AXBOROT-KOMMUNIKATSIYA TIZIMLARIDA AXBOROT XAVFSIZLIGI MONITORINGI MUAMMOLARI

DSc., dotsent Turapov Sh.N.
(AKT va AHI)

ПРОБЛЕМЫ МОНИТОРИНГА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ СИСТЕМАХ

д.н.т., доцент Турапов Ш.Н.
(Военный институт информационно-коммуникационных технологий и связи)

PROBLEMS OF MONITORING INFORMATION SECURITY IN INFORMATION AND COMMUNICATION SYSTEMS

Dr.Sc., Associate Professor Turapov Sh.N.
(Military Institute of Information and Communication Technologies and Communications)

Axborot xavfsizligini ta'minlashda samarali monitoringning ahamiyatini sezilarli darajada aniqlash bilan bog'liq jihatlari belgilab olingan. Ya'ni axborot xavfsizligini buzilishlarini vaqtning real rejimida aniqlash va ularga adekvat reaksiya ko'rsatish hamda personal faoliyati bilan bog'liq hodisalar va buzg'unchilar monitoringining uzluksizligini ta'minlash. Shu bilan birga, axborot xavfsizligini buzilishlarini aniqlamaslik va konfidensial axborotni himoyalash bo'yicha adekvat choralarni ko'rmaslik axborot xavfsizligi tizimi tomonidan ta'minlanadigan mavjud himoyalanganlik darajasini jiddiy pasayishi to'g'risida muammolar tahlili amalga oshirilgan.

Kalit so'zlar: *Axborot-kommunikatsiya tizimlari, axborot xavfsizligini buzilish jarayonlari, xavfsizlik siyosati, AKTning bazaviy dasturiy-apparat, samarali monitoring qilish, xavfsizlik jurnallari, normallashtirish, taxdidlarni aniqlash, insidentlarni boshqarish, hisobotlarni yaratish, Sentinel Log Manager dasturiy ilovalar.*

Определены аспекты, связанные с существенным определением важности эффективного мониторинга в обеспечении информационной безопасности. То есть выявление нарушений информационной безопасности в режиме реального времени и адекватное реагирование на них, а также обеспечение непрерывности мониторинга инцидентов и злоумышленников, связанных с деятельностью персонала. При этом был проведен анализ проблемы по поводу того, что невыявление нарушений информационной безопасности и непринятие адекватных мер по защите конфиденциальной информации серьезно снижает уровень защиты, обеспечиваемой системой информационной безопасности.

Ключевые слова: *Информационные и коммуникационные системы, процессы нарушения информационной безопасности, политика безопасности, ИТ-инфраструктура, эффективный мониторинг, журналы безопасности, нормализация, обнаружение угроз, управление инцидентами, формирование отчетов, программные приложения Sentinel Log Manager.*

The aspects related to the essential definition of the importance of effective monitoring in ensuring information security are defined. That is, identifying information security violations in real time and adequately responding to them, as well as ensuring the continuity of monitoring of incidents and intruders associated with the activities of personnel. At the same time, an analysis

of the problem was carried out regarding the fact that failure to identify information security violations and failure to take adequate measures to protect confidential information seriously reduces the level of protection provided by the information security system.

Keywords: *Information and communication systems, information security violation processes, security policy, IT infrastructure, effective monitoring, security logs, normalization, threat detection, incident management, report generation, Sentinel Log Manager software applications.*

Jahonda axborot-kommunikatsiya tizimlari rivojining hozirgi zamon bosqichida axborot xavfsizligi holatini baholashning asosiy mexanizmlaridan biri hisoblangan axborot xavfsizligi monitoringi tizimlarini ishlab chiqishga va ularni takomillashtirishga alohida e'tibor qaratilmoqda. «Kasperskiy laboratoriyasi ma'lumotiga asosan 2024 yilning ikkinchi choragida jahonning 187 davlatlarida joylashgan Internet resurslari orqali 962 947 023 ta hujum amalga oshirilgan». Bu yo'nalishda rivojlangan mamlakatlarda, jumladan, AQSh, Germaniya, Buyuk Britaniya, Fransiya, Janubiy Koreya, Rossiya Federatsiyasi va boshqa davlatlarda axborot kommunikatsiya tizimlarining himoyalanganligini baholovchi axborot xavfsizligi monitoringi vositalarini ishlab chiqish muhim ahamiyat kasb etmoqda.

