AXBOROT XAVFSIZLIGI MONITORINGI TIZIMINING ARXITEKTURASI

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

АРХИТЕКТУРА СИСТЕМЫ МОНИТОРИНГА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

доктор технических наук, доцент Турапов Ш.Н.
(Военный институт информационно-коммуникационных технологий и связи)

ARCHITECTURE OF INFORMATION SECURITY MONITORING SYSTEM

Doctor of Technical Sciences, Associate Professor Turapov Sh.N.
(Military Institute of Information and Communication Technologies and Communications)

Axborot xavfsizligi monitoringi tizimi arxitekturasi o‘rganildi va amalga oshirildi. Bunda asosan quyidagi belgilashlardan foydalanildi: Ya’ni G-modul: axborot xavfsizligi xabarlarini generatsiyalash, DB-modul: axborot xavfsizligi xabarlarining ma’lumotlar bazasini saqlash, R-modul: javob reaksiyasini ishlab chiqish, A-modul: axborot xavfsizligi xabarlarining tahlillash, N-modul: axborot xavfsizligi xabarlarini yig‘ish va normallashtirish. Shuningdek, xavfsizlik ma’murining axborot xavfsizligi monitoringi tizimi ishlashida ishtirok etishi ixtiyoriy sharoitda amalga oshiriladi. Bunda noma’lumlik darajasi monitoring tizimining quyi sathida joylashgan axborotni himoyalash tizimining haqiqiy holatini izohlamaydi. Sababi axborot xavfsizligi monitoringi tizimida axborot xavfsizligi hodisasi xususidagi xabarlarning paydo bo‘lish vaziyatlarining ma’murlar tomonidan turlicha izohlanishi sodir bo‘lganligidadir.

Kalit so‘zlar: *Axborot xavfsizligi monitoringi tizimini tahlillash, Axborot xavfsizligi monitoringi tizimi arxitekturasi, axborot xavfsizligi hodisalari, zaifliklar, suqilib kirishlarni aniqlash va bartaraf qilish, ma’lumotlari bazasini madadlovchi dasturlar.*

Изучена и реализована архитектура системы мониторинга информационной безопасности. В основном использовались следующие обозначения: G-модуль: формирование сообщений ИБ, БД-модуль: ведение базы данных сообщений ИБ, Р-модуль: выработка реагирования, А-модуль: анализ сообщений ИБ, Н-модуль: сбор и нормализация сообщений информационной безопасности. Также участие администратора безопасности в работе системы мониторинга информационной безопасности осуществляется на добровольной основе. В этом случае степень неопределенности не объясняет фактическое состояние системы защиты информации, расположенной на нижнем уровне системы мониторинга. Причина в том, что в системе мониторинга ИБ обстоятельства возникновения сообщений об инцидентах ИБ по-разному интерпретируются органами власти.

Ключевые слова: *Анализ системы мониторинга информационной безопасности, Архитектура системы мониторинга информационной безопасности, инциденты информационной безопасности, уязвимости, обнаружение и устранение вторжений, программы поддержки базы данных.*

The architecture of the information security monitoring system has been studied and implemented. The following designations were mainly used: G-module: formation of information security messages, DB-module: maintenance of the information security message database, R-module: response generation, A-module: analysis of information security messages, H-module: collection and normalization of information security messages. Also, the participation of the security administrator in the work of the information security monitoring system is carried out on a voluntary basis. In this

case, the degree of uncertainty does not explain the actual state of the information protection system located at the lower level of the monitoring system. The reason is that in the information security monitoring system, the circumstances of the occurrence of information security incident messages are interpreted differently by the authorities.

Keywords: *Analysis of the information security monitoring system, Architecture of the information security monitoring system, information security incidents, vulnerabilities, detection and elimination of intrusions, database support programs.*

