ZAMONAVIY AXBOROT XAVFSIZLIGI TIZIMLARINI LOYIIHALASH: AI VA IOT YONDASHUVLARI ASOSIDA

Djamatov Mustafa Xatamovich
IIV Akademiyasi Raqamli texnologiyalar va axborot xavfsizligi kafedrasi kata o‘qituvchisi, f.-m.f.n.
Abdazimov Saidaminxo‘ja Zoirxo‘ja o‘g‘li
IIV Akademiyasi Raqamli texnologiyalar va axborot xavfsizligi kafedrasi o‘qituvchisi;

Annotatsiya: *Mazkur maqolada zamonaviy axborot xavfsizligi tizimlarini loyihalashning asosiy tamoyillari, AI va IoT asosidagi monitoring yondashuvlari hamda real vaqtli xavfsizlikni ta’minlash usullari tadqiq etiladi. Sun’iy intellekt algoritmlari va IoT sensorlarining birgalikdagi ishlashini tizim samaradorligini oshirish, tahdidlarni aniqlash, foydalanuvchi identifikatsiyasini kuchaytirish va ruxsatsiz kirishlarni oldini olish bo‘yicha amaliy yechimlar bilan birlashtirish ko‘rib chiqiladi. Maqolada minimal narxli tizim yaratish, foydalanuvchi ruxsatlarini individualizatsiya qilish va AI + IoT integratsiyasi orqali proaktiv xavfsizlikni ta’minlash masalalari yoritiladi.*

Kalit so‘zlar: *Axborot xavfsizligi, AI, IoT, tizim loyihalash, real vaqtli monitoring, tahdidlarni aniqlash, foydalanuvchi identifikatsiyasi, ruxsatsiz kirish, minimal narxli tizim, proaktiv xavfsizlik*

Аннотация: *В статье рассматриваются основные принципы проектирования современных систем информационной безопасности с использованием подходов AI и IoT, а также методы обеспечения безопасности в реальном времени. Исследуется совместная работа алгоритмов искусственного интеллекта и сенсоров IoT для повышения эффективности системы, выявления угроз, усиления идентификации пользователей и предотвращения несанкционированного доступа. Рассматриваются задачи создания систем с минимальной стоимостью, индивидуализация прав пользователей и обеспечение проактивной безопасности через интеграцию AI и IoT.*

Ключевые слова: *Информационная безопасность, AI, IoT, проектирование системы, мониторинг в реальном времени, выявление угроз, идентификация пользователей, несанкционированный доступ, минимальная стоимость системы, проактивная безопасность*

Annotation: *This article examines the principles of designing modern information security systems based on AI and IoT approaches, as well as methods for ensuring real-time security. The integration of artificial intelligence algorithms and IoT sensors is analyzed for enhancing system efficiency, detecting threats, improving user identification, and preventing unauthorized access. The study also discusses low-cost system design, individualization of user permissions, and proactive security measures achieved through AI + IoT integration.*

Keywords: *Information security, AI, IoT, system design, real-time monitoring, threat detection, user identification, unauthorized access, low-cost system, proactive security*

Sun’iy intellekt (AI) algoritmlari axborot xavfsizligi tizimlarida tahdidlarni aniqlash, foydalanuvchi harakatlarini nazorat qilish va xavfsizlik darajasini oshirish uchun keng qo‘llaniladi. AI yordamida tizimlar faoliyatni doimiy monitoring qilish, anomal holatlarni avtomatik aniqlash va real vaqt rejimida xavfsizlik choralarini joriy etish imkoniyatiga ega bo‘ladi.