Bu borada, jumladan axborot-kommunikatsiya tizimlarini himoyalanganlik holatini real baholash, axborotni himoyalash vositalarida sodir bo'ladigan ko'p sonli hodisalarni normallashtirish, korrelyatsilash va agregatlash orqali axborot xavfsizligi insidentlarini aniqlash, axborotni himoyalash vositalarining ishidagi xatoliklarni tezkor aniqlash va bartaraf etish usullarini ishlab chiqish muhim ahamiyat kasb etadi. Shu bilan birga axborot xavfsizligi monitoringi tizimi ishlashining samaradorligini oshirish imkonini beruvchi jarayonlarni takomillashtirishni ilmiy asoslash zarur bo'lmoqda.

Ma'lumki, axborot-kommunikatsiya tizimlari (AKT) har xil texnologik jarayonni yoki uning qismini amalga oshiradi. Ravshanki, axborot oqimlari harakatidagi har qanday yanglishish yoki ulardan foydalanish qoidalarining buzilishi muammolarga va qo'shimcha harajatlarga yoki foydaning boy berilishiga olib kelishi mumkin. Shuning uchun, har qanday tashkilot yoki kompaniya axborot sohasidagi o'z qiziqishlarini himoya qilish maqsadida axborotni suiste'mol qilish, firibgarlik, muhim amallarning barbod bo'lishini va konfidensial axborotni ruxsatsiz oshkor etilishi kabi holatlarni oldini olish uchun AKT xavfsizligini ta'minlash bo'yicha kuchaytirilgan choralarni qo'llaydilar [1].

Shu sababli, o'z vaqtida va samarali monitoringning ahamiyatini sezilarli darajada aniqlaydigan axborot xavfsizligini (AX) ta'minlash bilan bog'liq, quyidagi jihatlarni belgilab olish mumkin.

Birinchidan, AX buzilishlarini vaqtning real rejimida aniqlash va ularga adekvat reaksiya ko'rsatish. Bu axborot xavfsizligi ma'murlarining ko'p sonli axborotni himoyalash vositalaridan(antiviruslar, tarmoqlararo ekranlar, xujumlarni aniqlash tizimlari va h.) keladigan ma'lumotlarni qabul qilish va keyingi tahlillash jarayonlariga zarur va tegishli e'tibor qaratishlari bilan bog'liq.

Ikkinchidan, personal faoliyati (tizimga kirish, kiritish/chiqarish portlaridan

foydalanish, axborotni eltuvchilarga yozish va h.) bilan bog‘liq hodisalar va buzg‘unchilar (tarmoqqa ruxsatsiz suqilib kirishga urinishlar, virusli hujumlarni o‘tkazish, xizmat ko‘rsatishdan voz kechishga undash va h.)monitoringining uzluksizligini ta’minlash.

Uchinchidan, axborot kommunikatsiya texnologiyalarining rivojlanishi natijasida jinoyatchilar tomonidan konfidensial axborotni ruxsatsiz va noqonuniy olishi uchun qo‘llaniladigan yangi usul va vositalarni aniqlash imkoniyati. Bu imkoniyatni amalga oshirish axborot xavfsizligi tizimida ma’lum intellektning mavjudligini talab qiladi.

O‘z vaqtida AX buzilishlarini aniqlamaslik va konfidensial axborotni himoyalash bo‘yicha adekvat choralarni ko‘rmaslik axborot xavfsizligi tizimi tomonidan ta’minlanadigan mavjud himoyalanganlik darajasini jiddiy pasayishiga olib keladi. Shuning uchun, har xil, xususan oldin ma’lum bo‘lmagan, axborot xavfsizligi taxdidlarini o‘z vaqtida aniqlashga imkon beradigan monitoring muolajasini yaratish va keyinchalik uni amalga oshirish zarur. Bunday jarayonning mavjud emasligi natijasida tashkilot yoki korxona ichki va tashqi jinoyatchilar harakatidan bir necha qadam orqada qoladi, hamda tashkilotning yirik moliyaviy yo‘qotishiga va obro‘sizlantirilishiga sabab bo‘ladigan axborotning sirqib chiqqanligi haqida bilmaydi [2].