Jahonda axborot xavfsizligini ta’minlash tizimlari va vositalarini ishlab chiqishga hamda ularni takomillashtirishga alohida e’tibor qaratilmoqda. Axborot-kommunikatsiya tizimlari rivojining hozirgi zamon bosqichida axborot xavfsizligini samarali ta’minlash mexanizmlaridan biri operatsion tizimlarda foydalanish cheklangan ma’lumotlarni himoyalash hisoblanadi. CrowdStrike tashkiloti ekspertlarining 2024 yilning birinchi choragidagi kibertaxdidlar bo‘yicha tahlil natijalari shuni ko‘rsatmoqdaki, amalga oshirilayotgan tarmoq hujumlarining katta qismini internet foydalanuvchilari ma’lumotlariga ega bo‘lish harakatlari hisoblanib, ularning asosiy qismini axborot almashinuviga zarar yetkazuvchilar va kiberbuzg‘unchilar tashkil etmoqda. Axborot texnologiyalari sohasida xizmat ko‘rsatuvchi provayderlar va dasturiy ta’minotlardan foydalanuvchi mijozlar ma’lumotlariga ega bo‘lish maqsadida amalga oshirilgan tarmoq hujumlari soni 2023 yilga nisbatan 2024 yilning birinchi choragida deyarli ikki barobarga oshib, bu ko‘rsatgich 83% ni tashkil etgan . Bir qator mamlakatlarda, jumladan AQSh, Rossiya Federatsiyasi, Xitoy, Buyuk Britaniya, Germaniya, Janubiy Koreya, Isroil, Belorussiya va boshqa davlatlarda kompyuter tizimlarining axborot xavfsizligi auditini tashkil etishning avtomatlashtirilgan apparat-dasturiy vositalarini yaratishga alohida e’tibor qaratilgan. Shu bilan birga axborot xavfsizligi monitoringi tizimi ishlashining samaradorligini oshirish imkonini beruvchi jarayonlarni takomillashtirishni ilmiy asoslash zarur bo‘lmoqda.

Axborot xavfsizligi monitoringi tizimini tahlillash uchun uning besh sathli arxitekturasi va axborot xavfsizligi monitoringi tizimlarida ma’lumotlarni ishlash jarayoni eng muhim hisoblanadi. Ma’lumotlarni ishlash jarayonida quyidagi beshta asosiy texnik amallar bajariladi:

–axborot xavfsizligi hodisalari xususidagi xabarlarni qaydlash;

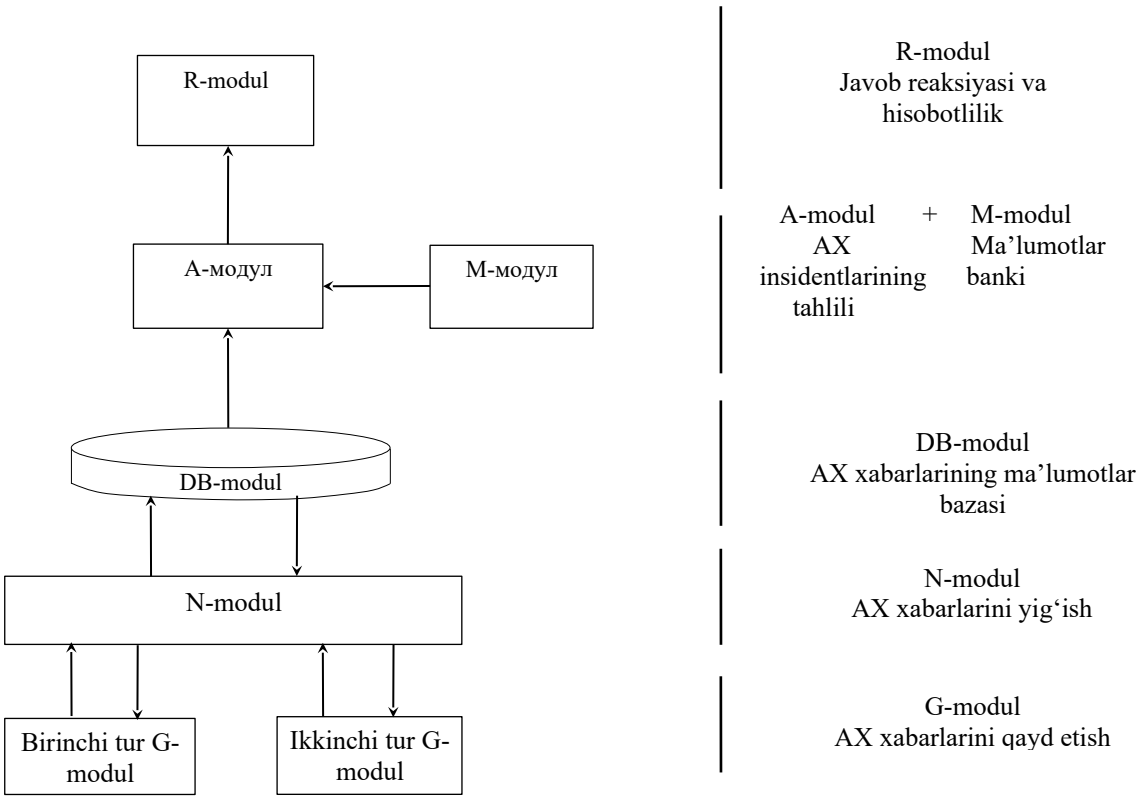
–axborot xavfsizligi xabarlarini yig‘ish;

