ANOMALIYALARNI IMMUN TIZIMI MEXANIZMLARI ASOSIDA ANIQLASH METODIKASI

Umarov Shuxratjon Azizjonovich,
Farg‘ona davlat texnika universiteti “Dasturiy injiniring va kiberxavfizlik” kafedrasi dotsenti
E-mail: sh.umarov81@mail.ru

Umarov Nurali Olimjonovich,
"Temurbeklar maktabi" Farg‘ona harbiy litseyi o‘qituvchisi
E-mail: nurali.umarov.82@bk.ru

Annotatsiya. Ushbu maqolada axborot tizimidagi anomalliyalarni aniqlash uchun biologik immun tizimi tamoyillariga asoslangan sun’iy immun tizimi taklif etilgan. Anomaliyalarni aniqlashda salbiy tanlov algoritmidan foydalanish orqali foydalanuvchilarning normal faoliyatidan chetga chiqadigan harakatlari aniqlanadi. Ushbu yondashuv real vaqt rejimida tizim faoliyatini monitoring qilish, shablonlar va detektorlar to‘plamini shakllantirish orqali anomaliyalarni aniqlashni ta’minlaydi. Shuningdek, maqolada sun’iy immun tizimining ishlash tamoyillari, gen kutubxonasi evolyutsiyasi va klonal seleksiya jarayonlari bayon qilingan. Bir qator shu kabi amaliy ishlanmalar keltirilgan. Taklif etilgan modelning samaradorligi amaliy tajribalar asosida ko‘rsatilgan va boshqa an’anaviy usullar bilan taqqoslangan.

Kalit so‘zlar: sun’iy immun tizimi, anomaliya, axborot xavfsizligi, salbiy tanlov algoritmi, tizim chaqiruvlari, detektorlar, gen kutubxonasi, kiberxavfsizlik

KIRISH

Anomaliya deganda odatda me’yordan ortiq yoki umumiy qoidadan chetga chiqish, tartibsizlik yoki g‘ayrioddiylik tushuniladi. Biologiya, tibbiyot, geologiya kabi fanlarda atama odatiy rivojlanishdan boshqacha, jismoniy shakllarni buzilishini anglatishi mumkin. Axborot xavfsizligida anomaliya deganda axborot tizimidagi odatiy faoliyatdan farq qiluvchi shubhali harakatni tushunamiz. Anomaliyalar axborot tizimidagi buzilishlar yoki hujumlar bo‘lishi mumkin. Masalan, foydalanuvchi odatdagidan boshqa vaqtda yoki boshqa joydan kirishga urinishi, bir necha marta noto‘g‘ri parol kiritish holatlari, tizimga birdaniga katta hajmdagi ma’lumotlarni yuklash yoki yuklab olish, port skanerlash kabi noodatiy tarmoq faoliyati.

Axborot tizimining anomal harakatlarini aniqlash jarayoni quyidagi bosqichlarni o‘z ichiga oladi [1]:

1. Tizim ishlashi haqidagi dastlabki ma’lumotlarni yig‘ish.
2. Yig‘ilgan ma’lumotlarni tahlil qilish.
3. Hujumni aniqlash.
4. Aniqlangan hujumga javob qaytarish.

Dastlabki ma’lumotlarni yig‘ish bosqichida tizimning barcha mumkin bo‘lgan harakatlar variantlarini ikki guruhga ajratish mumkin: normal harakat va anomal harakat. Normal harakat tizimning odatdagi rejimda ishlashiga mos kelsa, anomal harakat hujum, buzilish yoki shunchaki tizimning noto‘g‘ri ishlashiga mos keladi. Tizim harakatini tahlil qilish uchun ishlatiladigan dastlabki ma’lumotlar sifatida turli ilovalar tomonidan bajarilgan tizim chaqiruvlari ketma-ketligini yozib olish tanlanishi mumkin. Bunday yondashuv, Windows operatsion tizimida mavjud. Ushbu tizimdagi tajribada 133 ta tizim chaqiruvi hisobga olingan. Har bir chaqiruv butun son bilan kodlangan (1-jadval) va ma’lumotlarni yig‘ish har bir ilova faolligini uzluksiz kuzatish orqali amalga oshirilgan.