Monitoring yordamida hal qilinadigan vazifalar belgilangan:

- xavfsizlik siyosati buzilishida insidentlarni tekshirishda hodisalar orasidagi sabab-oqibat bog‘lanishlarini aniqlash;
- xavfsizlik siyosatidagi kamchiliklar, nomukammalliklar va xatoliklarni tahlillash;
- AKTning bazaviy dasturiy-apparat va AXni ta’minlash vositalarining noto‘g‘ri ishlashi (xatoliklar, yanglishishlar) sabablarining tahlili;
- foydalanuvchilar tomonidan tarmoq resurslaridan samarasiz va oqilona foydalanmaslik faktlarini aniqlash.

Yuqorida ta’kidlanganidek, muntazam monitoring o‘tkazish axborotni himoya qilishning zarur darajasini saqlab turishning kafolati hisoblanadi, monitoring tizimi faoliyati doirasidagi natijalar esa axborot xavfsizligini ta’minlash tizimini takomillashtirishga asos hisoblanadi.

AXning to‘liq va samarali monitoringini tashkil qilishda bir qator odatiy muammalorga duch kelish mumkinligini hisobga olish lozim:

- kompaniya yoki tashkilot ixtiyoridagi axborotni tahlillashda tizimli yondashuvning yo‘qligi;
- dasturiy-apparat vositalar himoyalashi kerak bo‘lgan aktivlarni identifikatsiyalashda noto‘g‘ri hisoblashlarning mavjudligi;
- elektron jurnallarda qayd etilgan ko‘plab hodisalar ichidan xavfsizlikni ta’minlash uchun ahamiyatga ega bo‘lgan axborotni aniqlashdagi qiyinchiliklar;
- axborot resurslaridan va ularni ishlovchi vositalardan maksimal foydalanish imkoniyatiga ega xodimlarning (dasturchilar, ma’murlar) faoliyati nazoratini avtomatlashtirilgan tarzda qamrab olinmasligi.

Ushbu muammolar ko‘plab sabablarga ko‘ra sodir bo‘lishi mumkin:

•personalning monitoring jarayoniga yuzaki munosabati;

•ma’lumotlarni sifatli tahlillashda personal malakasining yetarli emasligi;

•kiruvchi ma’lumotlar xajmining kattaligi va h.

•Axborot xavfsizligini to‘liq ta’minlash uchun har kuni quyidagi axborot manbalarini tahlillash lozim:

•antivirus dasturiy ta’minoti, pochta serverlari, xujumlarni aniqlash tizimlari, tarmoqlararo ekranlarning log fayllari;

•operatsion tizimlarning xavfsizlik jurnallari;

•laxzali xabar almashish uchun dasturlardan foydalanish haqidagi ma’lumotlar;

•telefon aloqasi xizmatini ko‘rsatish haqidagi yozuvlar va h.

•Ta’kidlash lozimki, xavfsizlik hodisalari haqidagi axborotni o‘z vaqtida qabul qilish va tahlillash quyidagilarni ta’minlashga imkon beradi:

•AKT axborot resurslarining konfidensialligini, yaxlitligini va foydalanuvchanligini buzishga qaratilgan jinoyatchilarning atayin yoki behosdan qilgan harakatlarini aniqlash;

•ko‘zda tutilmagan vaziyatlarni paydo bo‘lishini ogohlantirish hisobiga AKT ishlashining barqarorligini va ishonchligini oshirish;

•AKT axborot resurslarini buzish va yo‘qotish bilan bog‘liq xavflarni kamaytirish.

Ayrim hodisalarni aniqlash faktiga qanday reaksiya qilinganiga bog‘liq holda axborotni passiv va aktiv himoyalash vositalari farqlanadi [3].

