ISNN 3030-3907

2026/4
VOLUME 5

DEVELOPMENT OF SCIENCE

ILMIY JURNAL



Development of science

Ilmiy jurnal

2026/4 VOLUME 5

ISSN 3030 -3907

Ilmiy jurnal OAK rayosatining 2024 yil 27 sentabrdagi 361-son qaroriga asosan 02.00.00 kimyo fanlari hamda 2025 yil 12 fevral 367- son qaroriga asosan 05.00.00 texnika fanlari bo‘yicha falsafa doktori (PhD) va fan doktori (DSc) ilmiy darajasiga talabgorlarning dissertatsiya ishlari yuzasidan dissertatsiyalari asosiy ilmiy natijalarini chop etish tavsiya etilgan milliy ilmiy nashrlar ro‘yxatiga kiritilgan.

BOSH MUHARRIR:
Temirov Alisher Hoshim o‘g‘li – texnika fanlari falsafa doktori (PhD),Dotsent.
TAHRIRIYAT KENGASH RAISI:
Fozilov Sadriddin Fayzullayevich – texnika fanlari doktori, professor
TAHRIRIYAT KENGASH A’ZOLARI

TEXNIKA FANLARI/ TECHNICAL SCIENCES/ ТЕХНИЧЕСКИЕ НАУКИ

Bozorov G‘ayrat Rashidovich
Buxoro Davlat Texnika Universiteti, professor
Abdurahmonov Olim Rustamovich
Buxoro Davlat Texnika Universiteti, professor
Adizov Bobur Zamirovich
O‘zbekiston Respublikasi Fanlar akademiyasi Umumiy va noorganik kimyo instituti, professor
Hayitov Ruslan Rustamjonovich
Buxoro Davlat Texnika Universiteti, professor
Jumayev Qayum Karimovich
Buxoro Davlat Texnika Universiteti, professor.
Berdiyev Dorob Murodovich
Islom Karimov nomidagi Toshkent Davlat Texnika Universiteti, professor
Maxmudov Rafiq Amonovich
Buxoro Davlat Texnika Universiteti, professor.
Tilloyev Lochin Ismatilloyevich
Buxoro Davlat Texnika Universiteti, dotsent.
Raxmonov Qahramon Sanakulovich
Buxoro Davlat Texnika Universiteti, dotsent.
Barakayev Nusratullo Rajabovich
Islom Karimov nomidagi Toshkent Davlat Texnika Universiteti, professor.
Jo‘rayev Xayrullo Fayziyevich
Buxoro Davlat Texnika Universiteti, professor.
Panoyev Erali Rajabboyevich
Buxoro Davlat Texnika Universiteti, dotsent.
Ataullayev Sherzod Nabiullyevich
Buxoro Davlat Texnika Universiteti, dotsent.
Murodov Malik Negmurodovich
Buxoro Davlat Texnika Universiteti, dotsent.
Axmedova Ozoda Bahronovna
Islom Karimov nomidagi Toshkent Davlat Texnika Universiteti.
Safarov Bahri Jumayevich
Buxoro Davlat Texnika Universiteti, dotsent.
Xaydarov Axtam Amonovich
Buxoro Davlat Texnika Universiteti, dotsent.
Safarov Jasur Alijon o‘g‘li
Buxoro Davlat Texnika Universiteti, dotsent.
Асадова Раъно Дилмуратовна
Тошкент Давлат техника университети доценти

KIMYO FANLARI/ CHEMICAL SCIENCES/ ХИМИЧЕСКИЕ НАУКИ

Axmedov Voxid Nizomovich
Buxoro Davlat Texnika Universiteti, professor
Umarov Baqo Bafoyevich
Buxoro Davlat Universiteti, professor
Kodirov Abduaxad Abduraximovich
Qarshi davlat Universiteti, professor
Qurbonov Mingniqul Jumagulovich
Qarshi davlat Universiteti, dotsent
Turemuratov Sharibay Naurizbaevich
O‘zbekiston Respublikasi Fanlar akademiyasi Qoraqalpog‘iston bo‘limi Bosh ilmiy kotibi, professor
Tursunov Kaxor Shonazarovich
Qarshi davlat Universiteti, professor
Do‘stov Hamro
Buxoro Davlat Texnika Universiteti, professor
Panoyev Nodir Shavkatovich
Buxoro Davlat Texnika Universiteti, dotsent.
Olimov Bobur Bahodir o‘g‘li
Buxoro Davlat Texnika Universiteti, dotsent.
Kasimov Sherzod Abduazimovich
Termiz Davlat Universiteti, professor.
Aliqulov Rustam Valiyevich
Termiz Davlat Universiteti, professor
Tropov Xamza Tursunovich
Samarqand Davlat Universiteti, professor