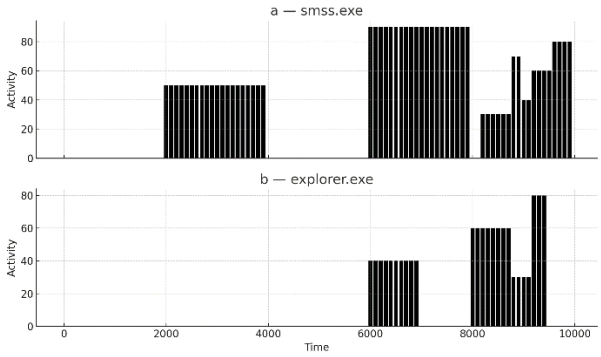
1-jadval

Tizim chaqiruvlarini kodlash usuli

Buyruq nomi	**Chaqiruv nomeri**
Cancel Remove Device	1
Cancel Stop Device	*2*

Close File	3
……	
Write File	133

1-rasmda smss.exe va explorer.exe dasturlarining faollik grafiklari keltirilgan. Ushbu rasmdan ko‘rinib turibdiki, har bir ilova o‘ziga xos faollik namoyon etadi. Uzoq muddatli kuzatuv davomida ilova faoliyatida takrorlanishlarni aniqlash mumkin, bu esa normal ishda u yoki bu dastur tizim chaqiruvlarining chekli miqdordagi turli ketma-ketliklarini amalga oshirishidan dalolat beradi.



1-rasm. Faol jarayonlar grafigi

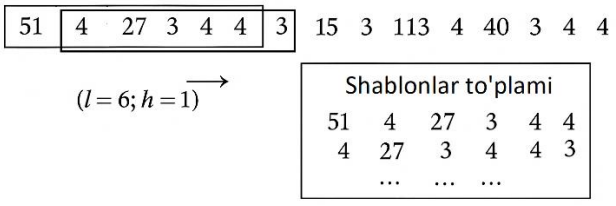
MATERIALLAR VA USULLAR

Anomaliyalarni aniqlash tizimini qurishda quyidagi usuldan foydalaniladi:

a) ma’lum vaqt oralig‘idagi tizim chaqiruvlari ketma-ketligi yozib olinadi;

b) siljuvchi vaqt oynasi o‘lchami l va vaqt oynasi siljishi h tanlanadi;

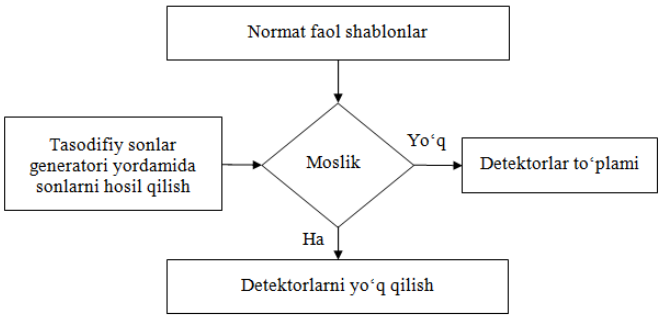
v) tizimning harakatini tasvirlovchi l uzunlikdagi satrlardan iborat shablonlar to‘plami yaratiladi (2-rasm). Bunda oyna o‘lchami l=6 va siljish o‘lchami h=1 qabul qilingan. Tasvirlangan usuldan foydalanib, axborot tizimining adekvat harakati modelini tuzish mumkin.



2-rasm. Tizim harakatlari uchun shablonlar to‘plamini shakllantirish

Hujumni aniqlash bosqichida salbiy tanlash algoritmi qo‘llaniladi, uning mohiyati quyidagicha [2]:

S orqali normal faol shablonlari to‘plamini belgilaylik. R detektorlar to‘plami tasodifiy ravishda yaratiladi (3-rasm).