Passiv vositalar bo‘lib o‘tgan hodisaga qarshi hech qanday chora ko‘rmaydi, faqat ushbu hodisa faktini qaydlaydi hamda ma’murga bu xususida xabar beradi. Aktiv vositalar ushbu faktni aniqlabgina qolmaydi, balki undan keladigan salbiy oqibatlarni blokirovkalash va neytrallash bo‘yicha choralarni aniqlashga kirishadi.

Tashkilotlarda axborot xavfsizligi holatini baholashda monitoring jarayonida axborotni himoyalashning quyidagi dasturiy va apparat vositalaridan olinadigan ma’lumotlardan foydalaniladi [4]:

•xavfsizlik skanerlari;

•antivirus dasturiy ta’minoti;

•kontentli tahlil vositalari;

•kiritish/chiqarish portlarini nazoratlash vositalari;

•tarmoqlararo ekranlar;

•xujumlarni aniqlash tizimlari va h.

Keltirilgan axborotni himoyalash vositalari axborotni uzluksiz yig‘adi, ammo ularni har xil vaqt onida ishlaydi.

Ma’lumotlarni qaydlash va tahlillashning ikkita asosiy mexanizmi farqlanadi:

1. Interval – mo‘ljallangan mexanizm. Bunda lokal mashinada joylashgan dasturiy agentlar, keyinchalik avtomatik tarzda yoki qo‘lda tahlillanuvchi, insidentlar xususidagi axborotni log fayllarda(jurnallarda) qaydlaydilar. Tahlillash jarayonida real vaqt rejimidagi tahlillashga nisbatan tizimga kam yuklama to‘g‘ri keladi, ammo axborotni yig‘ish va saqlash uchun diskli xotiraning katta xajmi talab

qilinadi.

2. Real vaqt mexanizmi. Bunda axborotni uzluksiz yig‘ish, uni tahlillash va mos xabarlarni berish imkoniyati mavjud. Xujumlarning yetarlicha tez aniqlanishi ularni to‘xtatishga imkon bersada, bunday tahlillash asosiy xotira va protsessor resurslarining katta xajmini talab etadi.

Axborot kommunikatsiya tizimlarining oldin noma’lum bo‘lgan tahdid va zaifliklar sonining doimiy o‘sib borishi sharoitida axborotni himoyalashning ko‘plab vositalarining paydo bo‘lishi, axborot xavfsizligi hodisalari haqidagi sezilarli miqdordagi ma’lumotlarni operativ ishlash muammosini keltirib chiqarmoqda. Ma’mur uchun bunday ishlashni qo‘lda amalga oshirish mumkin emas, shuning uchun hozirgi vaqtda axborot xavfsizligi monitoringi tizimi deb nomlanadigan avtomatlashtirilgan yoki to‘liq avtomat tizimlari qo‘llanilmoqda [2; 7-b.].

Axborot xavfsizligi monitoringi tizimi axborotni himoyalash vositalarining ishlashi va ishga layoqatligi imkoniyatining buzilishi hamda niyati buzuqlarning axborot konfidensialligini, yaxlitligini yoki foydalanuvchanligini buzishga qaratilgan harakatlari bilan bog‘liq axborot xavfsizligi hodisalarini qaydlashga imkon beradi.

Axborot xavfsizligi monitoringi tizimining asosiy funksiyalariga quyidagilar taalluqli [4]:

- xavfsizlik jurnallarini (log-fayllarni) yig‘ish – ularni markazlashgan holda yagona serverga jamlash;
- normallashtirish – har xil jurnallar yozuvlarini yagona formatga keltirish;
- to‘ldirish – olingan axborotga axborot-kommunikatsiya tizimlaridan olingan boshqa ma’lumotlarni, hamda taxdid va zaifliklar haqidagi ommaviy foydalaniladigan ma’lumotlarni qo‘shish;
- taxdidlarni aniqlash – jurnallardagi xavfsizlik hodisalari ichidan axborot xavfsizligining buzilishi alomatlarini aniqlash uchun sun’iy intellektni qo‘llash;
- insidentlarni boshqarish – taxdidlar aniqlanganidan so‘ng qo‘llaniladigan harakatlar. Bu xavfsizlik ma’muriga xabarnoma yuborish, insidentga avtomatik tarzda reaksiya ko‘rsatish(masalan, qandaydir dasturni bajarish) va boshqalar bo‘lishi mumkin;
- hisobotlarni yaratish – aniqlangan taxdidlar va tizim ishlashining samaradorligi haqidagi ma’lumotlarni taqdim qilish.

