MUHANDISLIK & IQTISODIYOT

ijtimoiy-iqtisodiy, innovatsion texnik, fan va ta'limga oid ilmiy-amaliy jurnal

2026-YIL

IYUL/7-SON, II-QISM

Milliy nashrlar

OAK: https://oak.uz/pages/4802

05.00.00 - Texnika fanlari
08.00.00 - Iqtisodiyot fanlar

Google Scholar

ISSN INTERNATIONAL STANDARD SERIAL NUMBER INTERNATIONAL CENTRE

OpenAIRE

ISSN: 3060-463X

РЭУ.РФ
РОССИЙСКИЙ ЭКОНОМИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ Г.В. ПЛЕХАНОВА ФИЛИАЛ В г. ТАШКЕНТЕ

TOSHKENT DAVLAT TRANSPORT UNIVERSITETI

TOSHKENT TO'QIMACHILIK VA DIZAYN UNIVERSITETI

muhandislik & iqtisodiyot

ijtimoiy-iqtisodiy, innovatsion texnik,
fan va ta'limga oid ilmiy-amaliy jurnal

Elektron nashr, 2026-yil, iyul.

muhandislik & iqtisodiyot

ijtimoiy-iqtisodiy, innovatsion texnik,
fan va ta'limga oid ilmiy-amaliy jurnal

05.01.00 – Axborot texnologiyalari, boshqaruv va kompyuter grafikasi
05.01.01 – Muhandislik geometriyasi va kompyuter grafikasi. Audio va video texnologiyalari
05.01.02 – Tizimli tahlil, boshqaruv va axborotni qayta ishlash
05.01.03 – Informatikaning nazariy asoslari
05.01.04 – Hisoblash mashinalari, majmualari va kompyuter tarmoqlarining matematik va dasturiy ta'minoti
05.01.05 – Axborotlarni himoyalash usullari va tizimlari. Axborot xavfsizligi
05.01.06 – Hisoblash texnikasi va boshqaruv tizimlarining elementlari va qurilmalari
05.01.07 – Matematik modellashtirish
05.01.11 – Raqamli texnologiyalar va sun'iy intellekt
05.02.00 – Mashinasozlik va mashinashunoslik
05.02.08 – Yer usti majmualari va uchish apparatlari
05.03.02 – Metrologiya va metrologiya ta'minoti
05.04.01 – Telekommunikasiya va kompyuter tizimlari, telekommunikasiya tarmoqlari va qurilmalari. Axborotlarni taqsimlash
05.05.03 – Yorug'lik texnikasi. Maxsus yoritish texnologiyasi
05.05.05 – Issiqlik texnikasining nazariy asoslari
05.05.06 – Qayta tiklanadigan energiya turlari asosidagi energiya qurilmalari
05.06.01 – To'qimachilik va yengil sanoat ishlab chiqarishlari materialshunosligi
05.08.03 – Temir yo'l transportini ishlatish
05.08.06 – "G'ildirakli va gusenisali mashinalar va ularni ishlatish" (texnika fanlari)
05.09.01 – Qurilish konstruksiyalari, bino va inshootlar
05.09.04 – Suv ta'minoti. Kanalizatsiya. Suv havzalarini muhofazalovchi qurilish tizimlari
10.00.06 – Qiyosiy adabiyotshunoslik, chog'ishtirma tilshunoslik va tarjimashunoslik
10.00.04 – Yevropa, Amerika va Avstraliya xalqlari tili va adabiyoti
08.00.01 – Iqtisodiyot nazariyasi
08.00.02 – Makroiqtisodiyot
08.00.03 – Sanoat iqtisodiyoti
08.00.04 – Qishloq xo'jaligi iqtisodiyoti
08.00.05 – Xizmat ko'rsatish tarmoqlari iqtisodiyoti
08.00.06 – Ekonometrika va statistika
08.00.07 – Moliya, pul muomalasi va kredit
08.00.08 – Buxgalteriya hisobi, iqtisodiy tahlil va audit
08.00.09 – Jahon iqtisodiyoti
08.00.10 – Demografiya. Mehnat iqtisodiyoti
08.00.11 – Marketing
08.00.12 – Mintaqaviy iqtisodiyot
08.00.13 – Menejment
08.00.14 – Iqtisodiyotda axborot tizimlari va texnologiyalari
08.00.15 – Tadbirkorlik va kichik biznes iqtisodiyoti
08.00.16 – Raqamli iqtisodiyot va xalqaro raqamli integratsiya
08.00.17 – Turizm va mehmonxona faoliyati

Ma'lumot uchun, OAK Rayosatining 2024-yil 28-avgustdagi 360/5-son qarori bilan "Dissertatsiyalar asosiy ilmiy natijalarini chop etishga tavsiya etilgan milliy ilmiy nashrlar ro'yxati"ga texnika va iqtisodiyot fanlari bo'yicha "Muhandislik va iqtisodiyot" jurnali ro'yxatga kiritilgan.