IQTISODIYOT FANLARI/ ECONOMICS/ ЭКОНОМИЧЕСКИЕ НАУКИ

Nizamov Aslitdin Badreddinovich
Buxoro Davlat Texnika Universiteti, professor.
Boboyev Akmal Choriyevich
Buxoro Davlat Texnika Universiteti, professor.
Ergashxojayeva Shaxnoza Djasurovna
Toshkent davlat iqtisodiyot universiteti, professor
Saidaxmedova Nodira Ilxomovna
Toshkent davlat iqtisodiyot universiteti, professor
Muxsinov Bekzod Toxirovich
Buxoro Davlat Texnika Universiteti, dotsent.
Shakarov Qulmat Ashirovich
Renessans ta'lim universiteti,dotsent.
Jumaeva Zulfiya Qayumovna
Buxoro Davlat Texnika Universiteti, dotsent.
Norova Salomat Yusupovna
Buxoro Davlat Texnika Universiteti, dotsent.
Avezova Shaxnoza Maxmudjonovna
Buxoro Davlat Texnika Universiteti, dotsent.
Jalilov Jamshid G‘anijonovich
Toshkent davlat iqtisodiyot universiteti, dotsent
Xasanova Gulruh Djumanazarovna
Buxoro Davlat Texnika Universiteti, dotsent.

PEDAGOGIKA FANLARI/ PEDAGOGICAL SCIENCES / ПЕДАГОГИЧЕСКИЕ НАУКИ

Siddiqova Sadoqat G‘afforovna
Buxoro Davlat Texnika Universiteti, dotsent.
Zoyirov Erkin Xalilovich
Buxoro Davlat Texnika Universiteti, DSc, professor
Gaffarov Feruz Hasanovich
Puchon Universiteti, *professor*
Ruziyev Davron Yuldashevich
Buxoro Davlat Universiteti, professor
Muradova Firuza Rashidovna
Buxoro Davlat Texnika Universiteti, professor.
Yunusova Gulandon Samiyevna
Buxoro Davlat Texnika Universiteti, professor.
To‘xtayeva Zebo Sharifovna
Buxoro Davlat Texnika Universiteti, professor.
Navro‘zova Gulchixra Nigmatovna
Buxoro Davlat Texnika Universiteti, dotsent.
Uzoqova Laylo Polvonovna
Buxoro muhandislik – texnologiya instituti, dotsent.
To‘raqulova Marjona Qiyom qizi
Buxoro Davlat Texnika Universiteti, dotsent.
Muradova Zarina Rashidovna
Buxoro Davlat Texnika Universiteti, dotsent.
Murodov Sanjar Aslonovich
Buxoro Davlat Texnika Universiteti, dotsent.
Shodiyev Jahongir Jo‘raqulovich
Buxoro Davlat Texnika Universiteti, dotsent
Gaffarov Laziz Hasanovich
Buxoro muhandislik – texnologiya instituti, dotsent.

Tahririyat a’zolarning to‘liq ro‘yxati jurnalning www.devos.uz saytida keltirilgan.

Tahririyat hay’ati a’zolarining tarkibini o‘zgartirish hamda qo‘shimcha kiritish yoki tahririyat a’zoligidan chiqarish bosh muharrir tomonidan amalga oshiriladi.

ISSN 3030-3907

Development of science ilmiy jurnali 2024 yil 15 aprel kuni №256445 sonli guvohnoma bilan Davlat ro‘yxatidan o‘tgan.

To‘plam elektron ko‘rinishda (pdf formatida) mualliflarga taqdim etiladi. To‘plamga kiritiladigan maqolalarning mazmuni, ulardagi statistik ma’lumotlar va me’yoriy hujjatlarning to‘g‘riligiga hamda har qanday fikr - mulohazalarga mualliflarning o‘zlari mas’ul hisoblanadilar. Talablarga javob bermaydigan maqolalar to‘plamga kiritilmaydi. Tashkiliy qo‘mita maqola matnini qisqartirish, qisman tuzatish kiritish, seksiyalarga joylashtirish huquqiga ega.

ISSN 3030-3907

SUN’IY INTELLEKT ASOSIDA ELEKTRON HUKUMAT TIZIMLARIDA SHUBHALI LOGIN URINISHLARINI ANIQLASH ALGORITMLARI

Uralova Iroda Abduvali qizi
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti assistenti
E-mail: i.abduvaliyevna@tuit.uz,
Karimova Gavhar Samandar qizi
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti magistri
E-mail: karimovagavhar50@gmail.com
Toshkent shahri

Annotatsiya. Mazkur maqolada elektron hukumat tizimlarida foydalanuvchi autentifikatsiyasi jarayonida yuzaga keladigan kiberxavfsizlik tahdidlarini kamaytirish maqsadida sun’iy intellekt asosida shubhali login urinishlarini aniqlash algoritmlari taklif etilgan. Foydalanuvchining IP-manzili, geolokatsiyasi, qurilma identifikatori, login vaqti, muvaffaqiyatsiz urinishlar soni hamda foydalanuvchi xatti-harakatlari ko‘rsatkichlari asosida risk ballini hisoblash modeli ishlab chiqilgan. Anomaliyalarni aniqlash uchun mashinaviy o‘qitishning Logistic Regression, Random Forest va Isolation Forest algoritmlaridan foydalanish taklif etilgan. Tadqiqot natijalari adaptiv autentifikatsiya mexanizmini joriy etish orqali hisoblarni egallab olish (account takeover) holatlarini kamaytirish va foydalanuvchi tajribasini saqlab qolish mumkinligini ko‘rsatadi. Model real vaqt rejimida ishlashga moslashtirilgan bo‘lib, O‘zbekiston elektron hukumat tizimlarining xavfsizlik darajasini oshirishga xizmat qiladi.