Keltirib o‘tilgan funksiyalar axborot xavfsizligi monitoringi tizimiga xavfsizlik hodisalariga reaksiya ko‘rsatish bo‘yicha yechimni qabul qilishda ma’murga mos madadni ta’minlashga imkon beradi.

Hozirgi kunda axborot xavfsizligini ta’minlash vositalari bozorida InTrust, EventTracker, Sentinel Log Manager, NXLog, LOGStorm kabi ishlab chiqaruvchilarning axborot xavfsizligi monitoringi dasturiy vositalari taqdim etilgan.

InTrust dasturiy vositasida tashkilot axborot kommunikatsiya tizimida foydalanish uchun qulay yagona axborot paneliga birlashtirilgan server tizimlari va

ma’lumotlarning umumiy manbalaridan keluvchi katta hajmli ma’lumotlarni yig‘ish, saqlash va qidirish uchun instrumentlar to‘plami mavjud. Dasturiy vositadan foydalanuvchi harakatlarini kuzatish orqali ilovalarning ishlash jarayonida xavfsizlik talablarining bajarilishini aniqlash imkonini beradi.

InTrust dasturiy vositasining xususiyatlari:

- tayyor shablon va algoritmlardan foydalangan holda xavfsizlik hodisalarining tahlili;
- tizim foydalanuvchilari, fayllar va hodisalar xususidagi ma’lumotlarning dinamik tadqiqi;
- Enterprise Reporter va Change Auditor ga asoslangan intelektual qidiruv instrumenti.

EventTracker dasturiy vositasi tashkilot axborot kommunikatsiya tizimining xavfsizligi, unumdorligi va foydalanuvchanligiga ta’sir o‘tkazuvchi salbiy harakatlarni identifikatsiyalash imkonini beradi. Dastur tizimni sodir etilishi mumkin bo‘lgan insidentlardan himoyalash uchun monitoring instrumentlari yordamida o‘zgarishlarni aniqlay oladigan jurnallarni boshqaradi. Oxirgi bosqichda ko‘p sonli hodisalarni birlashtirish va ro‘yhatga olish orqali axborot panelida yakuniy natijalarni taqdim etadi.

EventTracker dasturiy vositasining xususiyatlari:

- MD5 va VirusTotal dan foydalangan holda avtomat tarzda auditlash va zararli dasturlarni aniqlash;
- shablonlar asosida umumiy tarmoqdagi tahdidlarni qidirish;
- dasturni tezkor ravishda ishga tushirish;
- joriy etish va xavfsizlikning aksariyat talablari uchun dastlabki sozlangan ogohlantirishlar.

Sentinel Log Manager – dasturiy ilovalar paketi bo‘lib, ma’lumotlarning konfidensialligini va foydalanuvchanligini ta’minlash imkonini beruvchi jurnallarni yig‘ish, tahlillash va xavfsiz saqlash modullaridan iborat. Sentinel Log Managerning iqtisodiy jihatdan samarali va moslashuvchan platformasi sodir etilishi mumkin bo‘lgan axborot xavfsizligi tahdidlarini tashkilot jurnallarining real vaqt rejimida monitoringi orqali aniqlaydi [5].

Sentinel Log Manager dasturiy ilovalar paketining xususiyatlari:

- taqsimlangan qidiruv;
- tezkor hisobotdorlik;
- patentlanmagan ma’lumotlarni saqlash tizimlarini madadlash;
- jurnal ma’lumotlarini shifrlash.

NXLog dasturiy vositasi turli xil platformalar, manbalar va formatlardagi hodisalar jurnallarini tahlillash uchun zarur insrumentlarga ega. Unda tarmoqdan kelayotgan UDP, TCP va TLS / SSL protokollari orqali turli xil formatdagi fayllarning jurnallarini yig‘ib olish imkoniyati mavjud.