Bugungi kunda axborot xavfsizligi tizimlari nafaqat statik qoidalar asosida, balki sun’iy intellekt (AI) va IoT qurilmalari yordamida real vaqtli monitoring asosida samarali loyihalanmoqda. Tashqi va ichki tahdidlarni aniqlash, foydalanuvchi identifikatsiyasi va ruxsatlarni nazorat qilish jarayonlarida AI algoritmlari tizim samaradorligini sezilarli darajada oshiradi. Shu bilan birga, jamoaviy resurslardan optimal foydalanish va xavfsizlikni ta’minlash muammolari yangi texnologiyalar yordamida hal qilinadi. Ushbu maqolaning maqsadi — zamonaviy texnologiyalar yordamida axborot xavfsizligi tizimlarini loyihalashning asosiy tamoyillari, AI va IoT asosidagi monitoring yondashuvlari, shuningdek, real vaqtli xavfsizlikni ta’minlash usullarini tahlil qilishdir.

Sun’iy intellekt (AI) algoritmlari axborot xavfsizligi tizimlarida tahdidlarni aniqlash, foydalanuvchi harakatlarini nazorat qilish va xavfsizlik darajasini oshirish uchun keng qo‘llaniladi. AI yordamida tizimlar faoliyatni doimiy monitoring qilish, anomal holatlarni avtomatik aniqlash va real vaqt rejimida xavfsizlik choralarini joriy etish imkoniyatiga ega bo‘ladi.

AI asosida ishlaydigan yondashuvlar odatda quyidagi komponentlardan tashkil topadi:

1. Tahdidlarni aniqlash (Threat Detection)

- Mashinaviy o‘rganish (Machine Learning) va chuqur o‘rganish (Deep Learning) algoritmlari tizimdagi shubhali faoliyatni aniqlashda qo‘llaniladi.
- Masalan, foydalanuvchi odatdagi ish faoliyatidan chetga chiqqanida, AI tizimi log fayllarni tahlil qilib, anomal xatti-harakatlarni aniqlaydi.
- Autoencoder tarmoqlari yoki Convolutional Neural Networks (CNN) ma’lumotlarni tahlil qilib, normal va anormal naqshlarni farqlay oladi.

2. Foydalanuvchi harakatlarini nazorat qilish (User Behavior Monitoring)

- AI tizimlari foydalanuvchi profili va xatti-harakatlarini o‘rganadi, har bir foydalanuvchi uchun normal ish faoliyatini model qiladi.
- Shu asosda, ruxsat etilmagan kirishlar yoki shubhali harakatlar darhol aniqlanadi va tizim ma’muriga xabar beriladi.
- Bu yondashuvlar real vaqtli tahdidlarni aniqlash va foydalanuvchi identifikatsiyasini kuchaytirishga yordam beradi.

3. Predictive Security (Oldindan Bashorat Qilish)

• AI tizimlari faqat mavjud tahdidlarni aniqlash bilan cheklanmay, tarixiy ma’lumotlar va naqshlarni tahlil qilib, kelajakdagi xavf-xatarlarni oldindan bashorat qiladi.

• Masalan, AI tizimi ma’lum bir foydalanuvchi yoki IP manzilidan kelishi mumkin bo‘lgan tahdidlarni aniqlab, xavfsizlik choralarini avtomatik joriy etadi.

4. Integratsiya va avtomatlashtirish

• AI algoritmlari IoT qurilmalari, sensorlar va server loglari bilan birlashtiriladi, shu bilan tizim real vaqtli monitoring va xavfsizlik choralarini avtomatlashtirish imkoniyatiga ega bo‘ladi.

• Bu yondashuvlar yordamida tizim administratorlari faqat ogohlantirishlar va eskalatsiyalar bilan shug‘ullanadi, tizim esa doimiy ravishda xavfsizlikni ta’minlaydi.

5. AI modellari va texnologiyalar

• CNN (Convolutional Neural Networks) — xatti-harakatlarni vizual tahlil qilish va anomaliyalarni aniqlashda ishlatiladi.

• RNN (Recurrent Neural Networks) — vaqtga bog‘liq loglar va harakatlar tahlilida qo‘llaniladi.

