ISSN: 2181-3906 2025

International scientific journal
«MODERN SCIENCE AND RESEARCH»
VOLUME 4 / ISSUE 4 / UIF:8.2 / MODERNSCIENCE.UZ

TELEKOMMUNIKATSIYA TARMOQLARIGA BO‘LADIGAN HUJUMLARNI ANIQLASH VA OLDINI OLISHNING ZAMONAVIY YECHIMLARI

Alimardon Axmedov Muhiddin o'g'li
University of Management and Future Technologies
Telekommunikatsiya injiniringi magistranti

https://doi.org/10.5281/zenodo.15206109

Annotatsiya. *Ushbu maqolada O‘zbekiston Respublikasidagi davlat tashkilot va korxonalarida Axborot xavfsizlik monitoring markaz (Security operation center-SOC)larini joriy qilish istiqbollari hamda bu orqali kiberxavfsizlikni ta’minlashda erishiladigan natijalarni tahlil qilish ko‘zda tutilgan.*

Bunda zamonaviy telekommunikatsiya tarmoqlari va axborot tizimlari orqali uzatiladigan xizmatlari uzluksizligini hamda ularning kiberxavfsizligini ta’minlash maqsadida eng zamonaviy yechimlar tahlil qilingan.

Tadqiqot davomida davlat tashkilot va korxonalarida telekommunikatsiya infrastrukturasi apparat, dasturiy va apparatli-dasturiy vositalari xavfsizligini ta’minlash uchun axborot tizimining zamonaviy vositalar, funksional va tuzilmaviy ta’minotini monitoring qilishgacha bo‘lgan jarayonlar e’tiborga olingan.

Kalit so‘zlar: *telekommunikatsiya, tarmoq, aloqa, monitoring, server, xosting, tizim, dasturiy ta’minot, axborot tizimi, kiberxavfsizlik, kibertahdid, avtomatlashtirish, tizim samaradorligi, dasturiy vositalar, komplekslashgan axborot tizimi, AXMM (Axborot xavfsizlik monitoring markazi).*

MODERN SOLUTIONS FOR DETECTION AND PREVENTION OF ATTACKS ON TELECOMMUNICATION NETWORKS

Abstract. *This article provides an analysis of the prospects for the introduction of Information Security Monitoring Centers (Security Operation Center-SOC) in state organizations and enterprises in the Republic of Uzbekistan and the results achieved through this in ensuring cybersecurity.*

In this regard, the most modern solutions were analyzed to ensure the continuity of services transmitted through modern telecommunication networks and information systems and their cybersecurity.

During the study, the processes of ensuring the security of hardware, software and hardware-software tools of the telecommunication infrastructure in state organizations and

enterprises, up to monitoring of modern tools, functional and structural support of the information system, were taken into account.

Keywords: *telecommunications, network, communication, monitoring, server, hosting, system, software, information system, cybersecurity, cyber threat, automation, system efficiency, software tools, integrated information system, AXMM (Information Security Monitoring Center).*

СОВРЕМЕННЫЕ РЕШЕНИЯ ДЛЯ ОБНАРУЖЕНИЯ И ПРЕДОТВРАЩЕНИЯ АТАК НА ТЕЛЕКОММУНИКАЦИОННЫЕ СЕТИ

Аннотация. *Целью данной статьи является анализ перспектив внедрения Центров мониторинга информационной безопасности (ЦМИБ) в государственных организациях и предприятиях Республики Узбекистан и достигнутых при этом результатов в обеспечении кибербезопасности.*

Проанализированы самые современные решения для обеспечения непрерывности услуг, передаваемых через современные телекоммуникационные сети и информационные системы, а также их кибербезопасности.

В ходе исследования были рассмотрены процессы от мониторинга современных средств, функционального и структурного обеспечения информационной системы до обеспечения безопасности аппаратных, программных и программно-аппаратных средств телекоммуникационной инфраструктуры государственных организаций и предприятий.

Ключевые слова: *телекоммуникации, сеть, связь, мониторинг, сервер, хостинг, система, программное обеспечение, информационная система, кибербезопасность, киберугроза, автоматизация, эффективность системы, программные средства, интегрированная информационная система, AXMM (Центр мониторинга информационной безопасности).*

Global taraqqiyot sharoitida axborot texnologiyalari mohiyatini oshirishning yanada zamonaviy, innovatsion usullarini izlab topish, axborotlashtirish jarayoniga har tomonlama ko‘maklashish, ularni hayotga keng joriy etish davlat faoliyatining muhim yo‘nalishlaridan biriga aylanmoqda. Zero, axborotlashtirish tizimida davlat siyosatini olib borish masalasi strategik ahamiyatga ega vazifadir. Shubhasiz, davlat va jamiyat -boshqaruvi, biznes, fuqarolik jamiyati kommunikatsiyalari samaradorligi - axborotlashtirish, zamonaviy axborot texnologiyalarining ushbu sohalarga kirib borishi darajasi bilan uzviy bog‘liq.

