ISNN 3030-3907

2026
JUNE
ISSUE - 6
VOLUME -5

DEVELOPMENT OF SCIENCE

scientific journal



Development of science

Ilmiy jurnal

IYUN 2026
Issue - 6, 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.

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

КИБЕРХАВФСИЗЛИКДА АНОМАЛИЯЛАРНИ АНИҚЛАШ ТИЗИМЛАРИ

Юнусов Ғанишер Ғафирович
Бухоро инновациялар университети, Ахборот технологиялари ва амалий фанлар кафедраси профессор в.б., т.ф.н.
Хамидов Отабек Сидик ўғли
Бухоро давлат техника университети, магистр

Аннотация. Замонавий ахборот тизимларида кибернавлар сони ва уларнинг мураккаблиги йилдан-йилга ортиб бормоқда. Анъанавий имзоларга асосланган ҳимоя восита-лари янги, илгари маълум бўлмаган ҳужумларга нисбатан кам самарали бўлгани боис, аномалияларни аниқлашга йўналтирилган тизимлар алоҳида аҳамият касб этмоқда. Ушбу мақолада аномалияларни аниқлашнинг статистик, машинали ўқитишга асосланган ва чуқур нейрон тармоқлар ёрдамидаги ёндашувлари тизимли тарзда таҳлил қилинди. Тадқиқот доирасида Z-баҳолар, Маҳаланобис масофаси, Шеннон энтропияси, Изоляция ўрмонлари, автокодлагичлар (autoencoder) ва Кулбак-Лейблер кесишма ўлчови каби математик асбоблар ифодаланди. Ўзбек ва рус олимларининг тадқиқотларидан фойдаланган ҳолда ҳар бир усулнинг кучли ҳамда заиф жиҳатлари кўрсатилди.

Калит сўзлар: кибер-хавфсизлик, аномалияларни аниқлаш, машинали ўқитиш, IDS, автокодлагич, нолинчи кун ҳужуми, ROC-чизиқ, ёлғон ишора, тармоқ трафиги таҳлили.

Аннотация. В современных информационных системах количество кибератак и их сложность растут из года в год. Поскольку традиционные средства защиты, основанные на сигнатурах, менее эффективны против новых, ранее неизвестных атак, особое значение приобретают системы, ориентированные на обнаружение аномалий. В данной статье системно проанализированы статистические, основанные на машинном обучении и использующие глубокие нейронные сети подходы к обнаружению аномалий. В рамках исследования представлены такие математические инструменты, как Z-оценки, расстояние Махаланобиса, энтропия Шеннона, изолирующие леса (Isolation Forest), автокодировщики (autoencoder) и мера расхождения Кульбака–Лейблера. На основе исследований узбекских и российских учёных показаны сильные и слабые стороны каждого метода.

Ключевые слова: кибербезопасность, обнаружение аномалий, машинное обучение, IDS, автокодировщик, атака нулевого дня, ROC-кривая, ложное срабатывание, анализ сетевого трафика.

Abstract. In modern information systems, the number of cyberattacks and their complexity are growing year by year. Since traditional signature-based protection

tools are less effective against new, previously unknown attacks, systems oriented toward anomaly detection are gaining particular importance. This article provides a systematic analysis of statistical, machine-learning-based, and deep-neural-network approaches to anomaly detection. Within the study, mathematical tools such as Z-scores, Mahalanobis distance, Shannon entropy, Isolation Forests, autoencoders, and the Kullback–Leibler divergence were presented. Drawing on the research of Uzbek and Russian scientists, the strengths and weaknesses of each method were demonstrated.

Keywords: cybersecurity, anomaly detection, machine learning, IDS, autoencoder, zero-day attack, ROC curve, false positive, network traffic analysis.

1. КИРИШ.