3-rasm. Salbiy tanlash algoritmi sxemasi

Salbiy tanlash algoritmi qisman r-moslik prinsipidan foydalanadi. ya’ni ikkita satr r-mosligi hisoblanadi. Agar ularni tashkil etuvchi sonlar r ga teng yoki yonma-yon joylashgan pozitsiyalarda bir xil bo‘lsa, vazifaga qarab tanlov amalga oshiriladi. Umuman olganda, ikki shablonning yonma-yon pozitsiyalaridagi bir xil qiymatlar soni ushbu shablonlarning affiniti deb ataladi. Shunday qilib, R detektorlar to‘plamiga faqat uzunligi l bo‘lgan, affinitivligi r-normal faollik shabloniga nisbatan kichik bo‘lgan tasodifiy yaratilgan satrlar (shablonlar) kiradi.

Amaliyotda detektor to‘plamining elementlari ketma-ket yaratiladi va muayyan vazifani hal qilish uchun zarur bo‘lgan detektorlar soniga erishilgunga qadar generatsiya qilinadi. Ushbu sonni baholash uchun quyidagi belgilashlardan foydalanamiz:

- N_{RO} - generatsiya tomonidan shakllantirilgan detektorlar soni;
- N_R - normal shablonga mos kelmagan detektorlar soni;
- N_S - normal faollik shablonlari soni;
- P_M - tasodifiy yaratilgan ikki shablonning r-moslik ehtimoli;
- f - tasodifiy shablonning normal faollik shablonlariga mos kelmasligi ehtimoli;

- P_f - hujumni aniqlay olmaslik ehtimoli.

Agar P_M yetarlicha kichik bo‘lsa hamda N_S va N_R yetarlicha katta bo‘lsa:

$$f = (1 - P_M)^{N_S}; \quad (1)$$

$$N_R = N_{RO} \cdot f; \quad (2)$$

$$P_f = (1 - P_M)^{N_R} \approx e^{-P_M N_R} \quad (3)$$

Bundan

$$N_R = -\frac{\ln P_f}{P_M} \quad (4)$$

va shunga mos ravishda

$$N_{RO} = \frac{N_R}{f} = -\frac{\ln P_f}{P_M \cdot (1 - P_M)^{N_S}} \quad (5)$$

(5) formula hujumni o‘tkazib yuborish ehtimoli (P_j), normal faollik shablonlari soni (N_S) va ikkita tasodifiy satrning mos kelish ehtimoli (P_M) funksiyasi sifatida detektor nomzodlari satrlari sonini belgilaydi, bu satrlarni algoritm yordamida yaratish kerak.

O‘z navbatida, (P_M) ehtimolini hisoblash uchun quyidagi formuladan foydalanish mumkin:

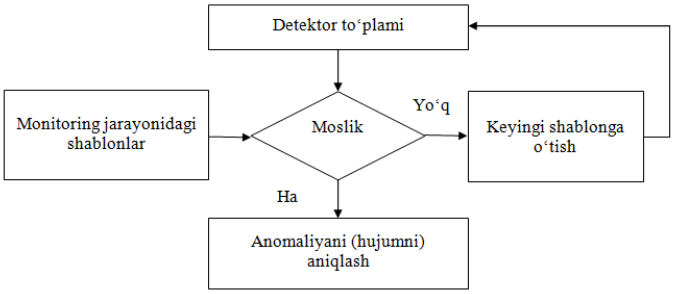
$$P_M = \frac{1}{m^{l-r+1}} \sum_{k=r}^{l} \binom{l-k+1}{1} \frac{(m-1)^{l-k}}{m^{l-k}} \quad (6)$$

bu yerda:

- m – alfavitdagi belgilar soni, ya’ni har bir pozitsiyada yoziladigan sonlar diapazoni (yuqorida ko‘rib chiqilgan holatda, m=133);
- l – satr uzunligi;
- r – satrlarning moslik sharti bajarilishini tekshirishda hisobga olinadigan yonma-yon pozitsiyalardagi bir xil qiymatlar soni.

Detektorlarni yaratish uchun hisoblash xarajatlarini kamaytirish maqsadida, aslida, turli yondashuvlardan foydalanish mumkin, masalan, genetik algoritmlarga asoslangan usul [3].