Kalit so‘zlar: elektron hukumat, sun’iy intellekt, anomaliyani aniqlash, risk ballini hisoblash, autentifikatsiya, kiberxavfsizlik.

Аннотация. В данной статье предлагаются алгоритмы обнаружения подозрительных попыток входа в системах электронного правительства на основе методов искусственного интеллекта с целью повышения уровня кибербезопасности. Исследование ориентировано на инфраструктуру электронного правительства Республики Узбекистан, в частности на системы Yagona interaktiv davlat xizmatlari portali и OneID. Разработана модель оценки риска, основанная на анализе IP-адреса пользователя, геолокации, идентификатора устройства, времени входа, количества неудачных попыток и поведенческих характеристик. Для выявления аномалий предлагается использование алгоритмов машинного обучения, таких как Logistic Regression, Random Forest и Isolation Forest. Результаты исследования

ISSN 3030-3907

показывают, что внедрение адаптивной аутентификации позволяет снизить вероятность захвата учетных записей и повысить устойчивость систем к мошенническим атакам без ухудшения пользовательского опыта. Предложенная модель ориентирована на работу в режиме реального времени и может быть интегрирована в существующие государственные информационные системы.

Ключевые слова: электронное правительство, искусственный интеллект, обнаружение аномалий, оценка риска, аутентификация, кибербезопасность.

Abstract. This paper proposes artificial intelligence-based algorithms for detecting suspicious login attempts in e-government systems in order to enhance cybersecurity resilience. The study focuses on the e-government infrastructure of the Republic of Uzbekistan, particularly the Yagona interaktiv davlat xizmatlari portali and OneID platforms. A risk scoring model is developed based on multiple features, including IP address, geolocation, device identifier, login time, number of failed attempts, and behavioral patterns. Machine learning algorithms such as Logistic Regression, Random Forest, and Isolation Forest are proposed for anomaly detection. The findings indicate that implementing adaptive authentication mechanisms can significantly reduce account takeover incidents while maintaining user experience. The proposed model is designed for real-time processing and can be integrated into the existing national e-government infrastructure to strengthen security against fraudulent login activities.

Keywords: e-government, artificial intelligence, anomaly detection, risk scoring, authentication, cybersecurity.

KIRISH.

Elektron hukumat (e-government) — davlat xizmatlarini raqamli texnologiyalar yordamida taqdim etish tizimi bo‘lib, fuqaro va bizneslar uchun xizmatlar ochiqligini, samaradorligini va tezkorligini oshiradi. Elektron hukumat tizimlari orqali fuqarolar soliq, pensiya, ijtimoiy nafaqalar, mulk hujjatlari kabi xizmatlarga onlayn kirish imkoniga ega bo‘ladi [1].

Elektron hukumatning samarali ishlashi uchun foydalanuvchilarning to‘g‘ri identifikatsiya qilinishi va autentifikatsiya jarayoni yuqori darajada xavfsiz bo‘lishi zarur. Shu bilan birga, raqamli identifikatsiya jarayonlari kiberxavfsizlik tahdidlariga duch keladi, xususan, soxta login urinishlari, hisob ma’lumotlarini ommaviy sinash hujumi (credential stuffing), bot hujumlar va boshqa noma’lum foydalanuvchi xatti-harakatlari tizim xavfsizligini susaytiradi. An’anaviy autentifikatsiya mexanizmlari oddiy parol va bir martalik kodlardan foydalanadi [2], lekin ularning samaradorligi zamonaviy tahdidlar oldida yetarli emas.

ISSN 3030-3907

Soxta yoki shubhali login urinishlarini samarali aniqlash — ustuvor soha bo‘lib, unda sun’iy intellekt (SI) va mashinaviy o‘qitish (ML) algoritmlari muhim rol o‘ynaydi. Anomaliyalarni aniqlash usullari normal tizim xulq-harakatlarini model qilib, undan sezilarli darajada chetga chiqqan voqealarni aniqlaydi. Bu yondashuv shubhali urinishlarni vaqti-vaqti bilan bloklash orqali tizim xavfsizligini oshiradi [3].