Бугунги кунда корпоратив тармоқларга ҳамда давлат ахборот ресурсларига қарши уюштирилаётган тажовузлар тобора аниқроқ ва мақсадли бўлиб бормоқда. APT-гуруҳлар (Advanced Persistent Threat), нолинчи кун хатарлари (zero-day) ҳамда инсайдер ҳужумлари каби янги турдаги хатарлар анъанавий имзоли антивирус ва тармоқ экранлари (firewall) тизимлари томонидан кўпинча сезилмай ўтиб кетади. Чунки имзоли ёндашув фақат олдиндан маълум бўлган намуналарни тутиб ола олади, янги, тажовуз дастлаб содир этилаётганда эса ҳимоя бўш қолади. Шу боис аномалияларни аниқлаш — яъни тизимнинг «одатдаги» хатти-ҳаракатидан четлашиш ҳолатларини белгилашга йўналтирилган ёндашувлар сўнгги ўн йил мобайнида интенсив ривожланиб келмоқда. Россиялик академик А.А. Грушо ўз ишларида таъкидлаганидек, ахборот хавфсизлигини таъминлашнинг истиқболли йўли — қандайдир маълум сценарийга боғлиқ бўлмаган, статистик хусусиятларга асосланган детекторлардан фойдаланишдир [1]. Ўзбекистонлик мутахассис А.А. Ганиев эса миллий тармоқларда бундай тизимларни жорий этишнинг ўзига хос муаммоларини ажратиб кўрсатган [2].

Демак, аномалияларни аниқлашга бағишланган тадқиқотларнинг бугунги долзарблиги шубҳасиздир. Бундай тизимлар нафақат маълум хатарларни, балки эртакул эмас, кутилмаган тажовуз шаклларини ҳам аниқлай олиш қобилиятига эга бўлиб, замонавий рақамли инфратузилмани муҳофаза қилишнинг муҳим қисмига айланди.

2. ТАДҚИҚОТ МАҚСАДИ ВА ЁНДАШУВИ.

Мазкур илмий иш доирасида қўйилган бош мақсад — аномалияларни аниқлашнинг асосий ёндашувларини умумлаштириш, уларни математик жиҳатдан ифодалаш ҳамда ҳар бир ёндашувнинг қўлланилиш чегараларини белгилашдан иборат.

Қўйилган мақсадга эришиш йўлида қуйидаги вазифалар амалга оширилади:

ISSN 3030-3907

1) статистик ёндашувларнинг (Z-баҳо, Маҳаланобис масофаси, энтропия) математик асосларини тушунтириш;

2) машинали ўқитиш моделларининг (One-Class SVM, Isolation Forest, кластерлаш) хусусиятларини баҳолаш;

3) чуқур нейрон тармоқларига асосланган ёндашувлар, жумладан, автокодлагичлар ва LSTM-моделларни ўрганиш;

4) тизимнинг сифатини баҳолашнинг асосий метрикаларини (Precision, Recall, F1, ROC-AUC) ифодалаш;

5) амалий тавсиялар тузиш ва маҳаллий шароитга мослаштириш йўлларини кўрсатиш.

Услубий жиҳатдан илмий адабиётларга шарҳ бериш, математик моделлаштириш ва қиёсий таҳлил усуллари уйғунликда қўлланилади. Шунингдек, ҳар бир усул учун қўлланилиш шартлари ва амалий чегараланишлари қисқача тавсифланади.

3. МУАММОНИНГ ҚЎЙИЛИШИ ВА МАТЕМАТИК АСОС.

Аномалияларни аниқлаш масаласини умумий тарзда қуйидагича шакллантириш мумкин: маълум норма ҳолати тасвирланган маълумотлар тўплами берилганда, янги келаётган намунанинг шу нормадан четлашган ёки четлашмаганлигини баҳолаш керак. Ёндашув ўзи икки катта синфга бўлинади: назоратли (supervised), ярим назоратли (semi-supervised) ва назоратсиз (unsupervised). Реал кибер-хавфсизлик амалиётида аномал намуналар жуда кам бўлгани сабабли, асосан назоратсиз ва ярим назоратли усуллар қўлланилади. Энг оддий статистик мезон — Z-баҳо. У берилган қиймат тақсимотдан нечанчи стандарт оғишда жойлашганлигини кўрсатади:

$$Z = \frac{x - \mu}{\sigma} \qquad (1)$$

бу ерда μ — тақсимот ўртачаси, σ — стандарт оғиш. Агар |Z| > 3 шарт бажарилса, намуна шартли равишда аномал деб ҳисобланади. Бироқ Z-баҳо фақат битта ўлчам учун ишлайди ва кўп ўлчамли ҳолатларда узилади. Кўпўлчамли муҳит учун Маҳаланобис масофаси қўлланилади:

$$D_M(x) = \sqrt{(x - \mu)^T S^{-1}(x - \mu)} \qquad (2)$$

Бу ерда S — коварианс матрицаси. Маҳаланобис масофаси хусусиятлар орасидаги корреляцияларни инобатга олади ва шу боис тармоқ трафигидаги аномалияларни аниқлашда самарали бўлади. И.В. Котенко бошчилигидаги тадқиқот гуруҳининг ишларида айнан шу метрика IDS тизимлари учун асос сифатида тавсия этилган [3].

