirlarining tasnifi

Aktiv audit tekshiruv jarayonida o‘rganilayotgan tizimga maqsadli ta’sir o‘tkazish orqali uning reaksiyasini tahlil qilish yoki uni kerakli holatga keltirishni nazarda tutadi. Bu, odatda, tizimning himoya darajasini pasaytirishni o‘z ichiga oladi. Aktiv auditga quyidagilar kirishi mumkin: tizimni maqsadli axborot-texnik va axborot-psixologik ta’sir vositalari orqali testdan o‘tkazish, noto‘g‘ri yoki yolg‘on ma’lumotlarni shakllantirish, tizim faoliyat ko‘rsatadigan noqulay muhit yaratish, uning tuzilishiga o‘zgartish kiritish yoki unga qo‘shimcha funksional elementlar qo‘shish.

1-5-asoslar bo‘yicha audit tasnifi yuqorida ko‘rib chiqilgan, keyin esa 6-9-asoslar bo‘yicha audit tasnifi ko‘rib chiqiladi.

Qonuniylik darajasiga ko‘ra, audit quyidagicha tasniflanishi mumkin [4, 13]:

– qonuniy;

– noqonuniy.

Qonuniy audit huquqiy xavfsizlik bilan ajralib turadi va odatda audit ob’yekti xavfsizligini ta’minlash bilan bevosita bog‘liq bo‘lgan buyurtmachi bilan auditor o‘rtasidagi shartnoma asosida amalga oshiriladi. Bu audit ob’yekti himoya darajasini oshirishga qaratilgan choralarni ishlab chiqish maqsadida o‘tkaziladi.

Noqonuniy audit o‘rganilayotgan tizimning zaifliklari haqidagi ma’lumotlarni noqonuniy va noqonuniy usullar yordamida olishga asoslangan. Bunday noqonuniy usullarga quyidagilar kiradi: o‘g‘rilik, qasddan aldash, ruxsatsiz eshitish, identifikatsiya qiluvchi hujjatlarni soxtalashtirish, hamda, noqonuniy harakatlar alomatlariga ega bo‘lgan turli xatti-harakatlarni qo‘llash.

Shuningdek, o‘rganilayotgan tizim yoki tashkilotga zarar yetkazish uchun keyinchalik audit natijalaridan foydalanish maqsadida uchinchi shaxslar ishtirokida yoki buyurtma asosida o‘tkaziladigan audit noqonuniy tadbirlarga kiritilishi mumkin. Shuningdek, o‘rganilayotgan tizim yoki tashkilotga zarar yetkazish uchun keyinchalik audit natijalaridan foydalanish maqsadida uchinchi shaxslar ishtirokida yoki buyurtma asosida o‘tkaziladigan audit noqonuniy jarayonlarga kiritilishi mumkin.

Auditni qonuniy va noqonuniy deb tasniflashda quyidagi qarama-qarshi jihatni e’tiborga olish lozim. Tegishli kuchlar (“kiberqo‘shinlar”) tomonidan axborot operatsiyalarini amalga oshirishda bu operatsiyalar ularni o‘tkazuvchi tomonning ichki nizomlari bilan tartibga solinadi, ya’ni ushbu tomon uchun raqib tizimlarining auditi qonuniy hisoblanadi. Shu bilan birga, bunday audit, odatda, audit obyektiga tegishli tomonning qonunchiligini buzish bilan bog‘liq bo‘ladi, shunga ko‘ra, ushbu tomon nuqtai nazaridan audit noqonuniy hisoblanadi.

O‘rganilayotgan tizimga nisbatan auditorning joylashgan joyiga qarab, auditni quyidagilarga ajratish mumkin: [4, 19]:

– tashqi;

– ichki.

Tashqi audit - mustaqil tashqi ekspertlar tomonidan yoki tadqiq qilinayotgan tizimdan tashqarida joylashgan texnik vositalar va test usullaridan foydalanilgan holda amalga oshiriladi. [4, 19] adabiyotlarda ta’kidlanganidek, odatda tashqi audit tashkilot rahbariyati tashabbusi bilan bir martalik jarayon sifatida o‘tkaziladi.

Ichki audit - bu doimiy faoliyat bo‘lib, u tashkilotning xavfsizlik xizmati bo‘limlari tomonidan tashkilotning tartibga soluvchi normativ hujjatlari asosida axborot xavfsizligini ta’minlash texnik vositalari va tashkilot ekspertlarini jalb qilish orqali amalga oshiriladi.

Audit turi bo‘yicha quyidagicha tasniflanishi mumkin [4, 9, 10]:

– ekspert auditi;

– muvofiqlikni baholash:

- sinov;
- attestatsiya;
- sertifikatlash;

– testlash:

- modelga asoslangan test;
- maxsus vositalar va usullardan foydalangan holda test o‘tkazish (shu jumladan instrumental audit va suqilib kirishga sinash);

– keng qamrovli audit.