• Autoencoderlar — normal va anomal naqshlarni o‘rganib, shubhali faoliyatni aniqlashda samarali.

• Reinforcement Learning — tizimni tahdidlarni aniqlash bo‘yicha o‘rganish va o‘zini optimallashtirish imkonini beradi.

Zamonaviy axborot xavfsizligi tizimlarida IoT (Internet of Things) qurilmalari va sensorlar nafaqat ma’lumotlarni to‘plash, balki tizimni real vaqt rejimida monitoring qilish va tahdidlarni oldindan aniqlash imkonini beradi.

AI algoritmlari bilan birlashtirilganda, IoT qurilmalari faoliyatsizlik, ruxsatsiz kirish, anomal xatti-harakatlar va tahdidlarni avtomatik aniqlash vazifasini bajaradi. Shu orqali xavfsizlik tizimi nafaqat passiv nazorat, balki proaktiv himoya imkoniyatiga ega bo‘ladi.

Smart qurilmalarni kirish punktlariga o‘rnatish: Biometrik sensorlar (barmoq izi, yuz tanish), RFID kartalar va NFC qurilmalari foydalanuvchi identifikatsiyasini avtomatik amalga oshiradi.

Har bir kirish harakati log faylga yoziladi va AI algoritmlari yordamida foydalanuvchining odatiy xatti-harakatlaridan chetga chiqqan holatlar aniqlanadi.

Shu orqali ruxsatsiz kirish yoki foydalanuvchi profilining buzilishi darhol aniqlanadi.

Ma’lumotlarni tahlil va avtomatik javob: IoT qurilmalaridan olingan ma’lumotlar AI algoritmlari orqali tahlil qilinadi. Shubhali faoliyat aniqlanganda tizim avtomatik choralar ko‘radi: foydalanuvchining ruxsati bloklanadi, qurilmalar izolyatsiya qilinadi yoki xavfsizlik protokollari ishga tushadi. Shu bilan tizim proaktiv xavfsizlikni ta’minlaydi va administratorlar faqat eskalatsiya va ogohlantirishlar bilan shug‘ullanadi.

Shu nazariy asoslar va AI yondashuvlari yordamida, tizimni loyihalashda quyidagi ikki asosiy masalani hisobga olish muhim: birinchisi – minimal narxli tizim yaratish, ikkinchisi – foydalanuvchi ruxsatlarini individualizatsiya qilish.

Bugungi kunda axborot xavfsizligi tizimlari nafaqat statik qoidalar asosida, balki sun’iy intellekt (AI) va IoT qurilmalari yordamida real vaqtli monitoring asosida samarali loyihalanmoqda. Tashqi va ichki tahdidlarni aniqlash, foydalanuvchi identifikatsiyasi va ruxsatlarni nazorat qilish jarayonlarida AI algoritmlari tizim samaradorligini sezilarli darajada oshiradi. Shu bilan birga, jamoaviy resurslardan optimal foydalanish va xavfsizlikni ta’minlash muammolari yangi texnologiyalar yordamida hal qilinadi. Ushbu maqolaning maqsadi — zamonaviy texnologiyalar yordamida axborot xavfsizligi tizimlarini loyihalashning asosiy tamoyillari, AI va IoT asosidagi monitoring yondashuvlari, shuningdek, real vaqtli xavfsizlikni ta’minlash usullarini tahlil qilishdir.

Sun’iy intellekt (AI) algoritmlari axborot xavfsizligi tizimlarida tahdidlarni aniqlash, foydalanuvchi harakatlarini nazorat qilish va xavfsizlik darajasini oshirish uchun keng qo‘llaniladi. AI yordamida tizimlar faoliyatni doimiy monitoring qilish, anomal holatlarni avtomatik aniqlash va real vaqt rejimida xavfsizlik choralarini joriy etish imkoniyatiga ega bo‘ladi.