Mamlakatimiz istiqlolni qo‘lga kiritgan davr fan-texnika inqilobining muhim bosqichiga to‘g‘ri keldi. O‘shanda kompyuterlarni keng miqyosda ishlab chiqarishning global to‘lqini kuzatilgandi. Shunga hamohang ravishda yurtimiz o‘z mustaqilligi salohiyatidan foydalangan holda, ijtimoiy-iqtisodiy islohotlarni amalga oshirishning “o‘zbek modeli” tamoyillariga asoslanib, davrning innovatsion talablariga har tomonlama mos javob bera oldi. O‘z navbatida, barqaror taraqqiyotning mustahkam asosi sanalgan milliy axborot makoni yaratildi.

Prezidentimiz tomonidan tasdiqlangan “Raqamli O‘zbekiston – 2030” strategiyasi doirasida yurtimizda axborotlashtirish sohasini jadal rivojlantirishda muhim dasturilamal bo‘ldi.

Unda nafaqat mamlakatni axborotlashtirishni yanada ravnaq toptirishning ustuvor yo‘nalishlari belgilab berildi, balki har bir davlat tashkilotlari o‘z qamrovida axborot kommunikatsiya texnologiyalarini joriy qilishlari uchun asosiy yo‘l xaritasi hisoblanadi.

Rivojlangan mamlakatlar raqamli transformatsiyaning to‘liq va xavfsiz ishlab turish tajribasi shuni ko‘rsatmoqdaki, axborotlashtirish tizimlari uzluksiz ishlashi va xavfsizligini ta’minlash uchun avtomatlashtirilgan axborot xavfsizligini ta’minlash mo‘ljallangan qurilma va vositalar amaliyotga keng joriy qilingan. Bunday tuzilmalar Germaniya, Janubiy Koreya, Yaponiya, Avstraliya, Singapur va boshqa ko‘plab davlatlarda mavjud bo‘lib, samarali faoliyat yuritmoqda. Boisi, axborot xavfsizligini ta’minlashda avtomatlashtirilgan tizimlarni qo‘llash kompleks hamda ko‘p tarmoqli jarayondir. Shunday ekan, davlat sektori, biznes tuzilmalari va fuqarolik jamiyati institutlarining axborot xavfsizligini ta’minlash darajasini oshirish, jamiyat hamda davlat tashkilotlarining barcha sohasiga ilg‘or xavfsizligini ta’minlashda avtomatlashtirilgan tizimlarni keng joriy qilish bo‘yicha sayharakatlarni muvofiqlashtirishga qaratilgan chora-tadbirlarni amalga oshirish yuqoridagi kabi davlat organlari faoliyatining eng asosiy vazifalari hisoblanmoqda.

O‘zbekiston Respublikasi Prezidenti tomonidan olib borilayotgan islohotlar natijasida raqamli transformatsiyaning qamrovi tobora ortib bormoqda, bu esa IT infratuzilmaning xavfsizligini ta’minlashga bo‘lgan talab ham parallel ravishda o‘sib bormoqda.

Bugungi kunga kelib mamlakatimiz IT infratuzilmasini barqaror, uzluksiz va xavfsiz faoliyatini ta’minlash ustuvor vazifalardan biri ekanligi hozirgi kunda barchamizga kundek ravshan bo‘lib ulgurdi. Ushbu vazifani ta’minlash maqsadida esa axborot xavfsizligini ta’minlash yoki kiberxavfsizlikka bevosita javobgar bo‘lgan tashkilot va korxonalar tomonidan bir qator yangiliklar keng tadbiq qilinmoqda, lekin tizim to‘liq avtomatlashtirilmaguniga qadar

ichki va tashqi xavf-xatarlarni sezilarli darajada kamaytirish ishlari samara bermasligi yaqqol namoyon bo‘lib bormoqda.

Yuqorida keltirtilgan muammolardan ko‘rinib turibtiku raqamli infratuzilmani kibertahdidlardan samarali va munosib himoya qilish va uzluksiz ishlashini ta’minlash uchun jahon tajribasi asosida quyidagi vazifalarni belgilab olishimiz kerak bo‘ladi.

Bularga:

1. Raqamli infratuzilmani himoya qilish;
2. Tahdidlarni aniqlash va ularga javob berish;
3. Zaifliklarni bartaraf etish;
4. Kibertahdidlar bo‘yicha razvetka olib borish;
5. Xalqaro hamkorliklarni yo‘lga qo‘yish;
6. Kiberxavfsizlik bo‘yicha talim va ilmiy salohiyatni rivojlantirish.

Belgilab olingan vazifalar asosida quyidagi chora-tadbirlarni olib borish imkoniyati yuzaga keladi.