NXLog dasturiy vositasining xususiyatlari:

- Linux, GNU, Solaris, BSD, Android va Windows operatsion tizimlari uchun

multiplatformali madadlash;

- o‘zgaruvchan plaginlar yordamida modulli muhit;
- jurnalni rotatsiyalash va vazifalar jadvali;
- SSL orqali tarmoqda xavfsiz ma’lumot almashuvi.

LOGStorm dasturiy vositasi joriy etilishi va foydalanishi oson kengaytirilgan funksiyalar orqali jurnallarni boshqarish imkonini beradi. LOGStorm xavfsizlik talablarini hisobga olgan holda paydo bo‘ladigan buzilishlar va xatoliklarni aniqlaydi.

LOGStorm dasturiy vositasining xususiyatlari:

- insidentlarni aniqlash uchun shablonlar mavjudligi;
- jurnallarni markazlashgan holda saqlash;
- xavfsizlik resurslari uchun oddiy sozlashlarning mavjudligi.

Yuqorida keltirilgan monitoring dasturiy vositalarining ishlash funksiyalarini o‘rganib chiqish natijasida ularning qiyosiy tahlili amalga oshirilgan (1-jadval). Qiyosiy tahlil stackify.com veb-saytida keltirilgan log fayllarga asoslangan axborot xavfsizligi monitoringi dasturiy vositalarini baholash asosida amalga oshirildi [6].

Jadvalda keltirilgan qiymatlarni quyidagicha tavsiflash mumkin: 4 – “a’lo”, 3 – “yaxshi”, 2 – “qoniqarli”, 1 – “qoniqarsiz”. Axborot xavfsizligi monitoringi dasturiy vositalarini baholash tahdidlarni aniqlash, resurs talabi, unumdorlik, foydalanuvchanlik, joriy qilinishi, boshqarilishi, madadlanishi, masshtablanishi, vositalar ishlashi holatlari ehtimolliklarining aniqlanishi mezonlari bo‘yicha amalga oshirilgan. Ushbu mezonlar bo‘yicha baholashning maksimal qiymati 36 ga teng.

1-jadval

Axborot xavfsizligi monitoringi dasturiy vositalarining qiyosiy tahlili

Axborot xavfsizligi monitoringi dasturiy vositalari	**Tahdidlarni aniqlash**	**Resurs talabi**	**Unumdorlik**	**Foydalanuvchanlik**	**Joriy qilinishi**	**Boshqarilishi**	**Madadlanishi**	**Masshtablanishi**	**Vositalar ishlashi holatlari ehtimolliklarining aniqlanishi**	Σ
InTrust	3	3	3	3	2	3	3	3	1	24
EventTracker	4	3	4	3	3	3	4	4	2	30
Sentinel Log Manager	4	3	4	4	3	4	4	4	2	32
NXLog	3	4	3	3	3	4	3	3	1	27
LOGStorm	3	3	3	3	3	3	4	3	1	26

Jadvalda keltirilgan axborot xavfsizligi monitoringi dasturiy vositalarining qiyosiy tahlili *vositalar ishlashi holatlari ehtimolliklarining aniqlanishi* mezoni bo‘yicha 40% qoniqarli va 60% qoniqarsiz natijalarni qayd etgan. Demak, hozirgi kunda tashkilotlarda foydalanilayotgan axborot xavfsizligi monitoringi dasturiy vositalari yordamida axborotni himoyalash vositalarining ishlashi holatlari

ehtimolliklarini aniqlash kutilgan natijalarni bermaydi [7]. Bu esa axborotni himoyalash vositalarining ishlashida uchraydigan buzilishlarni o‘z vaqtida aniqlay olmaslik holatlarini keltirib chiqaradi.