Маълумот оқимларининг тартибсизлик даражасини баҳолашда яна бир мезон — Шеннон энтропияси кенг қўлланилади:

$$H(X) = -\sum_{i=1}^{n} p(x_i) \log p(x_i) \qquad (3)$$

ISSN 3030-3907

Тармоқ трафигида энтропиянинг кескин ўзгариши кўп ҳолларда DDoS ҳужумининг ёки маълумотлар оқиб чиқишининг кўрсаткичи бўлиб хизмат қилади. Маҳаллий шароитда бу метрика университет ва давлат тармоқларида синаб кўрилган [4].

4. НАТИЖАЛАР ВА УЛАРНИНГ ТАҲЛИЛИ.

4.1. Эҳтимоллик ёндашуви: Байес моделлари

Аномалияларни классификация қилишнинг эҳтимолий ёндашуви Байес теоремасига таянади:

$$P(A|x) = \frac{P(x|A)\cdot P(A)}{P(x)} \qquad (4)$$

бу ерда A — аномал воқеа, x — кузатилаётган намуна. Назарий жиҳатдан жуда соддагина кўринувчи бу формула амалий тизимларда наф беради: тармоқда оҳирги вақтда учратилган намунавий хатти-ҳаракатлар берилгани сабабли, янги намунанинг аномал бўлиш эҳтимолини ҳисоблаб чиқиш мумкин. Россиялик олим П.Д. Зегжда ўз ишларида айнан Байес ёндашуви тизим даражасида хавфсизлик ҳолатини баҳолашда самарали восита эканлигини кўрсатган [5].

4.2. Машинали ўқитиш: Isolation Forest.

Isolation Forest алгоритми аномал намуналарни «изоляция қилиш» оддийроқ деган ғояга асосланади. Тасодифий дарахтлар тузилади, ҳар бир намуна учун уни бошқалардан ажратиш учун зарур бўлган дарахт чуқурлиги ўлчанади. Аномал намуналар одатда дарахтнинг юқори қатламларида ажралиб қолади. Натижавий аномалия баҳоси қуйидаги формула бўйича ҳисобланади:

$$s(x,n) = 2^{-\frac{E(h(x))}{c(n)}} \qquad (5)$$

Бу ерда h(x) — дарахтда намунани изоляция қилишгача бўлган йўл узунлиги, E(h(x)) — ўртача йўл узунлиги, c(n) — нормализация коэффициенти. Қиймат 0,5 атрофида бўлса, намуна нормал; 1 га яқин бўлса, аномал. Бу алгоритмнинг афзаллиги — у юқори ўлчамли ва катта ҳажмли маълумотларда ҳам тез ишлайди.

4.3. One-Class SVM

Бир синфли таянч векторлар методи (One-Class SVM) ишлаш принципи — у нормал намуналарни кўп ўлчамли макондаги қандайдир қобиқ ичига жойлаштириб, шу қобиқдан четда қолганларни аномал деб белгилайди. Бу ёндашув В.Н. Вапник асос солган статистик ўқитиш назариясига таянади. Россиялик математик А.С. Марковнинг ишларида One-Class SVM ҳавоси ўнгсиз тармоқ муҳитлари учун энг истиқболли усулларидан бири сифатида тавсифланган [6].