- *Raqamli infratuzilmani kibertahdidlardan himoya qilish* -telekommunikatsiya tarmoqlari va axborot tizimlari hamda ma’lumotlar bazasini himoya qilish, ularning yaxlitligi va butunligini ta’minlashdan iborat;

- *Tahdidlarni aniqlash va ularga javob berish* - potensial kiber hujumlarni aniqlash uchun doimiy monitoring ishlarini olib borish, tarmoq trafigi, tizim jurnal(log)lari va boshqa ma’lumotlar manbaalarini sinchikovlik bilan o‘rganish orqali yaqin kelajakda bo‘lishi mumkin bo‘lgan kiberhujumlarni aniqlash va tahlil qilish. Kiberhujum sodir bo‘lgan taqdirda ularning ta’sirini minimallashtirish va javob choralarini ko‘rish kerak bo‘ladi;

- *Zaifliklarni bartaraf etish* – raqamli infratuzilmada aniqlangan zaifliklarni o‘z vaqtida bartaraf etish va zaiflik aniqlangan tizimlarni tahlil qilish orqali infratuzilma chidamliligini oshirish hamda kiberxurujlar zarar miqdorini minimallashtirishdan iborat;

- *Kiber razvetka harakatlarini olib borish* – kibertahdidlar bo‘yicha ochiq va yoqip manbalarga asoslangan ma’lumotlarni to‘plash va tahlil qilish orqali xalqaro tajribaga asosan infratuzilma xavfsizlik darajasini baholash imkoni vujudga keladi;

- *Xalqaro hamkorliklarni yo‘lga qo‘yish* – kiberxavfsizlik sohasida xalqaro tajriba suv va havoday muhim yo‘nalish hisoblanib doimiy ravishta hodimlarni tajriba almashishlari, maxsus malaka va xalqaro tajriba ortirish maydoni yaratiladi;

- *Kiberxavfsizlik bo'yicha ta'lim va ilmiy salohiyatni rivojlantirish* – mutaxassislar salohiyatini oshirish va milliy kadrlar zaxirasi yaratish uchun asosiy tizim bo'lib xizmat qiladi, bunda ko'plab ilmiy ishlar va konstruktorlik ishlanmalarini amalga oshirish sezilarli darajada yangililar olib kelishiga erishish mumkin bo'ladi.

Olib borilgan o'rganishlar va tahlillar natijasida kibertahdidlardan hech bir tarmoq yoki tizim to'laqolni himoyalanmaganligini ko'rishimiz mumkin va kibermudofaa esa monitoring va kiberrazvetkaga asoslanganligini ko'rishimiz mumkin bo'ladi. Bu esa o'z navbatida avtomatlashtirilgan tizimlar orqali kam ishchi kuchi sarflab ko'proq natija olishni anglatadi.

- Telekommunikatsiya tizimlariga amalga oshirilayotgan kiber hujumlarni aniqlash uchun bir nechta usullar va algoritmlar qo'llaniladi. Bu usullar odatda kiberxavfsizlik texnologiyalariga asoslangan bo'lib, har xil kiberhujumlarni oldindan bilish, kuzatish va oldini olish imkonini beradi. Ushbu maqolada quyidagi kiberhujumlarni aniqlash usullarini ko'rib chiqamiz:

- imzo asosida aniqlash (Signature-Based Detection);
- anomaliya asosida aniqlash (Anomaly-Based Detection);
- xatti-harakatlar tahlili (Behavioral Analysis);
- o'rganishga asoslangan aniqlash (Machine Learning-Based Detection);
- xavfsizlik devorlari va IDS/IPS tizimlari;
- Deep Packet Inspection (DPI);
- yolg'on pozitivlarni kamaytirish (False Positive Reduction);
- hujumlarni bashorat qilish tizimlari (Predictive Analytics).

Imzo bo'yicha aniqlash - kiberxavfsizlikda keng tarqalgan yondashuv bo'lib, u hujumlarni aniqlash va ularga qarshi kurashda asosiy rol o'ynaydi. Ushbu usul avvaldan ma'lum bo'lgan kiberhujumlarni aniqlash uchun imzolarni ishlatadi.

Imzo asosida aniqlash tizimlari 1990-yillarda keng tarqaldi. Tizimlar tarmoq trafigini oldindan belgilangan hujum imzolari bilan taqqoslab, kiberhujumlarni aniqlay boshladi.

Imzo - bu zararli dastur, xakerlik usuli yoki kiberhujumlarning o'ziga xos xususiyatlari, masalan, kod uziga xos belgilari yoki harakatlar.

Dastlab zararli dasturlar hamda kiberhujumlar to'planiladi va tahlil qilinadi, tahlil jarayonida ularning kodlari, xatti-harakatlari va kirish xarakatlari o'rganiladi.

Tahlil natijasida olingan ma'lumotlar asosida imzo yaratiladi. Bu imzo, masalan, kodning bir qismi yoki dasturga xos bo'lgan muayyan xatti-harakatlar bo'lishi mumkin.