–axborot xavfsizligi xabarlarini saqlash;

–axborot xavfsizligi xabarlari ketma-ketligini tahlillash;

–axborot xavfsizligi xabarlariga javob reaksiyalarini ishlab chiqish.

Axborot xavfsizligi monitoringi tizimi arxitekturasi [1] doirasida ushbu amallarning har birining bajarilishi uchun alohida modullar javob beradi (1-rasm). Qulaylik uchun quyidagi belgilashlardan foydalanildi:



1-rasm. Axborot xavfsizligi monitoringi tizimi arxitekturasi

–G-modul: axborot xavfsizligi xabarlarini generatsiyalaydi;

–DB-modul: axborot xavfsizligi xabarlarining ma'lumotlar bazasini saqlaydi;

–R-modul: javob reaksiyasini ishlab chiqadi;

–A-modul: axborot xavfsizligi xabarlarining tahliliga javob beradi;

–N-modul: axborot xavfsizligi xabarlarini yig'ish va normallashtirish uchun javob beradi [2].

Bundan tashqari, zaifliklarni, suqilib kirishlarni aniqlash va bartaraf qilish tizimi signaturasining ma'lumotlari bazasini madadlovchi va insidentlar haqidagi bilimlarni boshqarishga javob beruvchi M-modulni ko'zda tutish lozim.

Har bir modul ma'lum harakatlarni bajaradigan funksional modullar guruhini tavsiflaydi. Masalan, N-modul Syslog (UDP/514) standart interfeysi vositasida axborot xavfsizligi hodisalari haqidagi xabarlarni yaratadigan ko'plab ilovalardan iborat bo'lishi mumkin. Bundan tashqari N-modul suqilib kirishlarni aniqlash va bartaraf qilish tizimlari, tarmoqlararo ekranlar, pochta xabarlarini filtrlash tizimlari va axborotni himoyalashning barcha vositalari sifatida taqdim etilishi ham mumkin.

G-modul ikkita turga ajratiladi:

Birinchi tur G-modul – hodisalarga asoslangan(event-based) xabarlar generatori. U operatsion tizimlarda, ilovalarda yoki tarmoqda sodir bo'luvchi ma'lum hodisa natijasidagi xabarlarni generatsiyalaydi. Bunday G-modulga Syslog-xabarlar generatori, sensorlar va h. misol bo'la oladi [3].

Eng ko'p tarqalgan birinchi tur G-modul –tarmoq va xost sathidagi suqilib kirishlarni aniqlash va bartaraf qilish tizimlari. Bu kategoriyaga o'zining tarkibiga protokollash xizmatini kiritadigan har qanday amaliy filtrlash(tarmoq, amaliy va foydalanuvchi) tizimini qo'shish mumkin. Masalan, tarmoqlararo ekranlar,

foydalanishni nazoratlash ro‘yxati mavjud marshrutizatorlar, MAS-adres bo‘yicha filtrlaydigan simsiz foydalanish nuqtalari, RADIUS-serverlari, SNMP traps xizmati va boshqalar. Honeypots sinf tizimlari va tarmoq paketlari snifferlarini ham birinchi tur G-modullarga kiritish mumkin.

Ikkinchi tur G-modul – ba’zi bir tashqi rag‘bat yoki so‘rovga reaksiya sifatida xabarlarni generatsiyalaydigan, holatga asoslangan (status- based) xabarlar generatori. Bunday G-modulga ob’ekt yaxlitligini yoki foydalanuvchanligini tekshirish, PING-paketlarni yuborish, SNMP-poll funksiyalarini bajarish natijasida xabarlarni shakllantiradigan generatorlar misol bo‘la oladi. Ushbu bloklar yetarlicha o‘ziga xos xabar generatorlaridir. Ularning vazifasi masofadagi uchinchi tizimda aniqlangan holatni qayd etganda xabarlarni generatsiyalashdan iborat.