AI asosida ishlaydigan yondashuvlar odatda quyidagi komponentlardan tashkil topadi:

1. Tahdidlarni aniqlash (Threat Detection)

• Mashinaviy o‘rganish (Machine Learning) va chuqur o‘rganish (Deep Learning) algoritmlari tizimdagi shubhali faoliyatni aniqlashda qo‘llaniladi.

• Masalan, foydalanuvchi odatdagi ish faoliyatidan chetga chiqqanida, AI tizimi log fayllarni tahlil qilib, anomal xatti-harakatlarni aniqlaydi.

• Autoencoder tarmoqlari yoki Convolutional Neural Networks (CNN) ma’lumotlarni tahlil qilib, normal va anormal naqshlarni farqlay oladi.

2. Foydalanuvchi harakatlarini nazorat qilish (User Behavior Monitoring)

• AI tizimlari foydalanuvchi profili va xatti-harakatlarini o‘rganadi, har bir foydalanuvchi uchun normal ish faoliyatini model qiladi.

• Shu asosda, ruxsat etilmagan kirishlar yoki shubhali harakatlar darhol aniqlanadi va tizim ma’muriga xabar beriladi.

• Bu yondashuvlar real vaqtli tahdidlarni aniqlash va foydalanuvchi identifikatsiyasini kuchaytirishga yordam beradi.

3. Predictive Security (Oldindan Bashorat Qilish)

• AI tizimlari faqat mavjud tahdidlarni aniqlash bilan cheklanmay, tarixiy ma’lumotlar va naqshlarni tahlil qilib, kelajakdagi xavf-xatarlarni oldindan bashorat qiladi.

• Masalan, AI tizimi ma’lum bir foydalanuvchi yoki IP manzilidan kelishi mumkin bo‘lgan tahdidlarni aniqlab, xavfsizlik choralarini avtomatik joriy etadi.

4. Integratsiya va avtomatlashtirish

• AI algoritmlari IoT qurilmalari, sensorlar va server loglari bilan birlashtiriladi, shu bilan tizim real vaqtli monitoring va xavfsizlik choralarini avtomatlashtirish imkoniyatiga ega bo‘ladi.

• Bu yondashuvlar yordamida tizim administratorlari faqat ogohlantirishlar va eskalatsiyalar bilan shug‘ullanadi, tizim esa doimiy ravishda xavfsizlikni ta’minlaydi.

5. AI modellari va texnologiyalar

• CNN (Convolutional Neural Networks) — xatti-harakatlarni vizual tahlil qilish va anomaliyalarni aniqlashda ishlatiladi.

• RNN (Recurrent Neural Networks) — vaqtga bog‘liq loglar va harakatlar tahlilida qo‘llaniladi.

• Autoencoderlar — normal va anomal naqshlarni o‘rganib, shubhali faoliyatni aniqlashda samarali.

• Reinforcement Learning — tizimni tahdidlarni aniqlash bo‘yicha o‘rganish va o‘zini optimallashtirish imkonini beradi.

Zamonaviy axborot xavfsizligi tizimlarida IoT (Internet of Things) qurilmalari va sensorlar nafaqat ma’lumotlarni to‘plash, balki tizimni real vaqt rejimida monitoring qilish va tahdidlarni oldindan aniqlash imkonini beradi.

AI algoritmlari bilan birlashtirilganda, IoT qurilmalari faoliyatsizlik, ruxsatsiz kirish, anomal xatti-harakatlar va tahdidlarni avtomatik aniqlash vazifasini bajaradi. Shu orqali xavfsizlik tizimi nafaqat passiv nazorat, balki proaktiv himoya imkoniyatiga ega bo‘ladi.

Smart qurilmalarni kirish punktlariga o‘rnatish: Biometrik sensorlar (barmoq izi, yuz tanish), RFID kartalar va NFC qurilmalari foydalanuvchi identifikatsiyasini avtomatik amalga oshiradi.