Anomaliya asosida aniqlash (Anomaly-Based Detection) - bu kiberxavfsizlikda ishlatiladigan hujumni aniqlash usuli bo‘lib, tizim yoki tarmoqdagi normal xatti-harakatlardan chetga chiqishni kuzatib, hujumlarni yoki zararli faoliyatlarni aniqlaydi. Bu usul imzo asosidagi aniqlashdan farqli ravishda, avvaldan ma’lum bo‘lmagan hujumlarni ham aniqlash qobiliyatiga ega, chunki u tizimning odatiy xatti-harakatlarini kuzatadi va ularni aniq model bilan solishtiradi.

Xatti-harakatlarni tahlil qilib aniqlash (Behavioral Analysis) - bu kiberxavfsizlikda ishlatiladigan texnologiya bo‘lib, foydalanuvchilar yoki tizimning odatiy faoliyatini tahlil qilish orqali nomaqbul yoki zararli xatti-harakatlarni aniqlashni maqsad qiladi. Bu yondashuv odatda hujumlarni anomaliya asosida aniqlash tizimlariga yaqin va u foydalanuvchilarning yoki dasturlar, tarmoq va qurilmalarning odatdagi faoliyatini kuzatadi.

O‘rganishga asoslangan aniqlash (Machine Learning-Based Detection) - kiberxavfsizlikda hujumlarni yoki nomaqbul faoliyatni aniqlash uchun sun’iy intellekt va mashina o‘rganish (ML) texnologiyalaridan foydalanadigan usuldir. Ushbu yondashuv odatdagi xatti-harakatlarni avtomatik ravishda o‘rganib, yangi tahdidlarni aniqlashda an’anaviy usullardan ancha samarali bo‘liadi. Mashina o‘rganishning asosiy maqsadi tizim yoki tarmoqdagi hujumlarni o‘z vaqtida aniqlash uchun avtomatik ravishda yangi hujumlarni va o‘zgarishlarni tushunishidir.

Xavfsizlik devorlari (Firewalls) va IDS/IPS tizimlari - kiberxavfsizlik infratuzilmasida muhim rol o‘ynaydigan vositalar bo‘lib, ular tarmoqni himoya qilish, hujumlarni aniqlash va ularga qarshi chora ko‘rish uchun ishlatiladi. Ularning vazifalari bir-biriga o‘xshash bo‘lsa-da, ishlash prinsiplari va funktsional farqlari mavjud.

Tarmoqlararo ekran - himoyalash vositasi bo‘lib, ishonchli tarmoq va ishonchsiz tarmoq orasida ma’lumotlarga kirishni boshqarishda qo‘llaniladi. Tarmoqlararo ekran ko‘p komponentli bo‘lib, u internetdan tashkilotning axborot zahiralarini himoyalash strategiyasi sanaladi. Ya’ni tashkilot tarmog‘i va internet orasida qo‘riqlash vazifasini bajaradi. Tarmoqlararo ekranning asosiy funksiyasi ma’lumotlarga egalik qilishni markazlashtirilgan boshqaruvini ta’minlashdan iborat. Tarmoqlararo ekran quyidagi himoyalarni amalga oshiradi:

IDS (Intrusion Detection Systems) va IPS (Intrusion Prevention Systems) tarmoqda yoki tizimda nomaqbul va zararli faoliyatni aniqlash va bartaraf etishga mo‘ljallangan tizimlardir.

IDS (Intrusion Detection System) - ruxsatsiz kirishni aniqlash tizimi yordamida tizim yoki tarmoq xavfsizlik siyosatini buzib kirishga harakat qilingan usul yoki vositalar aniqlanadi.

Ruxsatsiz kirishlarni aniqlash tizimlari deyarli chorak asrlik tarixga ega. Ruxsatsiz kirishlarni aniqlash tizimlarining ilk modellari va prototiplari kompyuter tizimlarining audit ma’lumotlarini tahlillashdan foydalangan. Bu tizim ikkita asosiy sinfga ajratiladi. Tarmoqqa ruxsatsiz kirishni aniqlash tizimi (Network Intrusion Detection System) va kompyuterga ruxsatsiz kirishni aniqlash tizimiga (Host Intrusion Detection System) bo‘linadi.