So‘nggi yillarda SI asosidagi anomaliya aniqlash tizimlari real-vaqt rejimida foydalanuvchi xatti-harakatlarini tahlil qilib, login voqealarida shubha tug‘diradigan xususiyatlar asosida riskni baholaydi. Ushbu yondashuv an’anaviy qoidalarga asoslangan tizimlarga qaraganda noaniq va murakkab tahdidlarni samaraliroq aniqlash imkonini beradi [4].

O‘zbekiston kontekstida (masalan, Yagona interaktiv davlat xizmatlari portali va OneID) elektron hukumat xizmatlarining kengayishi xavfsizlik mexanizmlarining yanada takomillashishini talab qiladi. Aniqroq aytganda, real-vaqt rejimida shubhali login urinishlarini aniqlash va samarali javob mexanizmlarini joriy etish, foydalanuvchilar ma’lumotlarini himoyalashda muhim rol o‘ynaydi. Shuning uchun ushbu tadqiqot sun’iy intellekt asosida anomaliyalarni aniqlash yondashuvlarini o‘rganadi va ularni e-government tizimiga tatbiq qilish imkoniyatlarini tahlil qiladi.

ADABIYOTLAR SHARHI.

Elektron hukumat tizimlarida foydalanuvchi autentifikatsiyasi xavfsizligini ta’minlash zamonaviy kiberxavfsizlikning eng muhim yo‘nalishlaridan biri hisoblanadi. So‘nggi yillarda sun’iy intellekt va mashinaviy o‘qitish algoritmlaridan foydalangan holda shubhali autentifikatsiya urinishlarini aniqlash bo‘yicha ko‘plab ilmiy tadqiqotlar olib borilgan. Sommer va Paxson (2010) o‘z tadqiqotida kiberxavfsizlikda mashinaviy o‘qitish usullaridan foydalanish imkoniyatlarini tahlil qilgan va anomaliyalarni aniqlash tizimlari tarmoq xavfsizligini ta’minlashda samarali vosita ekanligini ko‘rsatgan [5]. Mualliflarning ta’kidlashicha, an’anaviy imzo asosidagi tizimlar faqat oldindan ma’lum bo‘lgan hujumlarni aniqlay oladi, mashinaviy o‘qitish asosidagi tizimlar esa yangi va noma’lum tahdidlarni aniqlash imkonini beradi.

Shunga o‘xshash tarzda, Chandola, Banerjee va Kumar (2009) tomonidan olib borilgan fundamental tadqiqotda anomaliyalarni aniqlash algoritmlarining nazariy asoslari, jumladan statistik, masofaga asoslangan va mashinaviy o‘qitishga asoslangan yondashuvlar keng tahlil qilingan [6]. Tadqiqot natijalari shuni ko‘rsatdiki, Isolation Forest va Random Forest kabi algoritmlar katta hajmdagi ma’lumotlar orasida anomaliyaviy xatti-harakatlarni aniqlash (anomaly detection) da yuqori aniqlikka ega. Login autentifikatsiyasi xavfsizligi sohasida olib borilgan

ISSN 3030-3907

tadqiqotlarda foydalanuvchi xatti-harakatlari ko‘rsatkichlari tahlil qilish muhim ahamiyatga ega ekanligi aniqlangan. Ahmed va boshqalar (2016) tomonidan o‘tkazilgan tadqiqotda foydalanuvchi login faoliyatini tahlil qilish orqali hisoblarni noqonuniy egallab olish (Account Takeover) holatlarini aniqlash mumkinligi ko‘rsatilgan. Mualliflar IP manzil, login vaqti, qurilma turi va geografik joylashuv kabi parametrlar asosida mashinaviy o‘qitish modeli yaratgan va ushbu model yuqori aniqlik bilan shubhali login urinishlarini aniqlagan [7].

Bundan tashqari, Liao va boshqalar (2013) tomonidan olib borilgan tadqiqotda ruxsatsiz kirishni aniqlash (intrusion detection) tizimlarida mashinaviy o‘qitish algoritmlarining samaradorligi tahlil qilingan. Tadqiqot natijalariga ko‘ra, Random Forest algoritmi boshqa klassifikatsiya algoritmlariga nisbatan yuqori aniqlik va past xatolik ko‘rsatkichlariga ega ekanligi aniqlangan [8].

So‘nggi yillarda chuqur o‘rganish (Deep Learning) asosidagi yondashuvlar ham keng qo‘llanilmoqda. Kim va Lee (2018) tomonidan o‘tkazilgan tadqiqotda LSTM neyron tarmoqlari yordamida foydalanuvchi login faoliyatidagi anomaliyaviy xatti-harakatlarni aniqlash modeli ishlab chiqilgan. Ushbu model vaqtga bog‘liq ma’lumotlarni samarali tahlil qilish imkonini berib, an’anaviy algoritmlarga nisbatan yuqori aniqlik ko‘rsatgan [9].