Har bir kirish harakati log faylga yoziladi va AI algoritmlari yordamida foydalanuvchining odatiy xatti-harakatlaridan chetga chiqqan holatlar aniqlanadi.

Shu orqali ruxsatsiz kirish yoki foydalanuvchi profilining buzilishi darhol aniqlanadi.

Ma’lumotlarni tahlil va avtomatik javob: IoT qurilmalaridan olingan ma’lumotlar AI algoritmlari orqali tahlil qilinadi. Shubhali faoliyat aniqlanganda tizim avtomatik choralar ko‘radi: foydalanuvchining ruxsati bloklanadi, qurilmalar izolyatsiya qilinadi yoki xavfsizlik protokollari ishga tushadi. Shu bilan tizim proaktiv xavfsizlikni ta’minlaydi va administratorlar faqat eskalatsiya va ogohlantirishlar bilan shug‘ullanadi.

Shu nazariy asoslar va AI yondashuvlari yordamida, tizimni loyihalashda quyidagi ikki asosiy masalani hisobga olish muhim: birinchisi – minimal narxli tizim yaratish, ikkinchisi – foydalanuvchi ruxsatlarini individualizatsiya qilish.

Birinchi masala-minimal narxli tizimni yaratish. Bunday tizimlarni yaratish narxi jamoaviy resurslardan foydalanish darajasiga mutanosib. Bu degani, tizim narxini minimallashtirish maqsadida tizimdan foydalanuvchilarning barchasi uchun jamoaviy resurslarni, jumladan axborotni ishlovchi va boshqa vositalardan va tizimlardan

foydalanishning dasturiy va apparat vositalarini yaratish maqsadga muvofiq hisoblanadi. Foydalanishni tashkil etishning muvaffaqiyatli tanlanishi va jamoaviy resurslarning imkoniyati tizimni, uning ishlashiga qo‘yilgan talablarning amalga oshirilishida, yaratish va ekspluatatsiya narxini yetarlicha pasaytiradi.

Jamoaviy resurs imkoniyatlaridan foydalanib axborotni ishlash, bu imkoniyatlardan har bir foydalanuvchi foydalana olishi shart degani emas. Foydalanuvchanlik tizim yaratilishida ifodalangan qoidalar (talablar) orqali aniqlanadi. Tizimdan foydalanuvchilarni alohida sinflarga ajratishda aynan ushbu qoidalarga rioya qilish ikkinchi masalani yechish lozimligini oldindan belgilaydi, ya’ni axborotni uzatish va ishlash jarayonini shunday tashkil etish kerakki, har bir foydalanuvchi faqat unga ruxsat etilgan axborotni olsin. Ravshanki, har bir tizimdan foydalanuvchi uchun resursni individuallashtirish ikkinchi masalaning optimal yechimi hisoblanadi, ammo axborotni ishlash tizimini yaratish va ekspluatatsiya narxi yetarlicha oshadi. Aynan, shu nuqtai nazardan birinchi va ikkinchi masalalar maqsadida ziddiyat mavjud.

Axborotni ishlovchi kompyuter tizimlarining xavfsizligi deganda tizim bilan muloqot jarayonida axborot resurslariga zarar yetkazish urinishlariga qarshilik qilish qobiliyati tushuniladi. Bunday xavfsizlikka ishlanuvchi axborot konfidensialligini hamda o‘rnatilgan qoidalarga muvofiq tizim komponentlari va resurslarining yaxlitligini va foydalanuvchanligini ta’minlash evaziga erishiladi.