IPS (Intrusion Prevention System) - bu kompyuter tizimlari yoki tarmoqlarida yuz berayotgan hodisalarni kuzatish va kompyuter xavfsizligi siyosati yoki standart xavfsizlik qoidalarini buzishga olib keladigan holatlarning tahlili bilan birgalikda aniqlangan holatlarni to‘xtatishga, hujumlarga qarshi javob qaytarish qobiliyatli harakatlar yig‘indisidir. IPS texnologiyasi IDS texnologiyasini mustaqil ravishda nafaqat xavfni aniqlabgina qolmay, balki uni muvaffaqiyatli bloklashi bilan to‘ldiradi. Ushbu taxminiy IPS funktsiyasi IDS ga qaraganda ancha kengroq:

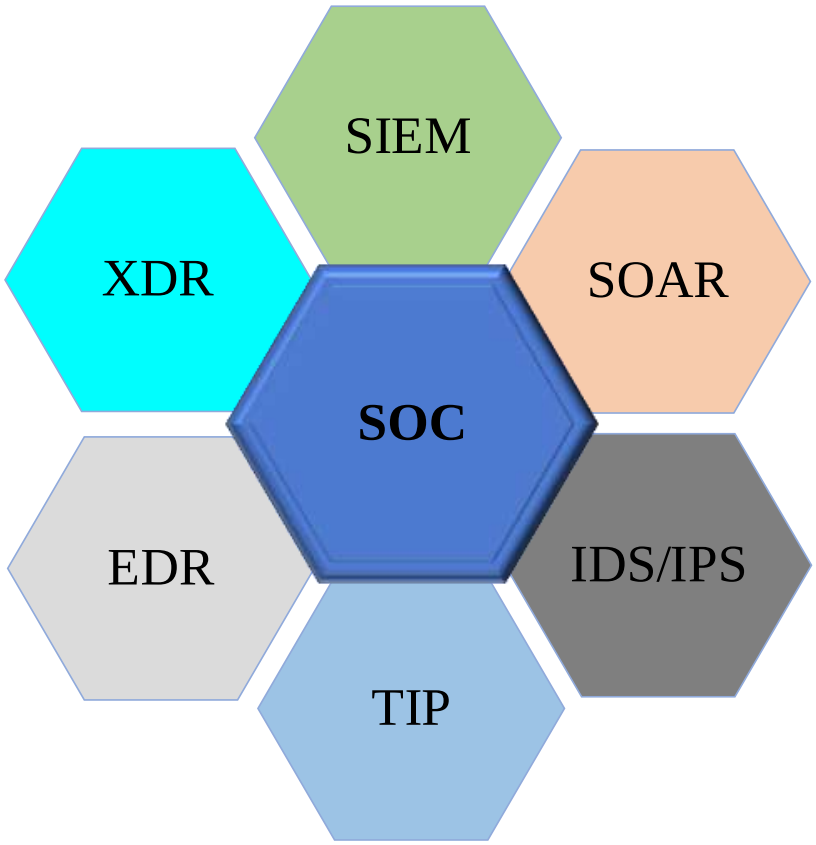
Deep Packet Inspection (DPI) - bu tarmoq trafigini chuqur tahlil qilish usuli bo‘lib, u paketlarning sarlavhasini (header) emas, balki butun mazmunini (payload) ham tahlil qiladi.

Oddiy xavfsizlik devorlari yoki marshrutizatorlar faqat paketlarning sarlavhasini tekshirib, qaysi manzildan qaysi manzilga ketayotganini aniqlaydi. DPI esa paket ichidagi ma’lumotlarni, ya’ni real trafikning mazmunini chuqurroq o‘rganib, paketlarning haqiqiy maqsadini aniqlashga imkon beradi.

Yolg‘on pozitivlarni kamaytirish (False Positive Reduction) - bu kiberxavfsizlik tizimlari, ayniqsa, intruziyani aniqlash va oldini olish tizimlari (IDS/IPS), shuningdek anomaliya asosida aniqlash va imzo bo‘yicha aniqlash usullarida juda muhim vazifadir. Yolg‘on pozitiv - bu xavfsizlik tizimi tomonidan hujum yoki xavf sifatida noto‘g‘ri tasniflangan, ammo aslida zararli bo‘lmagan qonuniy faoliyat yoki trafikdir.

Hujumlarni bashorat qilish tizimlari (Predictive Analytics) - bu xavfsizlik ma’lumotlarini oldindan tahlil qilish orqali kelajakdagi kiberxavf yoki hujumlarni prognoz qilish va oldini olishga qaratilgan usullardir. Predictive analytics texnologiyasi kiberxavfsizlikda hujumlar sodir bo‘lishidan oldin potentsial tahdidlarni aniqlash va hujumlarni bartaraf etishga imkon beradi.

Telekommunikatsiya tarmoqlariga bo‘ladigan hujumlarni aniqlash va oldini olishning eng zamonaviy yechimlaridan biri bu Axborot xavfsizlik monitoring markazi (**SOC -** Security Operations Center) yutuqlari va kamchiliklarini tahlil qilib chiqamiz. AXMM kiberxavfsizlikni ta’minlashda kompleks va avtomatlashtirilgan yondashuv tizimi hisoblanadi.



1-rasm. Axborot xavfsizlik monitoring markazi(SOC)ning asosiy elementlari.