Muassis: "Tadbirkor va ishbilarmon" MChJ

Hamkorlarimiz:

1. Toshkent shahridagi G.V.Plexanov nomidagi Rossiya iqtisodiyot universiteti
2. Toshkent davlat iqtisodiyot universiteti
3. Toshkent irrigatsiya va qishloq xo'jaligini mexanizatsiyalash muhandislari instituti" milliy tadqiqot universiteti
4. Islom Karimov nomidagi Toshkent davlat texnika universiteti
5. Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti
6. Toshkent davlat transport universiteti
7. Toshkent arxitektura-qurilish universiteti
8. Toshkent kimyo-texnologiya universiteti
9. Jizzax politexnika instituti

MUNDARIJA • СОДЕРЖАНИЕ • CONTENTS

MUNDARIJA

MUNDARIJA • СОДЕРЖАНИЕ • CONTENTS

HUJUMLARNI ANIQLASH TIZIMLARIDA TAHDID MODELINI ISHLAB CHIQISH

Barotova Zahro Akmaljon qizi
Muhammad al-Xorazmiy nomidagi Toshkent axborot texnologiyalari universiteti “Axborot xavfsizligi” kafedrasi tayanch doktoranti
ORCID: 0009-0008-2983-681X

Annotatsiya. Mazkur maqolada hujumlarni aniqlash tizimlari (IDS) va ularning asosiy turlari qisqacha ko‘rib chiqilgan. IDS tizimlarining tarmoq va tizim xavfsizligini ta’minlashdagi ahamiyati yoritilgan hamda ularning imzoga asoslangan, anomaliyaga asoslangan va gibrid turlari tavsiflangan. Shuningdek, tahdid modellashtirish tushunchasi va uning axborot xavfsizligidagi o‘rni tahlil qilingan. Ish doirasida IDS tizimlari uchun tahdid modeli ishlab chiqilgan bo‘lib, u STRIDE+DREAD metodologiyasi asosida baholangan. Taklif etilgan model yordamida tizimda yuzaga kelishi mumkin bo‘lgan asosiy zaifliklar aniqlangan va xavf darajasi asosida baholangan hamda yumshatish strategiyalari ishlab chiqilgan. Olingan natijalar IDS tizimlarida tahdidlarni oldindan aniqlash va xavfsizlik darajasini oshirish imkonini beradi.

Kalit so‘zlar: IDS, tahdid modeli, STRIDE, DREAD, kiberxavfsizlik, tahdid.

Abstract. This article briefly reviews intrusion detection systems (IDS) and their main types. The importance of IDS systems in ensuring network and system security is highlighted, and their signature-based, anomaly-based, and hybrid types are described. The concept of threat modeling and its role in information security are also analyzed. As part of the work, a threat model for IDS systems was developed and evaluated based on the STRIDE+DREAD methodology. Using the proposed model, the main vulnerabilities that may arise in the system were identified and assessed based on the level of risk, and mitigation strategies were developed. The results obtained allow for early detection of threats in IDS systems and an increase in the level of security.

Keywords: IDS, threat model, STRIDE, DREAD, cybersecurity, threat.

Аннотация. В данной статье кратко рассматриваются системы обнаружения вторжений (СОЗ) и их основные типы. Подчеркивается важность систем СОЗ в обеспечении сетевой и системной безопасности, а также описываются их сигнатурные, аномальные и гибридные типы. Также анализируется концепция моделирования угроз и ее роль в информационной безопасности. В рамках работы была разработана и оценена модель угроз для систем СОЗ на основе методологии STRIDE+DREAD. С помощью предложенной модели были выявлены и оценены основные уязвимости, которые могут возникнуть в системе, на основе уровня риска, а также разработаны стратегии смягчения последствий. Полученные результаты позволяют осуществлять раннее обнаружение угроз в системах СОЗ и повышать уровень безопасности.

Ключевые слова: СОЗ, модель угроз, STRIDE, DREAD, кибербезопасность, угроза.

KIRISH

Hozirgi kunda axborot texnologiyalarining jadal rivojlanishi bilan bir qatorda kiberxavfsizlik masalalari ham dolzarb ahamiyat kasb etmoqda. Tarmoqlar va axborot tizimlarining kengayib borishi, internet xizmatlarining ommalashuvi hamda raqamli infratuzilmaning rivojlanishi natijasida turli xil kiberhujumlar soni ortib bormoqda. Bu esa axborot resurslarini himoya qilishning samarali usullarini ishlab chiqishni talab etadi.