Kompyuter tizimlarining tashqi va ichki xavfsizligi farqlanadi.Tashqi xavfsizlik tizimni tabiiy ofatdan, niyati buzuqning tizimning alohida komponentini o‘g‘irlash, axborot eltuvchilardan foydalanish yoki tizimni ishdan chiqarish maqsadida, tashqaridan suqilib kirishidan himoyalashni ko‘zda tutadi. Ichki xavfsizlikning maqsadi tizimning ishonchli va to‘g‘ri ishlashini, uning dasturlari va ma’lumotlari yaxlitligini ta’minlash hisoblanadi. Hozirda kompyuter tizimlarining ichki xavfsizligini taminlashda ikkita yondashish ma’lum-fragmentar va kompleks. Fragmentar yondashish ma’lum sharoitlarda ma’lum tahdidlarga qarshi turishni ko‘zda tutadi. Bunday yondashishga misol sifatida ixtisoslashtirilgan antivirus vositalarini, qaydlash va boshqarishning alohida tadbirlarini, shifrlashning avtonom vositalarini va h. ko‘rsatish mumkin. Fragmentar yondashishning asosiy xususiyati (bir vaqtning o‘zida asosiy kamchiligi) axborotni ishlashning yagona himoyalangan muhitining mavjud emasligi.

Fragmentar yondashishning afzalligi uning muayan tahdidga nisbatan yuqori tanlash xususiyati va berilgan yo‘nalishdagi harakatlarning samaradorligi. Ammo tahdidning hatto ozgina o‘zgarishi himoya samaradorligining yo‘qolishiga olib keladi. Lokal tadbirlar ta’sirini butun tizimga darhol tarqatish amaliy jihatdan mumkin emas. Kompleks yondashishning xususiyati-tarkibida tahdidlarga qarshi turuvchi huquqiy, tashkiliy, dasturiy-apparat tadbirlar mavjud axborotni ishlashning himoyalangan muhitini yaratish. Axborotni ishlashning himoyalangan muhiti axborotni ishlash jarayonining reglamenti asosida shakllantiriladi. Himoyalangan muhitni tashkil etish,

qabul qilingan xavfsizlik siyosati doirasida, tizimni himoyalashning zaruriy darajasini kafolatlash imkonini beradi.

Kompleks yondashishdan ko‘pchilik foydalanuvchi davlat yoki tijorat tizimlarda ham, muhim iqtisodiy, siyosiy va harbiy axborotni ishlovchi nisbatan katta bo‘lmagan tizimlarda ham foydalaniladi. Ruxsatsiz foydalanilishdan himoyalangan kompyuter tizimi loyihalanuvchi ob’ekt sifatida murakkab tizim hisoblanadi. U quyidagi murakkab tizimga xos muhim xususiyatlarga ega: boshqarishning yagona maqsadi -kompyuter tizimining axborot xavfsizligi rejimida ishlashini ta’minlash; ko‘pgina avtonom qismtizimlarga dekompozitsiyalanish imkoniyati; qismtizimlarning guruhlanishi va tobelikning bir necha sathlariga ega ierarxik qurilishi; markazlashtirilishining yuqoriligi; tashqi ta’sirlarning tasodifiy xarakterligi bilan bog‘liq tizim ishlashining murakkabligi.

Himoya tizimini loyihalash-iteratsion muolaja, umumiy holda, quyidagi muolajalarni o‘tkazishni ko‘zda tutadi: himoyalanuvchi kompyuter tizimi funksional xarakteristikalarini tahlillash; bo‘lishi mumkin bo‘lgan buzilishlar modelini shakllantirish; bo‘lishi mumkin bo‘lgan ruxsatsiz foydalanish kanallarini aniqlash va tahlillash; axborotni himoyalashning dasturiy ta’minotini tanlash yoki ishlab chiqish uchun talablarni shakllantirish; axborotni himoyalash tizimini tanlash; axborotni himoyalash tizimi (AHT) samaradorligini baholash; himoyalanganlikni baholash asosida oldingi bosqichlarda shakllantirilgan talablarga aniqlik kiritish.

Axborotni ishlash texnologiyasi, tarkibida himoyalashning dasturiy-apparat vositalari va axborotni himoyalash bo‘yicha umumiy talablarning bajarilishini ta’minlovchi tashkiliy tadbirlar mavjud bo‘lsa, himoyalangan hisoblanadi.