Axborot xavfsizlik monitoring markazining asosiy elementlari sifatida quyidagilarni keltirib o‘tishimiz mumkin(1-rasm):

1. Axborot xavfszligi va hodisalarni boshqarish (**SIEM** - Security Information and Event Management);
2. Xavfsizlikni tartibga solish, avtomatlashtirish va javob berish (**SOAR** - Security orchestration, automation and response);
3. Hujumlarni aniqlash va ularning oldini olish tizimi (**IDS/IPS** - Intrusion Detection Systems and Intrusion Prevention Systems);
4. Kengaytirilgan(xavflarni) aniqlash va javob berish (**XDR** – Extended Detection and Response);
5. Oxirgi nuqtani aniqlash(xavflarni) va javob berish (**EDR** - Endpoint Detection and Response);
6. Tahdidlarni razvetka qilish platformasi (**TIP** - Threat Intelligence Platforms).

Ushbu tizim va platformalar Axborot xavfsizlik monitoring markazining asosiy va fundamental o‘zagi hisoblanadi, boshqa turdagi qo‘shimcha elementlar esa yordamchi vazifalarni bajarishda xizmat qiladi.Tizimni joriy qilmoqchi bo‘lgan tashkilot yoki korxona tarmoq masshtabi hamda joylashuv tuzilmasiga qarab elementlarni boyitishi yoki kamaytirishi mumkin bo‘ladi.

Axborot xavfsizlik monitoring markazi tarmoqdagi tahdidlarning turli shakllariga chidamliligini ta’minlashga yordam beradi. Quyida Axborot xavfsizlik monitoring markazining xavfsizlikka hissa qo‘shish usullari ko‘rsatilgan. (1-jadval):

1-jadval.

Aspektlar	Tarmoq xavfsizligidagi roli
Monitoring	Anomaliyalar va potensial tahdidlarni erta aniqlash uchun tarmoq trafigini doimiy real vaqt rejimida kuzatish.
Hodisaga javob	Zararlangan tizimlarni izolyatsiya qilishni o‘z ichiga olishi mumkin bo‘lgan tarmoqda asoslangan tahdidlarni tezkorlik bilan to‘xtatish.
Sozlamalar boshqaruvi	Xavfsizlik devorlari, IDS va IPS kabi tarmoq xavfsizligi vositalarining himoyani maksimal darajada oshirish uchun to‘g‘ri sozlanganligini ta’minlash.
Tahdid razvedkasi	Xavfsizlik choralarini faol ravishda o‘zgartirish uchun paydo bo‘lgan tahdidlar haqida so‘nggi ma’lumotlardan foydalanadi.
Zaiflikni baholash	Infratuzilma zaifliklarini aniqlash va tuzatish uchun muntazam ravishda tarmoqni skanerlash.
Ro‘yxatga olish va hisobot berish	Sud-tibbiy tahlil va muvofiqlik maqsadlari uchun barcha tarmoq hodisalari va o‘sha hodisalar haqida batafsil jurnallarini yuritish.
Muvofiqlik	Tarmoqning sanoat qoidalariga rioya qilishini ta’minlaydi.
Foydalanuvchi shaxs xatti-harakatlari tahlili	Tarmoqdagi xavfsizlik muammosini ko‘rsatishi mumkin bo‘lgan g‘ayritabiiy xatti-harakatlar namunalarini tahlil qiladi.
Avtomatlashtirish va jamlash	Umumiy tahdidlarni hal qilish uchun xavfsizlikni tartibga solish, avtomatlashtirish va javob berish (SOAR) vositalaridan foydalanadi, bu esa inson(operator)larga yanada murakkab masalalarga e’tibor qaratish imkonini beradi.
Trening va xabardorlik	Xodimlarni tarmoq xavfsizligining eng yaxshi amaliyotlari bo‘yicha o‘rgatadi, kiberxavfsizlikning inson omiliga tegishli elementiga yordam beradi.

Axborot xavfsizlik monitoring markazini tadbiq etgan tashkilot kiberxavfsizlik tizimini sezilarli darajada mustahkamlaydigan ko‘plab afzalliklarni olib keladi(2-jadval). Bu yerda asosiy afzalliklardan ba’zilarini keltirib o‘tamiz:

7. 2-jadval.