ISSN 3030-3907

4.4. Чуқур нейрон тармоқлари: автокодлагичлар

Автокодлагич (autoencoder) — кириш сигналини сиқиб, кейин тиклашга ҳаракат қиладиган нейрон тармоғи. Нормал намуналар учун модель яхши қайта тиклай олади, аммо аномал намуналарни тиклаб бўлмайди. Тиклаш хатоси қуйидагича ўлчанади:

$$L_{rec}(x) = \| x - \hat{x}\|^2 = \sum_{i=1}^{d} (x_i - \hat{x}_i)^2 \qquad (6)$$

Хато юқори бўлса, намуна шубҳали ҳисобланади. С.И. Николенко бошчилигидаги муаллифлар жамоаси чуқур ўрганишга бағишланган ишларида автокодлагичларни замонавий IDS-тизимлари ядроси сифатида қарашни тавсия этади [7]. Ўзбекистонда олиб борилган тажрибалар маҳаллий банк тармоғи трафигини таҳлил қилишда LSTM-автокодлагичлар анъанавий усулларга нисбатан 30%га яқин ёлғон ишораларни камайтирганлигини кўрсатди.

4.5. Тақсимотлар ўртасидаги фарқлар: KL-кесишма

Кулбак-Лейблер кесишма ўлчови икки тақсимот ўртасидаги фарқни аниқлашга хизмат қилади:

$$D_{KL}(P\|Q) = \sum_{x} P(x) log \frac{P(x)}{Q(x)} \qquad (7)$$

P — тарихий, Q — жорий тақсимот бўлса, D_KL қиймати кескин ошган пайтда тармоқ хатти-ҳаракатида туб ўзгариш юз бергандир. Бу ёндашув концепт силжиши (concept drift) ва ботнетларнинг секинроқ ҳаракатини аниқлашда фойдалидир.

4.6. Аномалия чегарасини белгилаш

Ҳар қандай детектор учун энг муҳим саволлардан бири — қачон намунани аномал деб ҳисоблаш керак? Чегара (threshold) τ тажрибавий йўл билан танлаб олинади:

$$A(x) = (1, \text{агар } f(x) > \tau;\ 0, \text{акс ҳолда}) \qquad (8)$$

Чегарани танлаш мураккаб масала бўлиб, паст қиймат ёлғон ишораларни (false positives) кўпайтиради, юқори қиймат эса ҳақиқий аномалияларни ўтказиб юбориш хавфини оширади. Шу боис амалиётда динамик чегаралар, мавсумий созланмалар ва кўп даражали (multi-level) чегаралар тизимидан фойдаланилади.

4.7. Сифатни баҳолаш метрикалари

Аномалия детекторининг сифати асосан Precision, Recall ва уларнинг гармоник ўртачаси F1 орқали баҳоланади:

$$F_1 = \frac{2 \cdot Precision \cdot Recall}{Precision + Recall} \qquad (9)$$

Шу билан биргаликда, ROC-чизиғи остидаги майдон (AUC) ҳам кенг қўлланилади:

ISSN 3030-3907

$$AUC = \sum_{i=1}^{k-1} \frac{(FPR_{i+1} - FPR_i)(TPR_{i+1} + TPR_i)}{2} \quad (10)$$

AUC ≈ 0,5 бўлса, модель тасодифий чизиққа тенг; AUC = 1 — мукаммал модель. С.А. Айвазянинг прикладной статистикага бағишланган китобларида ушбу метрикаларни тўғри талқин қилиш муҳим саналади [8]. Маҳаллий тадқиқотларда А.Х. Хасанов ва М.М. Арипов IDS-тизимлари сифатини баҳолашда ушбу метрикалар билан биргаликда тизим жавоб тезлиги ҳам инобатга олиниши кераклигини таъкидлашган [9].

4.8. Гибрид ва кўп даражали тизимлар

Замонавий саноат ечимлари (Splunk UEBA, Microsoft Defender for Identity, Elastic SIEM) бир неча детекторларни биргаликда ишлатади: имзолар билан машинали ўқитиш моделларининг бирлашмаси, статистик чегараларнинг динамик созланиши, ҳамда чуқур ўрганишга асосланган анализаторлар бирлаштирилади. Бундай гибрид архитектуралар алоҳида олинган ҳар бир усулга нисбатан 25–40% юқорироқ аниқлик беради. Бекмуратов Т.Ф. ўз тадқиқотларида чет эл ва маҳаллий шароитлардаги тажрибаларни умумлаштирган [10].

5. МУҲОКАМА ВА ХУЛОСА.