N-modul. Modulning asosiy vazifasi – har xil G-moduldan xabarlarni qabul qilish va xabarlarning gomogen ma’lumotlar bazasiga ega bo‘lishi uchun ularni standart formatga keltirish. Server xizmatlarini (klasterlash, komponentni takrorlash, yukni taqsimlash va h) himoyalashda foydalaniladigan standart usullarni amalga oshirish uchun bu modul foydalanuvchanlikni va masshtablilikni ta’minlashi muhim. Yig‘ilgan ma’lumotlarni formatlashning standartiga ega bo‘lish ham zarur.

DB-modul. DB-modul axborot xavfsizligi monitoringi tizimi arxitekturasida eng standartlashgan modul hisoblanadi va o‘zida ma’lumotlar bazasini ifodalaydi. Bu modul tomonidan bajariladigan axborot xavfsizligi monitoringi tizimi uchun o‘ziga xos asosiy amal – axborot xavfsizligi xabarlarini agregatlash. Agregatlash jarayonida yig‘ilgan ma’lumotlar optimallashtiriladi, bitta yoki bir nechta manbalarda takrorlangan xabarlar identifikatsiyalanadi va yo‘q qilinadi. Agregatlash ikkiti usulda amalga oshirilishi mumkin:

–hodisalar sathida - DB-modul bir yoki bir necha manbalardan olingan xabarlar manbai, turi va vaqtini tahlillaydi va bitta hodisa har xil vositalar tomonidan qayd etilgan bo‘lsa, yagona normallashtirilgan xabarni ma’lumotlar bazasida qoldirib, takrorlangan xabarlarni o‘chirib yuboradi;

–hodisalar oqimi sathida - DB-modul xabar vaqti va vazifasini, manbalar manzilini tahlillaydi va xabarning mavjud aloqalarini yagona xabar oqimiga yig‘adi. Bu usul axborot xavfsizligi monitoringi tizimini boshqarish konsolida axborotning tasvirlanishini optimallashtirish imkonini beradi.

Ma’lumotlar bazasi bilan bog‘liq klassik muammolardan (foydalanuvchanlik, yaxlitlik, konfidensiallik) DB-modul uchun asosiy mauammo unumdorlik hisoblanadi. G-modul miqdori yuzlar yoki minglarda o‘lchanishi mumkin. G-modul har sekundda o‘nlab xabarlarni generatsiyalashi mumkin. Xujumga urinish vaziyatlarida javob reaksiyasiga vaqt qolishi uchun ushbu xabarlarni ishlash, bazaga joylashtirish va imkon boricha tez tahlillash lozim [2].

A-modul. A-modul DB-modulda saqlanayotgan hodisalarni tahliliga javob beradi. O‘z vaqtida trevoga signalini generatsiyalash uchun xujumlarni aniqlash bo‘yicha turli amallarni bajaradi [3]. Ushbu modul ishida foydalaniladigan mexanizmlar korrelyatsiya algoritmlari, birinchi va ikkinchi xil xatoliklarini aniqlashga [4], xujumlarning matematik modellarini qurishga yoki himoyaning taqsimlangan vositalaridan

foydalanib xujumlarni aniqlashga [5] asoslangan.

A-modulning aksariyat amalga oshirishlari nostandart va yopiq hisoblanadi. Tadqiqotlar ko‘p olib borilgan, lekin ularning juda ham kam qismi amalga oshirilgan. Qolgan amalga oshirilganlari to‘liq bo‘lmay, faqatgina yondashishini namoyish qilish, boshqacha aytganda konsepsiyasini tasdiqlash uchun yetarlidir.

R-modul. R-modul o‘zida axborot xavfsizligi insidentlariga javob reaksiyasini amalga oshirish va hisobotni shakllantirish uchun instrumentlar jamlanmasini ifodalaydi. R-modul quyidagilarni hisobga olishi lozim: grafik interfeys ergonomikasini, xavfsizlik siyosatini amalga oshirish strategiyasini va tashkilotda mavjud huquqiy cheklovlarni. Bu cheklovlar javob reaksiyasi sifatida vaqt mobaynida to‘plangan real hayot tajribasiga asoslangan maslahat yoki eng yaxshi amaliyotdan boshqa xech narsani virtual tasavvur qilishning deyarli mumkin emasligiga olib kelishi mumkin [6]. Bu bilan R-modulning muhimligiga yetarlicha baho bermaslik kerak emas, chunki hujum to‘g‘ri tahlil qilingan va baholangan bo‘lishi mumkin, ammo o‘z vaqtida tegishli choralar qabul qilinmasa undan qochib bo‘lmaydi. Ushbu holda yagona reaksiya faqatgina hodisa sababini tahlillash bo‘ladi.