Imkoniyatlari	Tavsifi
Real vaqtda monitoring	Xavfsizlikga qaratilgan tahdidlarni erta aniqlash uchun tarmoq, tizim va ma’lumot ombori ustidan **24/7** nazoratni ta’minlaydi.
Muvofiqlik	Xalqaro toifadagi muvofiqlik standartlariga javob berishga yordam beradi.
Proaktiv tahdid aniqlash	E’tibor bermay qolish mumkin bo‘lgan tahdid ko‘rsatkichlarini faol ravishda qidiradi va proaktiv xavfsizlik yondashuvini ta’minlaydi.
Kuchli hodisa(hujum)larga javob	Ixtisoslashgan guruhlarga tez va samarali javob berish uchun har bir tahdid turi uchun aniq belgilangan protokollarga amal qiladi.
Markazlashtirilgan xavfsizlik	Osonroq korrelyatsiya va hujumni aniqlash uchun bir nechta manbalardagi Ma’lumotni birlashtiradi.
Mutaxassislik	Kiberxavfsizlik turli sohalaridagi mutaxassislardan iborat bo‘lib, xavfsizlik hodisalariga qarshi kurashishda yuqori darajadagi bilim va ko‘nikmalarni ta’minlaydi.
Iqtisodiy samaradorlik	Dastlabki o‘rnatish natijasiga ko‘ra xarajatlar yuqori bo‘lsada, xavfsizlikni ta’minlash yoki xavf-xatarlarni kamaytirish nuqtai nazaridan samarali yechim hisoblanadi. Autsorsing qilingan Axborot xavfsizlik monitoring markazlari ham maqbul variant taqdim etadi.
Ma’lumotlar va biznesning uzluksizligi	Kiberhujumlarni oldini olish va bartaraf etish biznes operasiyalar xavfsizligini ta’minlashga yordam beradi. Shuningdek, Ma’lumotni zaxiralash va tiklashda yordam beradi.
Strategik qarorlar qabul qilish	Resurslarni taqsimlash va strategik rejalashtirishda yuqori boshqaruvga yordam beruvchi xavfsizlik landshafti haqida qimmatli imkoniyatlar taqdim etadi.
Ogohlantirishlarni kamaytirish	Markazlashtirilgan monitoring va aniq vazifalarga yo‘naltirish noto‘g‘ri pozitivlarni filtrlashga yordam beradi, IT xodimlari o‘rtasida "ogohlantirish signallari" maksimal darajada kamaytiriladi.

Qiyosiy tahlili.

Yuqorida keltirilgan kiberxavfsizlikni ta’minlashda zamonaviy yondashuv hisoblangan Axborot xavfsizlik monitoring markazini tahlil qilamiz ya’ni avtomatlashtirilgan tizim va avtomatlashtirilmagan (tarqoq) tadbiq qilingan tizimlarni tahlil qilish orqali, tizimlarning samaradorlik koeffitsienti, ko‘rib chiqamiz, hamda ularni quyidagicha baholab boramiz(1-jadval). Jadvaldagi belgilashlarda dasturiy va apparat dasturiy ta’minotlarni umumiy Axborot xavfsizlik monitoring markaziga bog‘langan holda hamda o‘zaro bog‘lanmagan holda kiberhodisalarni qaysi usulda va qancha vaqt oralig‘ida bartaraf etilishini turli manbalardan olingan ma’lumotlar asosida baholab boramiz va jadvalga kiritamiz.

2-jadval.

№	Imkoniyatlari	Avtomatlashtirilgan axborot xavfsizlik tizimi(AXMM)	Avtomatlashtirilmagan axborot xavfsizlik tizimi
1	Xalqaro sanoat standarti imkoniyati mavjudligi	+	+
2	Real vaqt rejimida tizimga qo‘shimchalar kirita olish imkoniyati mavjudligi	+	-
3	Boshqa turdosh dasturlar bilan integratsiyalanganligi	+	-
4	Nazorat qilinadigan qurilmalar, portlar va datchiklar son chegarasi mavjud emasligi	+	-
5	Qo‘llab-quvvatlovchi qurilmalarni avtomat qo‘shish imkoniyati mavjudligi	-	-
6	Tanlangan protokollar orqali infratuzilma kartasini tuzish	+	-
7	Ma’lum qoidalar asosida guruhlash imkoniyati mavjudligi	+	+
8	Dasturga o‘zgartirish kiritilganida umumiy infratuzilmaga ta’sir qilmasligi	-	+
9	Hodisalar haqida ogohlantirishlarini avtomatik chop etish imkoniyati mavjudligi	+	-

10	Hodisalar haqida ogohlantirishlarini tartiblash imkoniyati	+	-
11	Yuqori sifat (IP SLA ,Class-based QOS) qo‘rsatkichlari bilan ishlash imkoniyati mavjudligi	+	+
13	Qo‘llab-quvvatlash va xizmat ko‘rsatish imkoniyati mavjudligi	+	+
14	Bir nechta serverlarda nusxani parallel saqlash imkoniyati mavjudligi	+	-
15	Hodisa xususiyatlari bo‘yicha so‘rovlarni alohida ko‘rib chiqish	+	-
16	Masofaviy boshqarish protokollarini dasturiy ta’minot interfeysiga bog‘lash imkoniyati mavjudligi	+	+
17	Tarmoqdagi paket to‘qnashuvlarini ortishini oldini olish tizimi mavjudliligi	-	+
18	Bitta muammoli so‘rovni chegarasiz vaqtda qo‘llab-quvvatlash imkoniyati mavjudligi	+	+

Olingan tahlil natijalari asosida (1-jadval) har bir funksional imkoniyatlar va ularning mavjud yoki aksincha mavjud emasligiga qarab tizim va dasturiy ta’minotlarni baholab borishimiz mumkin bo‘ladi. Olingan natijalar hisoboti quyidagi jadvalda keltirilgan (2-jadval).