Tizimning normal harakati haqidagi dastlabki ma’lumotlarni yig‘ish, ya’ni "o‘ziga xos" S - shablonlar to‘plamini tuzish va "begona" R - detektorlar to‘plamini shakllantirishdan keyingi bosqich – jarayon xulq-atvordagi mumkin bo‘lgan anomaliyalarni aniqlash maqsadida real vaqt rejimida ilova ishini bevosita kuzatish (monitoring qilish). Buning uchun tizimga kelib tushayotgan faollik shablonlari (profillari) R dagi detektorlar bilan doimiy ravishda solishtiriladi. Agar r -moslik mavjud bo‘lsa, bu anomaliyani ko‘rsatadi (4-rasm).

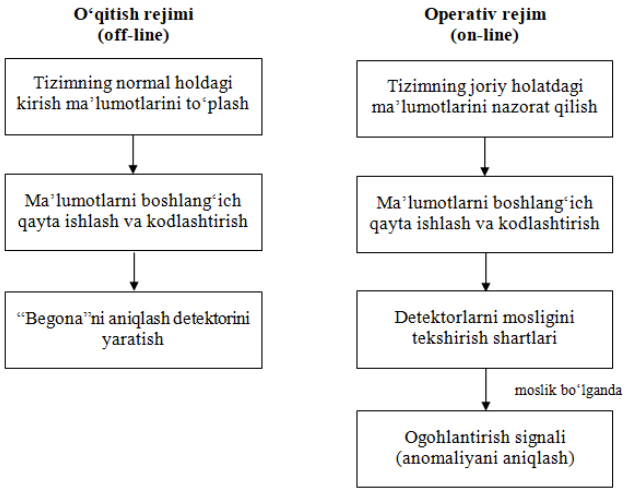


4-rasm. Anomaliyani aniqlash algoritm sxemasi

MUHOKAMA VA NATIJALAR

Shunday qilib, immun tizimi mexanizmlaridan foydalanishga asoslangan anomaliyalarni aniqlash tizimining umumiy ish sxemasi quyidagi ko‘rinishni oladi (5-rasm). Bu yerda tizimning ikkita asosiy ish rejimi ko‘rsatilgan:

- O‘qitish rejimi (off-line rejimi)**:** Tizim xulq-atvori haqidagi katta hajmdagi dastlabki ma’lumotlarni to‘plash va tahlil qilish bilan bog‘liq bo‘lib, shu sababli vaqt bo‘yicha ancha xarajatli hisoblanadi.
- Operativ rejim (on-line rejimi): Yuzaga kelayotgan anomaliyalarni aniqlash maqsadida ilovalar bilan ishlashda joriy faollikni monitoring qilishdan iborat.

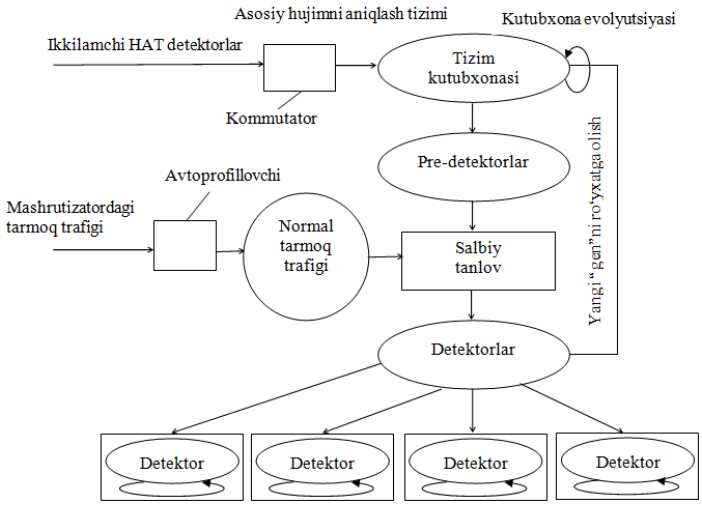


5-rasm. Anomaliyani aniqlash tizimining ishlash sxemasi

Anomaliyalarni aniqlash muammosini hal qilishga yuqorida ko‘rib chiqilgan, salbiy tanlash algoritmiga asoslangan yondashuvning o‘ziga xos xususiyati shundaki, u aniq bir anomaliyalarni emas, balki normadan chetlanishlarni izlashga qaratilgan. Boshqacha aytganda, bu usul yangi ma’lumotlar shablonlarini biron bir buzilishlar sinfiga mos kelish-kelmasligini tekshirmaydi, balki bu shablonlarning normal shablonlarga nisbatan yangi ekanligini qayd etadi.