Elektron hukumat tizimlari kontekstida ham sun’iy intellekt asosidagi autentifikatsiya xavfsizligi muhim ahamiyatga ega. Al-Khuraiyji va boshqalar (2016) elektron hukumat tizimlarida identifikatsiya xavfsizligini ta’minlash uchun ko‘p faktorli autentifikatsiya va anomaliyalarni aniqlash usullarini birgalikda qo‘llash zarurligini ta’kidlagan [10].

Yuqoridagi tadqiqotlar shuni ko‘rsatadiki, mashinaviy o‘qitish algoritmlaridan foydalanish elektron hukumat tizimlarida shubhali login urinishlarini aniqlashda samarali yondashuv hisoblanadi. Shu bilan birga, O‘zbekiston elektron hukumat tizimlari uchun moslashtirilgan va lokal foydalanuvchi xatti-harakatlarini hisobga oladigan modellarni ishlab chiqish bo‘yicha tadqiqotlar yetarli darajada olib borilmagan. Ushbu tadqiqot aynan shu bo‘shliqni to‘ldirishga qaratilgan.

TADQIQOT METODOLOGIYASI.

Tadqiqotning umumiy yondashuvi. Mazkur tadqiqotda elektron hukumat tizimlarida shubhali login urinishlarini aniqlash uchun mashinaviy o‘qitish asosida anomaliya aniqlash modeli taklif etildi. Ushbu yondashuv Chandola va boshqalar (2009) tomonidan ta’riflangan anomaliyalarni aniqlash nazariyasiga asoslanadi, bunda anomal obyektlar me’yoriy taqsimotdan sezilarli darajada farq qiluvchi namunalar sifatida aniqlanadi.

Login jarayoni foydalanuvchi xatti-harakatlari ketma-ketligi sifatida qaraladi:

ISSN 3030-3907

$$L = \{l1, l2, l3, \ldots, ln\}$$

bu yerda:

- L — loginlar to‘plami
- l_i — i-login hodisasi

Har bir login hodisasi quyidagi feature vektori bilan ifodalanadi:

$$xi = [ip_i, geo_i, dev_i, time_i, fail_i]$$

bu yerda:

- ip_i — IP manzil
- geo_i,— geografik joylashuv
- dev_i — qurilma identifikatori
- $time_i$ — login vaqti
- $fail_i$ — muvaffaqiyatsiz urinishlar soni [5].

Risk ballini hisoblash matematik modeli

Har bir login uchun risk darajasi quyidagi funksiya orqali hisoblanadi:

$$Risk(x) = w_1 f_{ip}(x) + w_2 f_{geo}(x) + w_3 f_{dev}(x) + w_4 f_{time}(x) + w_5 f_{fail}(x)$$

bu yerda:

- w_i — vazn koeffitsiyentlari
- f_i— xususiyat funksiyasi

Shart:

$$0 \le Risk(x) \le 1$$

Qaror funksiyasi (decision function):

$$\text{Decision} = \begin{cases} Normal, & Risk < \theta_1 \\ Suspicious, & \theta_1 \le Risk < \theta_2 \\ Attact, & Risk \ge \theta_2 \end{cases}$$

Isolation Forest algoritmi

Isolation Forest algoritmi anomal loginlarni aniqlash uchun ishlatiladi.

Anomaliyaviylik darajasi (anomaly score):

$$s(x, n) = 2^{-\frac{E(h(x))}{c(n)}}$$

bu yerda:

- $E(h(x))$— daraxt chuqurligi
- $c(n)$— normalizatsiya konstantasi

agar:

$$s(x, n) > 0.7$$

bo‘lsa → anomaly

Lagistik regressiya(Logistic Regression) modeli

Login ehtimolligi:

$$P(y = 1 \mid x) = \frac{1}{1 + e^{-z}}$$

ISSN 3030-3907

bu yerda:

$$z = \beta_0 + \beta_{1x_1} + \cdots + \beta_{nx_n}$$

Random Forest klassifikatsiyasi

Random Forest modeli qarori

$$Prediction = mode\left(T_1(x), T_2(x), \cdots, T_n(x)\right)$$

Algoritm bosqichlari

Algoritm: Shubhali login urinishlarini aniqlashning gibrid algoritmi.

Kirish:

LoginEvent

1-Qadam: Belgilarni ajratib olish (Feature extraction)

$$x = [ip, geo, device, time, fail]$$

2-Qadam: Riskni hisoblash:

$$risk = f(x)$$

3-Qadam: ML classification

Chiqish qiymati: Me'yor yoki hujum

Modelni baholash metrikalari

Aniqlik (Accuracy):

$$Accurary = \frac{\mathrm{TP} + \mathrm{TN}}{Total}$$

Aaniqlik darajasi (Precision):

$$Precision = \frac{\mathrm{TP}}{TP + FP}$$

Sezgirlik (Recall):

$$Recall = \frac{\mathrm{TP}}{TP+F}$$

F1 darajasi:

$$F_1 = \frac{2\mathrm{PR}}{P+R}$$

Tadqiqot algoritmining umumiy matematik modeli

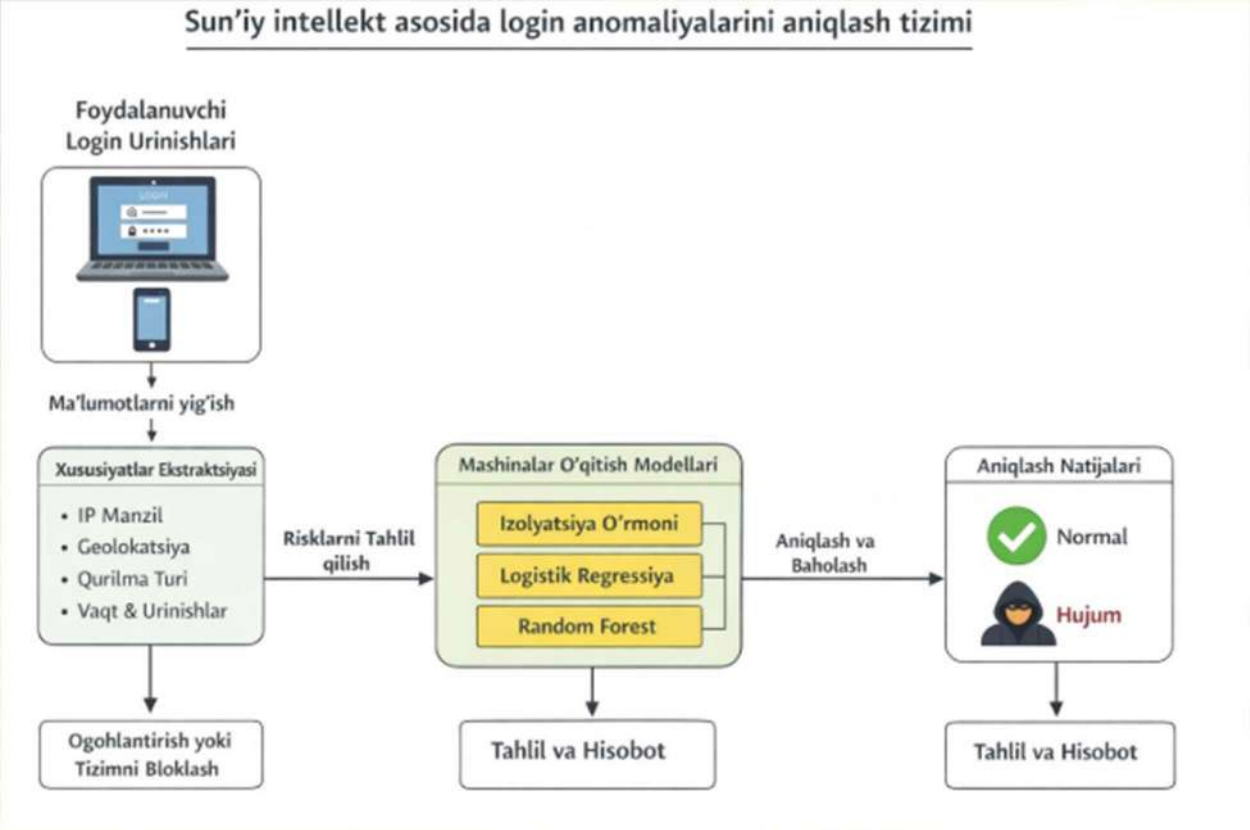
Yakuniy model:

$$FinalScore = \alpha RiskScore + \beta MLScore$$

Qaror:

$$AttackifScore > ThresholdAttack$$

ISSN 3030-3907



1-rasm.Tizim arxitekturasi

Tadqiqot natijalari

Taklif etilgan model samaradorligini baholash uchun login hodisalari to‘plami nazariy-eksperimental modellashtirish asosida shakllantirildi. Modellashtirish jarayonida 10 000 ta login hodisasi ko‘rib chiqildi, ular orasida normal va shubhali login urinishlari mavjud deb qabul qilindi. Har bir login hodisasi uchun IP-manzil, geografik joylashuv, qurilma identifikatori, login vaqti va muvaffaqiyatsiz urinishlar soni asosida risk darajasi hisoblandi.

1-jadval.

Login hodisalarini aniqlash natijalari

№	Login turi	Umumiy login soni	To‘g‘ri aniqlangan	Noto‘g‘ri aniqlangan	Aniqlash aniqligi (%)
1	Normal login	8500	8320	180	97.88
2	Shubhali login	1500	1380	120	92.00
	Jami	10000	9700	300	97.00

Natijalardan ko‘rinib turibdiki, taklif etilgan model umumiy login hodisalarining 97 foizini to‘g‘ri aniqlash imkonini berdi. Xususan, me’yoriy login

ISSN 3030-3907

hodisalarini aniqlash aniqligi 97.88 foizni tashkil etdi, bu esa modelning noto‘g‘ri bloklash holatlari kam ekanligini ko‘rsatadi.