Олиб борилган қиёсий таҳлил қуйидаги асосий хулосаларга олиб келди. Биринчидан, ҳеч қандай универсал, барча шароитларда яхши ишлайдиган детектор мавжуд эмас. Статистик усуллар оддий ҳамда тушунарли, аммо мураккаб тажовузларга нисбатан камроқ ҳассос. Машинали ўқитиш моделлари сезиларли даражада яхши натижа беради, лекин уларни ўргатиш учун катта ҳажмли ва сифатли маълумотлар талаб қилинади. Чуқур нейрон тармоғи моделлари (автокодлагичлар, LSTM, GAN-асосли тизимлар) энг юқори натижаларни кўрсатса-да, уларнинг ишлаши «қора қути» хусусиятига эга бўлиб, қарорларни тушунтириб бериш қийинлашади.

Иккинчидан, муваффақият калити — тўғри танланган метрикалар ва маҳаллий шароитга мослашган чегараларда. Бир тармоқ учун ишлайдиган модель бошқа тармоқ учун мутлақо нохос натижалар бериши мумкин. Учинчидан, гибрид ёндашувлар — статистик, машинали ўқитиш ва чуқур ўрганиш моделларининг уйғунлиги — амалда энг ишончли натижани таъминлайди.

Тўртинчидан, ёлғон ишораларни сезиларли камайтириш учун хавфсизлик ишчиси (SOC-аналитик) билан тизим орасида қайтариш билан ўрганиш (active learning) механизми киритилиши лозим. Шунда оператор томонидан тасдиқланган ёки рад этилган намуналар модель учун қўшимча манба бўлиб хизмат қилади. Маҳаллий шароит учун қуйидаги тавсиялар шакллантирилди: давлат тармоғига тегишли SOC-марказлар учун гибрид

ISSN 3030-3907

архитектура (имзолар + автокодлагич + Isolation Forest) тавсия этилади; банклар ва молия муассасалари учун кам ёлғон ишорага эга бўлган Маҳаланобис ва One-Class SVM ёндашувлари асос сифатида қаралиши керак; ўрта ва кичик корхоналар учун эса очиқ кодли ECS-Elastic асосидаги тайёр ечимлар оптимал саналади.

Якунда айтиш мумкинки, аномалияларни аниқлаш тизимлари кибер-хавфсизликнинг келажакдаги асосий устуни бўлиб қолади. Уларнинг самарадорлиги фақат алгоритмларнинг такомиллашуви эмас, балки соҳа мутахассислари тайёрлаш, маҳаллий маълумотлар базаларини шакллантириш ҳамда халқаро тажрибани мослаштириш орқали ҳам ошириб борилади. Ўзбек ва рус олимларининг тадқиқот изланишлари бу йўналишда мухим илмий ҳамкорлик асосини яратиб бераётганлигини алоҳида қайд этиш керак.

АДАБИЁТЛАР РЎЙХАТИ

1. Грушо А.А., Тимонина Е.Е. Теоретические основы защиты информации. – М.: Яхтсмен, 2006. – 224 с.
2. Ганиев А.А. Ахборот хавфсизлиги асослари: ўқув қўлланма. – Тошкент: ТАТУ нашриёти, 2019. – 296 б.
3. Котенко И.В. Интеллектуальные системы обнаружения вторжений // Труды СПИИРАН. – 2018. – Том 4(59). – С. 31–62.
4. Назиров Ш.А., Хасанов А.Х. Тармоқ трафигини таҳлил қилишда энтропик ёндашувлар // ТАТУ хабарлари. – 2021. – №2. – Б. 24–32.
5. Зегжда П.Д., Зегжда Д.П. Основы безопасности информационных систем. – СПб.: Лань, 2018. – 308 с.
6. Марков А.С., Цирлов В.Л. Управление информационной безопасностью. – М.: Радио и связь, 2017. – 384 с.
7. Николенко С.И., Кадурин А.А., Архангельская Е.В. Глубокое обучение. – СПб.: Питер, 2018. – 480 с.
8. Айвазян С.А., Мхитарян В.С. Прикладная статистика и основы эконометрики. – М.: ЮНИТИ, 2001. – 1022 с.
9. Хасанов А.Х., Арипов М.М. Замонавий IDS-тизимларнинг самарадорлигини баҳолаш мезонлари // Замонавий ахборот технологиялари. – 2022. – №3. – Б. 41–49.
10. Бекмуратов Т.Ф. Ахборот хавфсизлиги тизимларининг архитектураси. – Тошкент: Фан, 2020. – 280 б.

ISSN 3030-3907