Tizimlarni monitoring qilishning ko‘pchilik holatlarida, ma’lumotlar shablonidagi asta-sekinlik bilan yuz beradigan o‘zgarishlarni aniqlash, noto‘g‘ri yoki o‘zgartirilgan ma’lumotlarni aniqlashdan ko‘ra muhimroq vazifa hisoblanadi. Shu sababli, tasvirlangan ehtimoliy algoritm mavjud yondashuvlarga foydali muqobil hisoblanadi. Bu holatda foydalaniladigan tasodifiy yaratilgan detektorlar to‘plami, axborot tizimining normal xulq-atvori uning eskirishi yoki modernizatsiya qilinishi jarayonida o‘zgarishi bilan, yangi detektorlarni yaratish orqali davriy ravishda yangilanib turishi mumkin.

Yuqorida bayon qilingan immun tizimining faoliyat modellaridan foydalanilgan holda, tarmoqning bir segmenti uchun qurilgan anomaliyalarni aniqlash tizimining bazaviy arxitekturasi 6-rasmda keltirilgan.



6-rasm. Sun’iy immun tizimlari asosidagi anomaliyalarni aniqlash tizimining arxitekturasi

Ushbu tizim asosan 2 ta analoglardan iborat bo‘ladi: orqa miya limfa tugunlari [4]. Asosiy tizimda sun’iy immun tizimining ikkita jarayon imitatsiyasi, ya’ni gen kutubxonasining evolyusiyasi va salbiy tanlovdan foydalaniladi.

Gen kutubxonasi evolyusiyasi bosqichida tarmoq trafigi anomaliyalarining xususiyatlari haqidagi ma’lumotlar to‘planadi. Sun’iy immun tizimining gen kutubxonasi paketlarning xos xususiyatlari – ularning soni, uzunligi, tuzilishi, tipik xatolari va hokazolar haqidagi ma’lumotlarni o‘z ichiga olishi kerak, ular asosida detektorlar (limfotsitlar analoglari) yaratiladi. Gen kutubxonasini shakllantirish uchun dastlabki ma’lumotlar qo‘llaniladigan tarmoq protokollarining xususiyatlaridan, xususan, ularning himoya nuqtai nazaridan zaif tomonlaridan kelib chiqadi. Keyinchalik, detektorlar tarmoqda anomal faollikni aniqlaganda, kutubxona ushbu anomaliyalarga mos keladigan yangi "genlar" bilan to‘ldiriladi.

Keyingi bosqichda, "genlarni" ixtiyoriy ravishda birlashtirish orqali pre-detektorlar - "embrional" limfotsitlar analoglari hosil qilinadi. Ular salbiy tanlov algoritmi yordamida normal tarmoq trafigi shablonlari bilan mos kelishi yoki kelmasligi tekshiriladi. Bunda tarmoq segmentining kirish qismida joylashgan marshrutizatordan keladigan ma’lumotlar oqimini doimiy ravishda tahlil qiluvchi

avtomatik profayler tomonidan shakllantirilgan ma’lumotlardan foydalaniladi.