Hujumlarni aniqlash tizimlari axborot xavfsizligini ta’minlashda muhim vositalardan biri hisoblanadi. Ushbu tizimlar tarmoq yoki tizim faoliyatini kuzatish orqali ruxsatsiz kirishlar va zararli faoliyatlarni aniqlash imkonini beradi. Biroq an’anaviy IDS tizimlari asosan mavjud yoki allaqachon yuzaga kelgan hujumlarni aniqlashga yo‘naltirilgan bo‘lib, ular orqali tahdidlarni oldindan baholash va prognozlash imkoniyatlari cheklangan.

Shu sababli zamonaviy yondashuvlarda tahdidni modellashtirish muhim ahamiyat kasb etmoqda. Tahdidni modellashtirish tizimdagi zaifliklarni aniqlash, ehtimoliy hujum ssenariylarini tahlil qilish va xavf darajasini baholash imkonini beradi. Bu esa kiberhujumlarning oldini olishda proaktiv yondashuvni ta’minlaydi.

MAVZUGA OID ADABIYOTLAR SHARHI

Hujumlarni aniqlash tizimlari (IDS) dasturiy ta’minot yoki apparat mahsuloti sifatida ta’riflanadi [1], u tajovuzkorlar tomonidan yuzaga kelishi mumkin bo‘lgan hodisalarga e’tibor qaratadi va aniqlaydi, bu hujumlar

haqidagi ma’lumotlarni nazorat qiladi, ularni tugatishga harakat qiladi hamda real vaqt muhitida xavfsizlik ma’murlari uchun hisobot tayyorlaydi [2]. Shunday qilib, tajovuzni aniqlash tizimini himoyani to‘ldiruvchi xavfsizlik operatsiyasi sifatida ko‘rish mumkin, masalan, xavfsizlik devorlari [3]. Shuningdek, u tajovuzkorlar tomonidan yuzaga keladigan turli xil hujumlardan himoyalanish va ularning oldini olishga yordam beradi.

IDS tizimlarining asosiy uch turi mavjud bo‘lib, quyidagicha ta’riflanadi:

Imzoga asoslangan IDS (S-IDS). Oldindan ma’lum bo‘lgan hujumlar signaturalari asosida ishlaydigan hujumlarni aniqlash tizimlari turi hisoblanadi [4].

Anomaliyaga asoslangan IDS (A-IDS). Ushbu turdagi hujumlarni aniqlash tizimlari tizimning normal xatti-harakatlarini o‘rganishga va undagi chetga chiqishlarni aniqlashga qaratilgan tur hisoblanadi.

Gibrid IDS. Yuqoridagi ikkala yondashuvni birlashtiradi [5].

Ushbu IDS texnologiyalarining turli mezonlar bo‘yicha qiyosiy tahlili 1-jadvalda keltiriladi [6].

1-jadval. IDS turlarining muhim mezonlar bo‘yicha qiyosiy tahlili

Mezon	Anomaliya asosidagi	Imzoga asoslangan
Ishlash prinsipi	Oddiy xatti-harakatlarni modellashtirish va og‘ishlarni aniqlash	Hujum xatti-harakatlarini imzo sifatida ifodalash
Aniqlash yondashuvi	Ma’lumotlar oqimlarini, trafik modellarini va aloqa naqshlarini kuzatish	Namunalarni imzo ma’lumotlar bazasi bilan taqqoslash
Noma’lum hujumlarga qarshi samaradorlik	Yuqori	Past
Noto‘g‘ri ijobiy boshqaruv	Yuqori soxta signal darajasi	Soxta signal darajasi past
Hujum haqida ma’lumot	Aniqlangan anomaliyalarning aniq sabablarini keltira olmaslik	Hujum turlari va mumkin bo‘lgan sabablar haqida batafsil ma’lumot beradi
Asosiy qiyinchiliklar	Oddiy xatti-harakatlar profilini aniq belgilash	Samarali imzolarni loyihalash
Afzalliklari	Yuqori umumlashtirish qobiliyati, noma’lum hujumlarni aniqlaydi	Soxta signal darajasi past, hujumlar haqida batafsil ma’lumot
Kamchiliklari	Yuqori soxta signal darajasi, anomaliyalarning sabablarini aniqlashda qiyinchilik	O‘tkazib yuborilgan signallarning yuqori darajasi, noma’lum hujumlarni aniqlay olmaslik, katta imzo ma’lumotlar bazasini saqlash zarurati

Tahdidni modellashtirish – bu axborot tizimlarida yuzaga kelishi mumkin bo‘lgan xavf va tahdidlarni oldindan aniqlash, tahlil qilish va ularni kamaytirish choralarini ishlab chiqishga qaratilgan jarayondir. Ushbu yondashuv tizim xavfsizligini ta’minlashda muhim bosqichlardan biri hisoblanadi [7].