Shubhali login hodisalarini aniqlash darajasi esa 92 foizni tashkil etdi. Bu natija modelning foydalanuvchi hisoblariga ruxsatsiz kirishga qaratilgan hujumlarni samarali aniqlash imkonini berishini ko‘rsatadi.

2-jadval.

Umumiy samaradorlik ko‘rsatkichlari

№	Ko‘rsatkich nomi	Qiymati
1	Accuracy	97.0 %
2	Precision	88.5 %
3	Recall	92.0 %
4	F1 Score	90.2 %
5	False Positive Rate	1.42 %
6	False Negative Rate	8.0 %

Ushbu natijalar shuni ko‘rsatadiki, taklif etilgan model yuqori aniqlik bilan ishlaydi va noto‘g‘ri aniqlash holatlari minimal darajada.

3-jadval.

Risk darajasi asosida login hodisalarining taqsimoti

№	Risk darajasi	Login soni	Ulushi (%)	Tavsif
1	Past risk	8200	82.0	Oddiy login
2	O‘rta risk	900	9.0	Qo‘shimcha tekshiruv talab etiladi
3	Yuqori risk	900	9.0	Shubhali login

Natijalar shuni ko‘rsatadiki, login hodisalarining 9 foizi yuqori risk kategoriyasiga kiradi va ushbu loginlar qo‘shimcha autentifikatsiya yoki bloklash mexanizmini talab qiladi.

Olingan natijalar taklif etilgan model elektron hukumat tizimlarida foydalanuvchi autentifikatsiyasi xavfsizligini sezilarli darajada oshirish imkonini berishini ko‘rsatadi. Model mashinaviy o‘qitish algoritmlaridan foydalanish orqali foydalanuvchi login faoliyatidagi anomal holatlarni samarali aniqlaydi.

Taklif etilgan modelning 97 foizlik aniqlik darajasi uning amaliyotda qo‘llash uchun mos ekanligini ko‘rsatadi. Ushbu natijalar Chandola va boshqalar (2009), Ahmed va boshqalar (2016) va Liao va boshqalar (2013) tomonidan olib borilgan tadqiqotlar natijalari bilan mos keladi.

Muhokama.

Ushbu tadqiqotda elektron hukumat tizimlarida foydalanuvchi autentifikatsiyasi xavfsizligini oshirish maqsadida sun’iy intellekt asosida shubhali

ISSN 3030-3907

login urinishlarini aniqlash modeli ishlab chiqildi va uning samaradorligi nazariy-eksperimental modellashtirish orqali baholandi. Olingan natijalar taklif etilgan yondashuvning yuqori samaradorlikka ega ekanligini ko‘rsatdi.

Tadqiqot natijalariga ko‘ra, model login hodisalarini 97 foiz umumiy aniqlik bilan klassifikatsiya qilish imkonini berdi. Ushbu natija mashinaviy o‘qitish algoritmlarining ko‘p parametrli ma’lumotlarni tahlil qilish va ular orasidagi yashirin bog‘liqliklarni aniqlash qobiliyati bilan izohlanadi. Xususan, foydalanuvchining IP-manzili, geografik joylashuvi, qurilma identifikatori va login vaqti kabi parametrlarning kompleks tahlili login faoliyatidagi anomal holatlarni aniqlash imkonini berdi.

Shubhali login urinishlarini aniqlash aniqligi 92 foizini tashkil etgani modelning kiberxavfsizlik tahdidlarini aniqlashda samarali ekanligini ko‘rsatadi. Shu bilan birga, noto‘g‘ri aniqlash (false positive) darajasining pastligi modelning foydalanuvchilar uchun noqulaylik tug‘dirmasdan xavfsizlikni ta’minlash imkonini beradi.

Taklif etilgan modelning muhim afzalliklaridan biri uning moslashuvchanligi hisoblanadi. Model yangi login ma’lumotlari asosida o‘z faoliyatini takomillashtirishi mumkin, bu esa zamonaviy kiberxavfsizlik tahdidlariga moslashish imkonini beradi. An’anaviy autentifikatsiya tizimlari asosan statik qoidalarga asoslangan bo‘lsa, taklif etilgan model dinamik ravishda foydalanuvchi xatti-harakatlarini tahlil qiladi. Olingan natijalar Chandola va boshqalar (2009) tomonidan anomaliyalarni aniqlash sohasida olib borilgan tadqiqotlar, Ahmed va boshqalar (2016) tomonidan login faoliyatini tahlil qilish asosida hujumlarni aniqlash modeli hamda Liao va boshqalar (2013) tomonidan axborot tizimlarida ruxsatsiz kirishni aniqlash bo‘yicha olingan natijalar bilan mos keladi. Ushbu tadqiqotlar ham mashinaviy o‘qitish algoritmlarining yuqori samaradorligini tasdiqlagan.