Salbiy tanlov algoritmidan foydalanib, keyinchalik maksimal tarmoq anomaliyalarini aniqlash mumkin bo‘lgan detektorlar to‘plami yaratiladi. Ushbu to‘plam tarmoq tugunlariga yuboriladi. Anomaliya aniqlanganda klonal seleksiya amalga oshiriladi – unga mos keladigan detektor "klonlanadi" va barcha tugunlarga yuboriladi. Tarmoqqa hujum bo‘layotganligi yoki yo‘qligi haqidagi yakuniy qaror bir nechta tugunlardan olingan ma’lumotlar asosida qabul qilinadi. Har bir tugun bir komponentni – kommunikatorni o‘z ichiga oladi. Agar biron bir tugunda shubhali faollik kuzatilsa, kommunikator o‘z risk darajasini oshiradi va tegishli xabarni boshqa tugunlar va asosiy tizim kommunikatorlariga yuboradi, ular ham o‘z risk darajalarini oshiradilar. Agar qisqa vaqt ichida bir nechta tugunlarda anomaliyalar paydo bo‘lsa, bu daraja tez o‘sadi. Agar risk ma’lum bir chegaraga erishilsa, tarmoq administratori darhol xavotir signalini oladi.

Sun’iy immun tizimlarini yaratish sohasidagi quyidagi amaliy ishlanmalar mavjud [6].

Lisys tarmoq anomaliyalarini aniqlash tizimi – TCP SYN trafigini nazorat qilishni ta’minlaydi. Tizim "data-path triple", ya’ni manba va IP-manzillari, shuningdek portlarni nazorat qiluvchi 49 bayt hajmdagi taqsimlangan detektorlardan iborat. Dastlab, detektorlar tasodifiy ravishda yaratiladi va ish jarayonida normal trafikka mos keladiganlari asta-sekin o‘chiriladi. Bundan tashqari, detektorlarning "yashash vaqti" bor. Xotiraga yozilganlardan tashqari, ularning butun to‘plami ma’lum vaqt o‘tgach qayta yaratiladi. Soxta signallar sonini kamaytirish uchun faollashtirish chegarasi qo‘llaniladi, bu chegaradan oshish datchikning ishlashiga olib keladi. Bu faollashtirish chegarasi butun tarmoq uchun umumiydir. G‘ayrioddiy ruxsatsiz davlat aloqalari ulanishlari aniqlanganda, tizim administratorga elektron pochta orqali ogohlantirish yuboradi. Agar anomaliya tasdiqlansa, detektor to‘plamning bir qismiga aylanadi va shunga o‘xshash ulanish aniqlanganda foydalanuvchini har safar ogohlantirib turadi.

Homeostasis Process (HP) tizimi – Linux yadrosiga qo‘shimcha bo‘lib, ilova dasturlarining g‘ayrioddiy harakatlarini aniqlash imkonini beradi. Bunday anomaliyalarni aniqlash uchun, avvalo, turli dasturlar tomonidan amalga oshirilgan tizim chaqiruvlarining shablonlari yaratiladi. Bunday shablonni yaratish uchun ma’lum vaqt ketadi, shundan so‘ng dastur mustaqil ravishda ishlay oladi, avval anomal chaqiruvlar uchun vaqtni kechiktirib, so‘ngra bu jarayonlarni butunlay bartaraf etadi. Barcha tizim chaqiruvlarini nazorat qilish maqsadga muvofiq emas, shu sababli tizim faqat kompyuter resurslariga to‘liq kirish imkoniyatiga ega bo‘lgan tizim chaqiruvlari bilan ishlaydi.

STIDE (Sequence Time - Delay Embedding) tarmoq tizimining o‘xshash loyihasi – tizim chaqiruvlarining g‘ayrioddiy ulanishlarini aniqlash orqali kiberhujumlarni aniqlashga yordam berishga mo‘ljallangan. O‘qitish jarayonida STIDE barcha noyob, uzluksiz tizim chaqiruvlaridan ma’lumotlar bazasini shakllantiradi va keyinchalik ularni oldindan belgilangan qat’iy uzunlikdagi qismlarga ajratadi. Ish vaqtida STIDE yangi g‘ayrioddiy ulanishlarni ma’lumotlar bazasida mavjud bo‘lganlar bilan solishtiradi va anomaliya aniqlangani haqida xabar beradi.

Kompyuter immun tizimlarini yaratish bo‘yicha boshqa loyihalar ham mavjud, masalan, Computational Immunology for Fraud Detection (CIFD) loyihasi (http://www.icsa.ac.uk/CIFD), uning maqsadi Angliya pochta xizmati uchun su’niy immun tizimi texnologiyasi asosida axborot himoyasi tizimini ishlab chiqishdir.