M-modul. Tahlil jarayoni o‘zida har xil xujumlar xususiyatlarini [7] va signaturasini, himoyalangan tizimning etalon modelini, xavfsizlik siyosatini va h o‘z ichiga olgan ba’zi kiruvchi ma’lumotlarni talab qiladi. Axborot xavfsizligi insidentlari tarixini saqlab qolish ham yaxshi tajriba hisoblanadi. Ushbu maqsadlar uchun M-modul ishlatiladi.

Axborot xavfsizligi monitoringi tizimining besh sathli arxitekturasining tahlili hozirgi vaqtda axborotni ximoyalash vositalarini sozlash usullari va vositalarining tizimga integratsiyalashmagani haqida fikrlashga imkon beradi. Axborot xavfsizligi monitoringi tizimi arxitekturasi doirasida axborot xavfsizligini boshqarish jarayonlarini birlashtirish asosida ishlash qulayligini oshirish maqsadga muvofiq hisoblanadi. Uning ustiga, monitoring tizimida axborot xavfsizligi hodisalariga avtomat tarzda yoki avtomatlashtirilgan reaksiya ko‘rsatish imkoniyati axborot xavfsizligi insidentlariga javob harakatlariga ketadigan vaqtni sezilarli kamaytirishga va natijada AKT himoyalanganligini oshishiga imkon beradi.

Quyida axborot xavfsizligi monitoringi tizimi ishlashining asosiy bosqichlarining qisqacha tavsifi keltirilgan (2-rasm).

1. G-modul axborot xavfsizligi insidenti bo‘lishi mumkin bo‘lgan axborot xavfsizligi hodisasini aniqlaganidan so‘ng bu xususida xabarni shakllantiradi [8] va uni mos N-modulga yuboradi.

2. Xabarlar mos yig‘uvchi N-modulga yuborilayotgan vaqtda ular miqdorini baholash [8] amalga oshiriladi.

3. N-modul axborot xavfsizligi hodisasi tahlili uchun xabardan zarur ma’lumotlarni chiqarib oladi va ularni axborot xavfsizligi monitoringi tizimida foydalaniladigan formatga keltiradi, ya’ni ma’lumotlarni normallashtirishni amalga oshiradi.

4. Axborot xavfsizligi hodisalari haqidagi normallashgan ma’lumotlar hodisalar ma’lumotlari bazasiga yoziladi (DB-modulga).

5. Bu ma’lumotlar hodisalar ma’lumotlari bazasidan A-modulga kelib tushadi.

Agar u bo‘sh bo‘lsa(modulda ishlash uchun joylashgan ma’lumotlar xajmi uning o‘tkazuvchanlik qobiliyatidan kam bo‘lsa), 9-bosqichga, aks holda 6- bosqichga o‘tiladi.

6. Axborot xavfsizligi hodisalari haqidagi ma’lumotlar A-modulda keyingi tahlil uchun navbatda turadi.

7. Navbat uzunligini baholashni amalga oshirish asosida axborot xavfsizligi monitoringi tizimining o‘rta sathida joylashgan komponentlar ishida buzilishlar mavjud yoki mavjud emasligi to‘g‘risida xulosa qilinadi.