Tizim va dasturiy ta’minotlar imkoniyatlari bo‘yicha tahlil natijalarida faqat mavjudlari inobatga olingan.

2-jadval

№	**Axborot xavfsizlik monitoring markazi**	**Avtomatlashtirilmagan axborot xavfsizlik monitoring tizimi**
1	15	8

Tizim va dasturiy ta’minotlarga olingan natijalar asosida qo‘yidagi formula asosida baholash mezonini ishlab chiqamiz - $S(nom) = \frac{N1}{N0} * 100\%$.

$S(nom)$ – bu tizim va dasturiy ta’minotga qo‘yilgan umumiy ball,

$N1$- bu 2- jadvaldagi tizim va dasturiy ta’minot natijasi,

$N0$- bu 1- jadvaldagi tizim va dasturiy ta’minotni solishtirish uchun olingan barcha imkoniyatlar soni, uning qiymati o‘zgarmas $N0 = 18$.

Axborot xavfsizlik monitoring markazi tizimi natijalari:

$$N1 = 14, \; N0 = 18, \; S(AXMM) = ?$$

$$S(AXMM) = \frac{N1}{N0} * 100 = \frac{15}{18} * 100 = 83{,}3$$

Avtomatlashtirilmagan axborot xavfsizlik tizimi natijalari:

$$N1 = 8, \; N0 = 18, \; S(AAXMT) = ?$$

$$S(AAXMT) = \frac{N1}{N0} * 100 = \frac{8}{18} * 100 = 44{,}4$$

Axborot xavfsizlik monitoring markazi va Avtomatlashtirilmagan axborot xavfsizlik tiziminining olingan natijalar quyidagi jadvalda shakllantirildi(3-jadval).

3-jadval.

№	Axborot xavfsizlik monitoring markazi	Avtomatlashtirilmagan axborot xavfsizlik tizimi
1	83,3	44,4

Olingan natijalar esa avtomatlashtirilgan tizimlar qatoriga kiruvchi Axborot xavfsizlik monitoring markazining ish faoliyati va xavfsizlikni ta’minlash samaradorligi qanchalik yuqori ekanligini ko‘rishimiz mumkin bo‘ladi.

Xulosa

Xulosa qilib shuni aytish mumkinki bugungi kunga kelib, nafaqat rivojlangan davlatlar qatorida O‘zbekiston ham to‘liq raqamli transformatsiya tizimini joriy etishni jadal sur’atlarda olib bormoqda. Shu bilan birga, zamonaviy telekommunikatsiya tarmoqlari xavfsizligini ta’minlashda birlamchi instrument hisoblangan monitoring qilish va markazlashgan holda boshqarishni ta’minlashga asoslangan tizim va dasturiy ta’minotlardan tashqari to‘g‘ridan-to‘g‘ri

axborot va kiberxavfsizlikni ta’minlash vositalarini joriy qilish tizim xavfsizligi uchun asosiy omil bo‘lmoqda, lekin faqat shuning o‘zi yetarli emas deyish mumkin. Sabab esa bu elementlar asosida avtomatlashtirilgan va markazlashgan boshqaruv usuliga ega bo‘lgan tizimlarni joriy etishga qaratilgan chora-tadbirlarni jadallashtirilayotganligi quvonarlidir.

Zamonaviy telekommunikatsiya infratuzilmasi xafvsizligini ta’minlash maqsadida davlatning butun tarmoq infratuzilmalarini qamrab olgan yagona va markazlashgan Axborot xavfsizlik monitoring markazini joriy qilinishi telekommunikatsiya infratuzilmasi ish salohiyatini oshiribgina qolmasdan, axborot va kiberxavfsizlik talablari asosida ishlashigi ta’minlanishi olib borilgan tahlil natijalarida ham yaqqol ko‘rinish berdi. Bu yesa o‘z navbatida O‘zbekistorn Respublikasida axborot va kiberxavfsizlik salohiyatini yanada oshirish uchun bosilgan ulkan qadam bo‘ladi.

REFERENCES

1. “Security Operation Center: Building, Operating and Maintaining Your SOC” by Joseph Muniz, Gary McIntyre and Nadhem AlFardan – 2015 year.
2. “The Cybersecurity Playbook: How Every Leader and Employee Can Contribute to a Culture of Security” by Allison Cerra – 2019 year.
3. “A Taxonomy of Cyber Attacks on Machine Learning Systems” by Battista Biggio and Fabio Roli – 2018 year.
4. “A Survey on Security Information and Event Management (SIEM) Systems” by A. Khraisat et al. – 2019 year.
5. “NIST Special Publication 800-137: Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations” – 2011 year.