Umumiy talablar quyidagilarni ko‘zda tutadi:

- avtomatlashtirilgan tarzda ishlanishi lozim bo‘lgan konfidensial axborotlar ro‘yxatining mavjudligi;

- ma’lum (yaratilgan) javobgar qism bo‘limning mavjudligi.

Ushbu qism bo‘limga axborotni ximoyalash texnologiyasini joriy etish, axborotning himoyalanganligi darajasini nazoratlash buyicha vakolatlar taqdim etiladi;

- kompyuter tizimining ishlashi mobaynida axborotni himoyalashni ta’minlashga mo‘ljallangan tashkiliy va injenertexnik tadbirlar, dasturiy-apparat vositalari majmui hisoblanuvchi AHTni yaratish;

- Kompyuter tizimidagi AHTning axborotni himoyalash bo‘yicha me’yoriy hujjatlarga mosligi attestatining mavjudligi;

- AHT vositalari yordamida foydalanuvchilar vakolatlarining bir necha ierarxik sathlarini va axborotning bir necha tasnifiy sathlarini aniqlash imkoniyati;

-kompyuter tizimidagi barcha foydalanuvchilar va ularning konfidensial axborotga nisbatan harakatlari qaydlanishi shart;

- foydalanuvchilarga kompyuter tizimida ishlanuvchi konfidensial axborotdan, faqat xizmat zaruriyati sharoitida, ruxsatli va nazoratlanuvchi foydalanishni taqdim etish imkoniyati;

- kompyuter tizimidagi konfidensial axborotning ruxsatsiz va nazoratsiz modifikatsiyalanishi taqiqlanadi; - AHT yordamida funksional masalaning yechilishi natijasidagi ma'lumotlarni, tarkibida amal qilinuvchi hujjatlarga muvofiq konfidensial axborot bo'lgan, chop etilgan hujjat shaklida hisobga olishni amalga oshirish;

- konfidensial axborotni ruxsatsiz nusxalash, ko'paytirish, elektron shaklda tarqatish taqiqlanadi;

- AHT yordamida konfidensial informatsiyaning ruxsatli nusxalanishini, ko'paytirilishini, elektron shaklda tarqatilishini nazoratlash;

-har bir ro'yxatga olingan foydalanuvchini bir ma'noli identifikatsiyalashni va autentifikatsiyalashni amalga oshirish imkoniyati;

- AHTning ro'yxatga olingan kompyuter tizimlaridan foydalanuvchilarining konfidensial axborotdan o'z vaqtida foydalanishlari imkoniyatini ta'minlash.

Yuqorida keltirilgan talablar bazaviy hisoblanadi va turli xil kompyuter tizimlarida axborotni ruxsatsiz foydalanishdan himoyalashda ishlatiladi.

Foydalanishni boshqarish qismtizimi quyidagi talablarni qondirishi lozim:

- tizimga kirishda foydalanuvchi sub'ektlarni identifikatsiyalash va ularning xaqiqiyligini tekshirish;

- terminallarni, kompyuter tarmog'i uzellarini, aloqa kanal larini, tashqi qurilmalarni, ularning mantiqiy adresi (nomeri) bo'yicha identifikatsiyalash;

- dasturlarni, tomlarni, kataloglarni, fayllarni, yozuvlarni va yozuv hoshiyalarini ularning nomi bo'yicha identifikatsiyalash;

- foydalanish matritsasiga muvofiq sub'ektlarning himoya lanuvchi resurslardan foydalanishlarini nazoratlashni amalga oshirish.