8. A-modul «bo‘shaganidan» so‘ng, unga navbatda birinchi turgan ma’lumotlar ishlanishga yuboriladi.

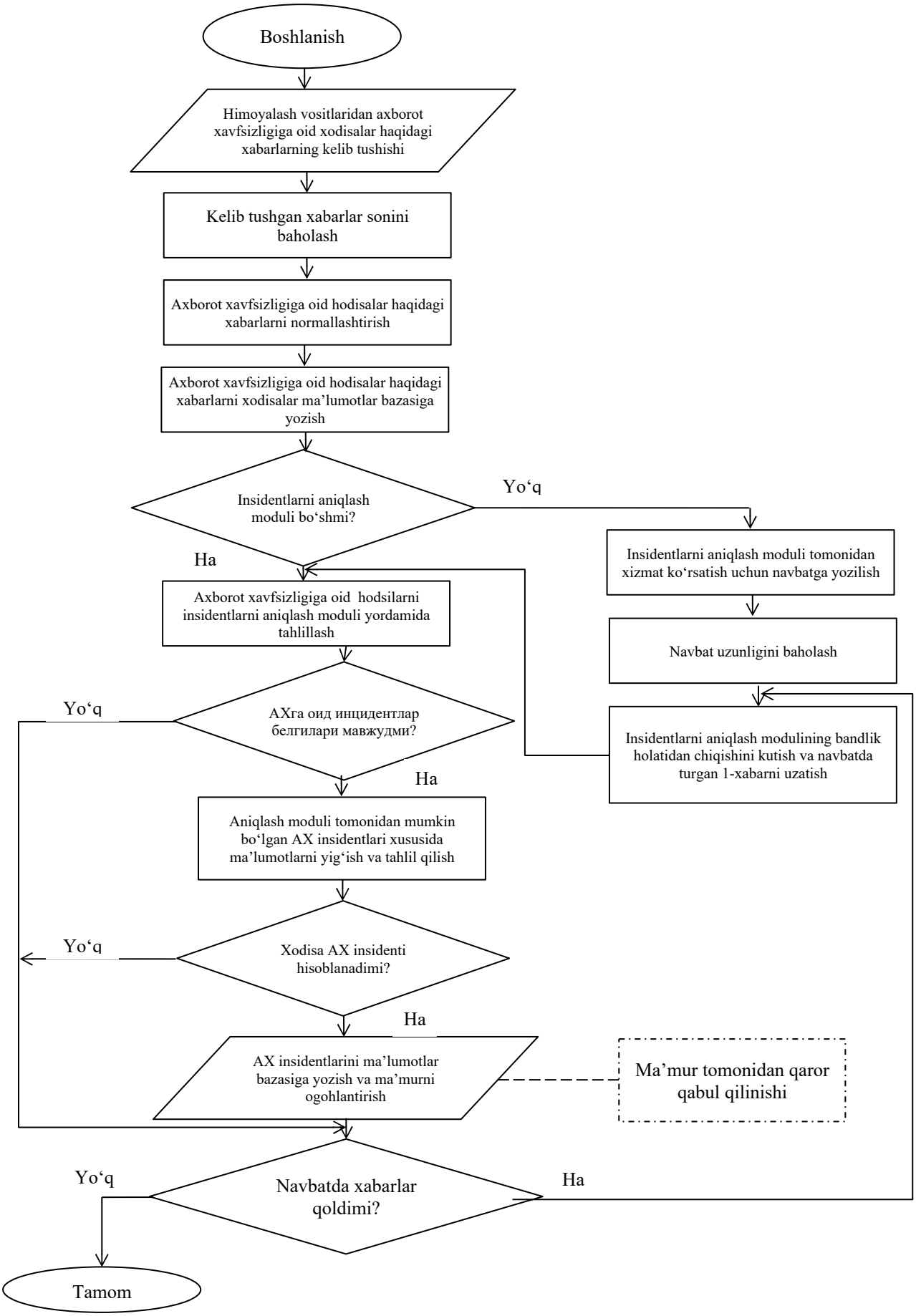
9. A-modul M-modulda saqlanayotgan ekspert bilimlardan foydalanib, axborot xavfsizligi insidentlarining formal alomatlarini qidirishni amalga oshiradi.

10. Agar A-modul axborot xavfsizligi hodisasi qandaydir ehtimollik bilan axborot xavfsizligi insidenti bo‘lishi mumkinligini aniqlasa 11 bosqichga, aks holda 14 bosqichga o‘tiladi.

11. A-modul ushbu onda sodir bo‘lgan axborot xavfsizligi hodisalari xususidagi axborotni himoyalashning boshqa vositalaridan qo‘shimcha ma’lumotlarni yig‘ishni amalga oshiradi va shu ma’lumotlarning tahlili asosida ushbu axborot xavfsizligi hodisalari orasidagi korrelyatsiya mavjudligini aniqlaydi va axborot xavfsizligining sodir bo‘lishi mumkin bo‘lgan insidentlarini ko‘rib chiqadi.

12. Agar insidentlarni tahlil qiluvchi modul tahlil qilingan axborot xavfsizligi hodisasi haqiqatdan ham axborot xavfsizligi insidenti ekanligiga ishora qiluvchi korrelyatsiyani aniqlasa, 13-bosqichga, aks holda 14-bosqichga o‘tiladi.