XULOSA

Axborot tizimining anomal harakatlarini aniqlash jarayonida ma’lumotlarni tahlil qilish va qayta ishlash blokini amalga oshirishda salbiy tanlov algoritmi qo‘llanilishi maqsadga muvofiq. Detektorlarni yaratish jarayonini tezlashtirish uchun genetik algoritmdan foydalangan holda modifikatsiyalangan usulini qo‘llash yaxshi natijani beradi.

Hujum aniqlanganda, faol audit tizimi uni neytrallash usuli haqida qaror qabul qiladi. Tegishli qaror mantiq algoritmi asosida, tahdid ostidagi ob’ekt turi va hujumning bajarilish shartlarini hisobga olgan holda qabul qilinadi.

Immun javob usulining amalga oshirilishi tegishli apparat-dasturiy yechimga yetkaziladi. Kompyuter hujumlariga qarshi kurashish tizimi markazlashgan "genlar kutubxonasi"ni o‘z ichiga oladi, u potensial begona hodisalarni tavsiflovchi cheklangan vektorlar to‘plamini shakllantiradi, shuningdek, axborot-texnik ta’sirlarni bevosita aniqlash va bostirishni amalga oshiruvchi va "genlar kutubxonasi" bilan teskari aloqaga ega bo‘lgan sensorlar tizimini ham o‘z ichiga oladi. Tajribalar shuni ko‘rsatdiki, immun javob usuli yordamida hujumlarni aniqlashning to‘liqligi 95% ga yetdi. Taqqoslash uchun, signatura tahlili usulidan foydalanganda bu ko‘rsatkich atigi 50% dan sal ko‘proq, harakatlar bloklagichidan foydalanganda esa 80% ni tashkil etgan.

FOYDALANILGAN ADABIYOTLAR

1. Davlatova D. Axborot tizimlari anomaliyalarini sun’iy immun tizimlar asosida aniqlash mexanizm va algoritmlari //Nordic_Press. – 2024. – Т. 3. – №. 0003.

2. Мухториддинов М., Акбаров Н., Умаров Ш. Machine learning for network security and anomaly detection //Conference on Digital Innovation:" Modern Problems and Solutions. – 2023.

3. Kumaravel H. V. An anomaly-based intrusion detection system based on artificial immune system (AIS) techniques : дис. – Purdue University, 2016.

4. Селеменев А. В., Астахова И. Ф., Трофименко Е. В. Применение искусственных иммунных систем для обнаружения сетевых вторжений //Вестник ВГУ. Серия: Системный анализ и информационные технологии. – 2019. – №. 2. – С. 49-56.

5. Umarov S., Umarova M. Axborotni himoya qilishda sun’iy immun tizimlar ahamiyati va roli. *Digital transformation and artificial intelligence*, *3*(4), 29-34. – 2025.

6. Bejoy B. J. et al. A generic cyber immune framework for anomaly detection using artificial immune systems //Applied Soft Computing. – 2022. – Т. 130. – С. 109680.

7. Salah Sobh T. Anomaly detection based on hybrid artificial immune principles //Information Management & Computer Security. – 2013. – Т. 21. – №. 4. – С. 288-314.

8. Umarov S. A. et al. The need and importance of using antiviral defense systems based on artificial immune systems //Miasto Przyszłości. – 2025. – Т. 61. – С. 543-548.

9. Yinka-Banjo C. et al. Intrusion detection using anomaly detection algorithm and snort //Illumination of Artificial Intelligence in Cybersecurity and Forensics. – Cham : Springer International Publishing, 2022. – С. 45-70.

10. Das R. K. et al. Application of artificial immune system algorithms in anomaly detection //Progress in Computing, Analytics and Networking: Proceedings of ICCAN 2017. – Singapore : Springer Singapore, 2018. – С. 687-694.

11. Бурлаков М. Е., Ивкин А. Н. Система обнаружения вторжения на основе искусственной иммунной системы //Вестник Пермского национального исследовательского политехнического университета. Электротехника, информационные технологии, системы управления. – 2019. – №. 29. – С. 209-224.