Shunday qilib, monitoring samaradorligi axborot xavfsizligi monitoringi tizimining har qanday komponentida buzilishlar paydo bo‘lishi bilan pasayishi mumkin, biroq amaliyot ko‘rsatadiki, monitoring tizimi tarkibidagi axborotni himoyalash vositalari ishidagi xatoliklar sodir bo‘lganida eng salbiy ta’sir bo‘ladi. Bu holda axborotni himoyalash vositalarining bekor turishi yoki noto‘g‘ri ishlashi mobaynida axborot-kommunikatsiya tizimlari ishlashi samaradorligining pasayishiga olib keladigan axborot xavfsizligi insidentlarini o‘tkazib yuboruvchi qo‘shimcha taxdidlar paydo bo‘ladi. Shu sababli, axborot xavfsizligi ma’muri uchun qiyinchilik tug‘diradigan, axborotni himoyalash vositalari ishlashining buzilishi sabablarini operativ aniqlash va bartaraf etish lozim. Bu axborot xavfsizligi monitoringi tizimining ishlashi va yuqori darajadagi noaniqliklar (tashvishlar) tug‘diradigan va ma’murning qaror qabul qilish jarayoniga ta’sir qiluvchi e’tiborga olinishi qiyin juda ko‘p omillar mavjudligi bilan izohlanadi [8].

Shuning uchun, axborot xavfsizligi monitoringi tizimi tarkibiga kiruvchi axborotni himoyalash vositalarining hozirgi ishonchlik holati haqida ma’murning yetarlicha ma’lumotga ega emasligi bilan bog‘liq noaniqliklarni kamaytirish hisobiga, yanada samaraliroq axborot xavfsizligi monitoringi tizimini ishlab chiqish vazifasi dolzarb hisoblanadi.

Xulosa qilib aytganda, Axborot xavfsizligi monitoringida mavjud muammolarning va monitoring dasturiy vositalarining tahlili shuni ko‘rsatadiki, ko‘plab inobatga olish qiyin bo‘lgan omillar axborotni himoyalash vositalarining ishlashida uchraydigan buzilishlarni o‘z vaqtida aniqlay olmaslik holatlarini keltirib chiqarishi bilan birga, axborot xavfsizligi monitoringi tizimining ishlash jarayoniga va ma’mur tomonidan qaror qabul qilish jarayoniga ham o‘z ta’sirini o‘tkazadi.

FOYDALANILGAN ADABIYOTLAR RO‘YHATI

[1] Andriashin X.A., S.Ya.Kazansev., V.N.Kalinina, O.E.Zgadzay., Ye.R.Rossinskaya., A.V.Fillippon. Informatika i matematika dlya yuristov: Uchebnoe posobie dlya vuzov. M.: Yuniti-Dana, 2002, — S. 463.

[2] Chris Fry., Martin Nystrom. Security Monitoring // Printed in the United States of America, Published by O’Reilly Media, Inc., 1005 © 2009, – P. 248.

[3] Abdurakhmanov A.A., Nasrullayev N.B., Varisov A.A. E-Government, Open Data, and Security: Overcoming Information Security Issues with Open Data // Computer Science and Information Technology, DOI: 10.13189/ csit.2015.030407, 3(4) 2015, – P.133-137.

[4] Viktor Serdyuk. HP ArcSight - effektivnыy instrument dlya monitoringa sobытiy IB // Jurnal "Information Security/ Informatsionnaya bezopasnost" №1, 2013, – S. 32-33.

[5] Soddalashgan muvofiqlik va xavfsizlik uchun jurnallarni boshqarish:

[sayt]. URL:https://www.netiq.com/products/sentinel-log-manager/.html (murojaat vaqti: 20.10.2024).

[6] Loglarni boshqarishning eng yaxshi vositalari: [sayt]. URL:https://stackify.com/best-log-management-tools.html (murojaat vaqti: 20.10.2024)..

[7] Gulomov Sh.R., Nasrullaev N.B. Nedostatki suщestvuyuщix SIEM sistem s tochki zreniya analiza bezopasnosti // “Elektron hukumat tizimida axborot xavfsizligi muammolari va ularning yechimlari” mavzusi bo‘yicha Respublika seminari, Toshkent 27 oktabr, 2017, –B. 60-62.

[8] Eva Weishäupl., Emrah Yasasin., Guido Schryen. Information Security Investments: An Exploratory Multiple Case Study on Decision-Making, Evaluation and Learning // Exploratory Multiple Case Study on Information Security Investments, accepted for publication in Computers & Security, 2018, – P. 13-14.