13. Sodir bo‘lgan axborot xavfsizligi insidenti xususidagi ma’lumot insidentlar ma’lumotlari bazasiga yoziladi, xavfsizlik ma’muriga mos xabar va qarshi chora qabul qilish uchun tavsiya yuboriladi. Ma’mur olingan axborot asosida aniqlangan insidentga reaksiya zarurligi haqida qaror qabul qiladi (R-modul).



2-rasm. Axborot xavfsizligi monitoringi tizimi ishlashining asosiy bosqichlari

14. A-modulda navbatda xizmat ko‘rsatish uchun axborot xavfsizligi hodisalari xususidagi ma’lumotlar qolgan bo‘lsa, 6-bosqichga o‘tiladi, aks holda – axborot xavfsizligi monitoringi tizimi keyingi axborot xavfsizligi hodisalari haqidagi xabar kelishini kutadi.

15. Axborot xavfsizligi monitoringi tizimi ishlashining 1- va 6- bosqichlarida katta ehtimollik bilan uning komponentlari ishida buzilishlar yuzaga kelishi mumkin. Shu sababli, axborot xavfsizligi monitoringi tizimiga ta’sir qilmaydigan 2- va 7-qo‘shimcha bosqichlar kiritilgan. Bu bosqichlardan chiqadigan axborot (kiruvchi holatlar soni va navbat uzunligi) axborotni himoyalashning alohida vositalarining yoki axborot xavfsizligi monitoringi tizimining umumiy ishlashida buzilishlarning mavjud yoki mavjud emasligi xususida xavfsizlik ma’murining qaror qabul qilishiga imkon beradi.

Yuqorida keltirilganlardan **xulosa qilish** mumkinki, xavfsizlik ma’murining axborot xavfsizligi monitoringi tizimi ishlashida ishtirok etishi noma’lum sharoitda amalga oshiriladi.Ushbu noma’lumlik darajasi monitoring tizimining quyi sathida joylashgan axborotni himoyalash tizimining haqiqiy holatini izohlamaydi. Natijada axborot xavfsizligi monitoringi tizimida axborot xavfsizligi hodisasi xususidagi xabarlarning paydo bo‘lish vaziyatlarining ma’murlar tomonidan turlicha izohlanishi sodir bo‘ladi.

FOYDALANILGAN ADABIYOTLAR RO‘YHATI

[1] Котенко И.В., Саенко И.Б, Кушнеревич А.Г. Архитектура системы параллельной обработки больших данных для мониторинга безопасности сетей Интернета вещей // Труды СПИИРАН, № 4 (59), 2018, – С. 19-25..

[2] Насруллаев Н.Б., Исломов Ш.З., Файзиева Д.С. Ахборот хавфсизлиги мониторинги тизими архитектураси // Муҳаммад ал-Хоразмий авлодлари, Илмий-амалий ва ахборот-таҳлилий журнал 2(4), 2018, – Б.15 -16.

[3] Meera Gandhi, S.K.Srivatsa. Detecting and preventing attacks using network intrusion detection systems // International Journal of Computer Science and Security, Volume (2): Issue (1), 2008 – P. 49-60.

[4] Jaydip Sen. Autonomous Agent–Based Distributed Fault-Tolerant Intrusion Detection System // 2nd International Conference on Distributed Computing and Internet Technology, December 22 - 24, 2005, – P. 2-6.

[5] Vollmer T., Manic M. Computationally Efficient Neural Network Intrusion Detection Security Awareness // 2nd Intern. Symp. on Resilient Control Systems, 2009, – P. 25–30.

[6] Igor Kotenko, Igor Saenko, Alexey Kushnerevich. Parallel big data processing system for security monitoring in Internet of Things networks // Journal of Wireless Mobile Networks, Ubiquitous Computing, and Dependable Applications (JoWUA), Vol.8, No.4 December 2017, – P. 10-15.

[7] Igor Saenko, Igor Kotenko, and Alexey Kushnerevich. Parallel Processing of Big Heterogenious Data for Security Monitoring of IoT Networks // Proceedings of the 25th Euromicro International Conference on Parallel, Distributed and network-based

Processing (PDP 2017). St. Petersburg, Russia, March 6-8, 2017. Los Alamitos, California. IEEE Computer Society. 2017, – P.329-336.

[8] Anger Anne Tondel, Maria B. Line, Martin Gilje Jaatun. Information security incident management: Current practice as reported in the literature Computers & security 45, 2014, – P. 42 -57.