Ekspert auditida axborot xavfsizligini ta’minlash tizimidagi kamchiliklar, audit jarayonida ishtirok etayotgan ekspertlarning mavjud tajribasiga asoslanib aniqlanadi. Ekspert auditida tizimning axborot xavfsizligi holati ba’zi bir “ideal” tasvir bilan solishtiriladi, bu esa quyidagi omillarga asoslanadi:

– auditni o‘tkazish jarayonida rahbariyat tomonidan qo‘yilgan talablar;

– “ideal” xavfsizlik tizimining tavsifi.

Ekspert audit odatda, tashkilotning ichki hujjatlari, ya’ni xavfsizlik siyosati, himoya rejalari, turli xil ko‘rsatmalar, shuningdek, himoya tizimini joriy etish va takomillashtirish loyihalari tahlil qilinadi. Ushbu hujjatlar axborot xavfsizligini ta’minlashning e’lon qilingan maqsadlari va choralari bilan mosligi va ziddiyatli emasligi nuqtai nazaridan baholanadi. Bunday tahlil jarayonida mavjud himoya tizimining kamchiliklari va zaifliklari aniqlanadi, shuningdek, xavfsizlik darajasini oshirishga qaratilgan kompleks choralari taklif qilinadi. Shuni ta’kidlash lozimki, ekspert auditida oldingi tekshiruvlar natijalari (shu jumladan, boshqa auditorlar tomonidan o‘tkazilgan tekshiruvlar) hisobga olinadi, hamda loyihalash qarorlari va axborot tizimini yaratish bilan bog‘liq boshqa ish hujjatlari tahlil qilinadi. Ekspert auditiga oid batafsil ma’lumotlar [4, 20] ishlarida keltirilgan.

Muvofiqlikni baholash - mahsulot, jarayon, tizim, shaxs yoki organ uchun belgilangan talablarning bajarilganligini isbotlash. Isbotlash to‘g‘ridan-to‘g‘ri yoki bilvosita, rasmiy yoki norasmiy bo‘lishi mumkin. Talablar bo‘yicha hujjatli tasdiqlovchi bayonot (guvohnoma) berishni muvofiqlikni tasdiqlash deb atashadi. Bunday tasdiqlovchilarga misollar sifatida sertifikatlar, attestatlar, xulosalar, rasmiy muvofiqlikni baholash organlari tomonidan berilgan hujjatlar bo‘lishi mumkin. Bunday hujjatli tasdiqlashning mavjudligi muvofiqlikni baholashni boshqa turdagi auditlardan ajratib turadi, chunki ular davlat namunasidagi hujjat shaklida hujjatli tasdiqlovchiga ega bo‘lmasligi mumkin. Shu bilan birga, audit mezonlari yanada moslashuvchan bo‘lishi mumkin, uning o‘tkazilish usullari va vositalari esa turli xil

bo‘lishi mumkin. Muvofiqlikni baholash tadbirlari quyidagi tadbirlarga bo‘linishi mumkin: sinov, attestatsiya, sertifikatlash [10].

Muvofiqlikni baholash bo‘yicha batafsil ma’lumot [10] da keltirilgan.

Sinov - obyektining ishlashi yoki modellashtirilishida unga turli omillar ta’siri natijasida uning miqdoriy yoki sifat tavsiflarini eksperimental aniqlash. Sinovlar “sinov dasturi va metodologiyasi” hujjati asosida o‘tkaziladi va sinov natijalari, sinov bayonnomalari yoki texnik hisobot shaklida rasmiylashtiriladi [10].

Attestatsiya - bu axborotlashtirishni himoya qilinayotgan obyektini haqiqiy ekspluatatsiya sharoitlarida kompleks tekshirish bo‘lib, uning xavfsizlikni ta’minlash bo‘yicha qo‘llanilayotgan choralar va vositalarning talab qilingan axborot xavfsizligi darajasiga mosligini baholash maqsadida amalga oshiriladi. Attestatsiyaning ijobiy natijasi *muvofiqlik attestati* shaklida rasmiylashtiriladi.

Sertifikatlash - bu axborotni himoya qilish texnik vositalarini mustaqil sinov laboratoriyalarida sinovdan o‘tkazish bo‘lib, uning maqsadi sertifikatlash obyektining axborotni himoya qilish bo‘yicha normativ hujjatlarga muvofiqligini tasdiqlashdir.