Ro'yxatga va hisobga olish qismtizimi quyidagi talablarni qondirishi lozim:

- foydalanuvchi sub'ektlarning tizimga kirishini (tizimdan chiqishini) yoki operatsion tizimni yuklash va ishga tushishini va uning dasturiy to'xtatilishini ro'yxatga olish;

- chop etilgan hujjatlarning "qattiq" nusxaga o'tkazilishini ro'yxatga olish;

- himoyalanuvchi faylarni ishlashga mo'ljallangan dasturlarni va jarayonlarni ishga tushirilishini (tugallanganligini) ro'yxatga olish;

- dasturiy vositalarning (dasturlar, jarayonlar, topshiriqlar, masallalar) himoyalanuvchi fayllardan foydalanishga urinishlarini ro'yxatga olish;

- dasturiy vositalarning foydalanuvchi qo'shimcha himoyalanuvchi ob'ektlardan, (terminllardan, tarmoq uzellaridan, aloqa kanallaridan, tashqi qurilmalardan, dasturlardan, fayllardan va h.) foydalanishga urinishlarini ro'yxatga olish;

- barcha himoyalanuvchi axborot eltuvchilarni, ularning belgilari yordamida jurnallarda qaydlash yo'li bilan hisobga olish;

- himoyalanuvchi axborot eltuvchilarni taqdim etishda ro'yxatga olish;

- asosiy xotira va tashqi to'plagichlarda bo'shagan zonalarni tozalashni amalga oshirish.

Yaxlitlikni ta'minlash qismtizimi quyidagi talablarni qondirishi lozim:

- АНТ dasturiy vositalarining yaxlitligini, ishlanuvchi axborotni ruxsatsiz foydalanishdan himoyalash, hamda dasturiy muhitning o‘zgarmasligini ta’minlash;

dasturiy muhit va kompyuter tizimi xodimi o‘zgarganida АНТ funksiyalarini, ruxsatsiz foydalanishini imitatsiyalovchi test-dasturlar yordamida, davriy testlash;

- ruxsatsiz foydalanishdan himoyalash tizimlarini tiklash vositalarining mavjudligi. Bunda ruxsatsiz foydalanishdan himoyalashning dasturiy vositalarining ikkita nusxasini yuritish, hamda ularni davriy yangilash va ishga layoqatligini nazoratlash ko‘zda tutiladi.

Yuqorida keltirilgan barcha mexanizmlar eng muhim hisoblanadi. Ular quyidagicha o‘zaro bog‘langan: resurslardan foydalanishning barcha huquqlari (resurslardan foydalanishning cheklangan siyosati) foydalanishning muayyan sub’ektiga beriladi. Shu sababli, sub’ekt tizimga kirishida identfikatsiyalanishi va uning xaqiqiyligi nazoratlanishi lozim.

АДАБИЁТЛАР:

1. Гайдамакин Н.А. Теоретические основы компьютерной безопасности:учеб. пособие. Екатеринбург: изд-во Уральского университета, 2008. - С. 212.

2. Гайдамакин Н. А. Разграничение доступа к информации в компьютерных системах. Екатеринбург: изд-во Уральского университета, 2003.-С.328.

3. Галатенко В. А. Основы информационной безопасности. Учеб. пособие:под ред. В. Б. Бетелина.-4-е изд. М.:Интернет-Университет Информационных Технологий; БИНОМ. Лаборатория знаний, 2008. -С. 205

4. Irgasheva D.Y., Abramov A.S. Access control policy subjects to objects in distributed Information and Communication systems//2013 International Conference in Central Asia on Internet (ICI 2013, 8th-10th of October).

7. Мирзаева М. Б., Абдазимов С. З. Использование технологий искусственного интеллекта в сфере высшего образования. – 2022.

8. S.Z.Abdazimov. Ijtimoiy tarmoqlarda axborot xurujlarini tarqalish ehtimolligini bashoratlash va ulardan himoyalash usuli va modellari //Central Asian Research Journal for Interdisciplinary Studies (CARJIS). – 2022. – Т. 2. – №. 5. – С. 109-115.