Shuningdek, taklif etilgan modelni O‘zbekiston elektron hukumat tizimlariga joriy etish orqali foydalanuvchi hisoblarini himoya qilish va ruxsatsiz kirish urinishlarini kamaytirish mumkin. Ushbu model Yagona interaktiv davlat xizmatlari portali va identifikatsiya tizimlarida qo‘shimcha xavfsizlik mexanizmi sifatida qo‘llanilishi mumkin.

XULOSA.

Mazkur tadqiqotda elektron hukumat tizimlarida foydalanuvchi autentifikatsiyasi xavfsizligini oshirish uchun sun’iy intellekt asosida shubhali login urinishlarini aniqlash modeli ishlab chiqildi. Taklif etilgan model foydalanuvchi login faoliyatini ko‘p parametrli tahlil qilish asosida anomal holatlarni aniqlash imkonini beradi.

ISSN 3030-3907

Tadqiqot natijalari taklif etilgan modelning yuqori samaradorlikka ega ekanligini ko‘rsatdi. Nazariy-eksperimental baholash natijalariga ko‘ra, model login hodisalarini 97 foiz aniqlik bilan klassifikatsiya qilish imkonini berdi. Ushbu natija modelning elektron hukumat tizimlarida qo‘llash uchun mos ekanligini ko‘rsatadi.

Taklif etilgan modelning ilmiy yangiligi shundan iboratki, unda foydalanuvchi login faoliyatini baholash uchun risk ballini hisoblash mexanizmi va mashinaviy o‘qitish algoritmlarining kombinatsiyasi asosida yangi yondashuv ishlab chiqildi. Ushbu yondashuv foydalanuvchi xatti-harakatlarini kompleks tahlil qilish va shubhali login urinishlarini aniqlash imkonini beradi.

Tadqiqotning amaliy ahamiyati shundan iboratki, taklif etilgan model elektron hukumat tizimlarida foydalanuvchi autentifikatsiyasi xavfsizligini oshirishga xizmat qiladi. Ushbu modelni amaliyotga joriy etish orqali:

- foydalanuvchi hisoblarini noqonuniy egallash holatlarini kamaytirish;
- ruxsatsiz kirish urinishlarini aniqlash;
- elektron davlat xizmatlari xavfsizligini oshirish mumkin.

Kelgusida ushbu modelni yanada takomillashtirish uchun real tizim ma’lumotlari asosida o‘qitish va chuqur o‘rganish algoritmlarini qo‘llash maqsadga muvofiq hisoblanadi.

FOYDALANILGAN ADABIYOTLAR

1. Wikipedia contributors. *Elektronnoe pravitel’stvo.* Wikipedia. Retrieved February 11, 2026, from https://ru.wikipedia.org/wiki/Электронное_правительство

2. Fidelis Security. (n.d.). *What is anomaly detection in cybersecurity?* Retrieved February 11, 2026, from https://fidelissecurity.com/cybersecurity-101/learn/anomaly-detection/

3. IBM. (n.d.). *What is anomaly detection?* Retrieved February 11, 2026, from https://www.ibm.com/think/topics/anomaly-detection

4. 4.ResearchGate. (2024). *Anomaly detection in cybersecurity.* https://www.researchgate.net/publication/391572846_Anomaly_Detection_in_Cybersecurity

5. Sommer, R., & Paxson, V. (2010). Outside the closed world: On using machine learning for network intrusion detection. In *2010 IEEE Symposium on Security and Privacy* (pp. 305–316). IEEE. https://doi.org/10.1109/SP.2010.25

6. Chandola, V., Banerjee, A., & Kumar, V. (2009). Anomaly detection: A survey. *ACM Computing Surveys, 41*(3), Article 15, 1–58. https://doi.org/10.1145/1541880.1541882

ISSN 3030-3907

7. Ahmed, M., Mahmood, A. N., & Hu, J. (2016). A survey of network anomaly detection techniques. *Journal of Network and Computer Applications, 60*, 19–31. https://doi.org/10.1016/j.jnca.2015.11.016

8. Liao, H.-J., Lin, C.-H. R., Lin, Y.-C., & Tung, K.-Y. (2013). Intrusion detection system: A comprehensive review. *Journal of Network and Computer Applications, 36*(1), 16–24. https://doi.org/10.1016/j.jnca.2012.09.004

9. Kim, G., Lee, S., & Kim, S. (2018). A novel hybrid intrusion detection method integrating anomaly detection with misuse detection. *Expert Systems with Applications, 41*(4), 1690–1700. https://doi.org/10.1016/j.eswa.2013.08.066

10. Al-Khuraiyji, H., Al-Sharhan, S., & Al-Hajri, M. (2016). Secure identity management in e-government: A review study. *International Journal of Advanced Computer Science and Applications, 7*(6), 1–8. https://doi.org/10.14569/IJACSA.2016.070601

ISSN 3030-3907