Testlash - bu mahsulot, jarayon yoki xizmatning bir yoki bir nechta xususiyatlarini tegishli protseduraga muvofiqligini aniqlashdan iborat texnik operatsiya. Shunday qilib, axborot xavfsizligini audit qilishda testlash - bu axborot tizimining bir yoki bir nechta parametrlarini aniqlash bo‘lib, ular ma’lum bir axborot xavfsizligi kategoriyasini (masalan, konfidensiallik, yaxlitlik, foydalanuvchanlik) tavsiflaydi. Testlash risklar va zaifliklarni tahlil qilish maqsadida o‘tkazilishi mumkin. Axborot tizimining testlash majmuasi sinov dasturi shaklida rasmiylashtirilishi va ularning yakuni natijalari bo‘yicha tegishli protokol tuzilishi mumkin.

Umuman olganda, barcha turdagi testlash, auditga nazariy yoki amaliy yondashuvdan foydalanishga qarab, quyidagicha tasniflanishi mumkin:

– *modellar asosida testlash* - testlashning nazariy yondashuvi bo‘lib, bunda tegishli modellar quriladi va testlash ushbu modellarni tadqiq qilish asosida amalga oshiriladi;

– *maxsus vositalar va usullar bilan testdan o‘tkazish* - testdan o‘tkazishga amaliy yondashuv bo‘lib, bunda testdan o‘tkazish axborot-texnik ta’sirlar va axborot-psixologik ta’sirlar vositalari va usullarining audit obyektiga yoki uning prototipiga ta’siri bo‘yicha tajribalar asosida o‘tkaziladi.

Kompleks audit - auditni o‘tkazishning yuqorida sanab o‘tilgan bir necha turlaridan foydalanishni o‘z ichiga oladi.

Xulosa

Axborot xavfsizligi auditi zamonaviy axborot tizimlarini himoya qilishda muhim strategik vosita hisoblanadi. Ushbu maqolada auditning maqsadi, shakli, obyekti, qonuniylik darajasi, o‘tkazilish usullari va auditorning joylashuvi kabi mezonlar asosida tasniflash yondashuvlari chuqur tahlil qilindi. Ayniqsa, passiv va aktiv auditlar o‘rtasidagi metodik va amaliy farqlar, ular orqali tizimlarning zaif joylarini aniqlash hamda xavfsizlik siyosatini takomillashtirish mexanizmlari alohida yoritildi.

Shuningdek, qonuniy va noqonuniy audit faoliyatlari o‘rtasidagi huquqiy tafovutlar, ichki va tashqi auditlar, hamda real tizimga bevosita ta’sir o‘tkazuvchi testlash, attestatsiya va sertifikatlash kabi muvofiqlikni baholash shakllari asosida axborot xavfsizligi holatini aniqlash imkoniyatlari ko‘rsatildi. Ekspert auditi, instrumental audit va kompleks audit yondashuvlarining ustunliklari hamda cheklovlari ilmiy-amaliy misollar orqali asoslab berildi.

Ushbu tadqiqot natijalariga ko‘ra, tashkilotlar axborot xavfsizligini ta’minlashda faqatgina standartlarga asoslangan yondashuv emas, balki tizimli, kompleks va moslashuvchan auditori nazorat strategiyasini ishlab chiqishi zarur. Bu esa nafaqat mavjud xavflarni aniqlash va bartaraf etishga, balki xavfsizlik darajasini uzluksiz monitoring qilish va takomillashtirishga xizmat qiladi. Shu nuqtai nazardan, axborot xavfsizligi auditining tasnifiy yondashuvi uni samarali rejalashtirish va amalga oshirish uchun metodik asos vazifasini bajaradi.

Foydalanilgan adabiyotlar

1. ISO/IEC 19011:2018 — ***Guidelines for auditing management systems***. International Organization for Standardization (ISO).

2. ISO/IEC 15408-1:2009 — ***Information technology – Security techniques – Evaluation criteria for IT security – Part 1: Introduction and general model***.

3. ISO/IEC 27001:2022 — ***Information Security, Cybersecurity and Privacy Protection – Information Security Management Systems – Requirements***.

4. ГОСТ Р ИСО/МЭК 7498-2–99 – ***Информационные технологии. Взаимосвязь открытых систем. Основная эталонная модель. Архитектура информационной безопасности***.

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

6. Solovev D.A. (2021). ***Audit of Information Security: Theoretical and Practical Aspects***. Moscow: INFRA-M.

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

8. Rasulov A.T. (2019). ***Axborot xavfsizligi auditi: nazariy va amaliy asoslari***. Toshkent: Fan va texnologiya.

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

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

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

12. Stallings, W. (2017). ***Information Security: Principles and Practice***. Pearson.

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

14. Xolmatov Z.S., Xaydarov T.E. (2022). ***Axborot xavfsizligi asoslari va himoya mexanizmlari***. Toshkent: Innovatsion texnologiyalar markazi.

15. Karimov B.E., Sharipov U.T. (2023). ***Audit va axborot xavfsizligi boshqaruvi***. Toshkent: Iqtisodiyot va moliya.