Tahdidni modellashtirishning asosiy maqsadi – tizimdagi zaifliklarni aniqlash va ulardan foydalanish ehtimoli mavjud bo‘lgan hujum ssenariylarini oldindan baholashdan iborat. Bu esa kiberhujumlarning oldini olish yoki ularning ta’sirini kamaytirishga yordam beradi.

Mazkur jarayon odatda quyidagi bosqichlarni o‘z ichiga oladi:

- tizim arxitekturasini o‘rganish va modellashtirish;
- potensial tahdidlarni aniqlash;
- xavf darajasini baholash;
- himoya choralarini ishlab chiqish [8].

Tahdidni modellashtirish axborot xavfsizligi sohasida proaktiv yondashuv hisoblanadi, ya’ni muammo yuzaga kelgandan keyin emas, balki oldindan aniqlashga qaratilgan. Bu esa an’anaviy hujumlarni aniqlash tizimlariga nisbatan sezilarli ustunlik beradi [9].

Hozirgi kunda axborot tizimlarida tahdidlarni aniqlash va baholash uchun turli xil modellashtirish usullari ishlab chiqilgan. Ushbu usullar tizimdagi zaifliklarni aniqlash, tahdidlarni tasniflash va xavf darajasini baholashda qo‘llaniladi.

Eng keng tarqalgan tahdid modellashtirish usullari 2-jadvalda keltirib o‘tiladi.

2-jadval. Keng tarqalgan tahdid modeli usullari [10]

Usul nomi	Tavsifi	Afzalliklari	Kamchiliklari
STRIDE	Tahdidlarni 6 turga ajratadi	Oddiy va tushunarli, tizimli yondashuv	Faqat tahdidni aniqlaydi, baholamaydi
DREAD	Tahdidlarni risk asosida baholash	Xavfni miqdoriy baholash imkoniyati	Subyektivlik mavjud
PASTA	Riskga yo‘naltirilgan ko‘p bosqichli metodologiya	Biznes va texnik jihatlarni qamrab oladi	Murakkab va ko‘p vaqt talab qiladi
ATT&CK	Hujumchilarning xatti-harakatlari va texnikalariga asoslangan model	Real hujum ssenariylariga yaqin	Implementatsiya qilish qiyin
OCTAVE	Tashkilotga yo‘naltirilgan risk baholash usuli	Strategik qarorlar uchun foydali	Texnik jihatdan chuqur emas

TADQIQOT METODOLOGIYASI

Hujumlarni aniqlash tizimlari arxitekturasi bir nechta o‘zaro bog‘langan komponentalardan iborat bo‘lib, ularning har biri uchun potensial xavflar mavjud. Mavjud IDS tizimlari uchun tahdid modelini qurish undagi mavjud kamchilik va zaifliklarni aniqlash hamda tizimning bardoshliligini mustahkamlash imkonini beradi. Ishning maqsadi tahdidlarni modellashtirish, xavfni baholash va yumshatish strategiyalarini taqdim etishdan iborat bo‘lib, quyidagi bosqichlar ketma-ketligida amalga oshiriladi (1-rasm):

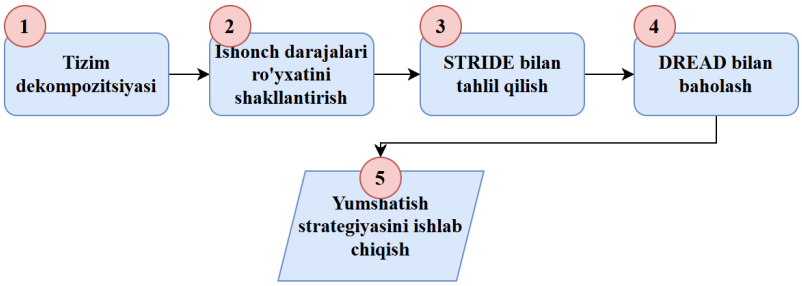
Tizim dekompozitsiyasi: IDS arxitekturasini uning asosiy komponentlariga ajratish, ma’lumotlarning dastur orqali qanday oqishini ko‘rsatadigan kontekst diagrammasini yaratish.

ID (Ishonch darajasi) ro‘yxati: Kontekst diagrammasida ishonch darajasi o‘zgaradigan joylarni belgilash. Bitta ID barcha komponentlarni bir xil xavfsizlik atributlari bilan o‘rab oladi.

Tahdidlarni ro‘yxatga olish: Har bir IDda har bir STRIDE toifasi uchun potensial tahdidlarni tizimli ravishda aniqlash.

Xavfni baholash: Har bir IDda potensial tahdidlarni DREAD toifasi yordamida baholash.

Yumshatish: Yumshatish strategiyalarini taqdim etish(1-rasm).



1-rasm. Ishning bajarilish bosqichlari

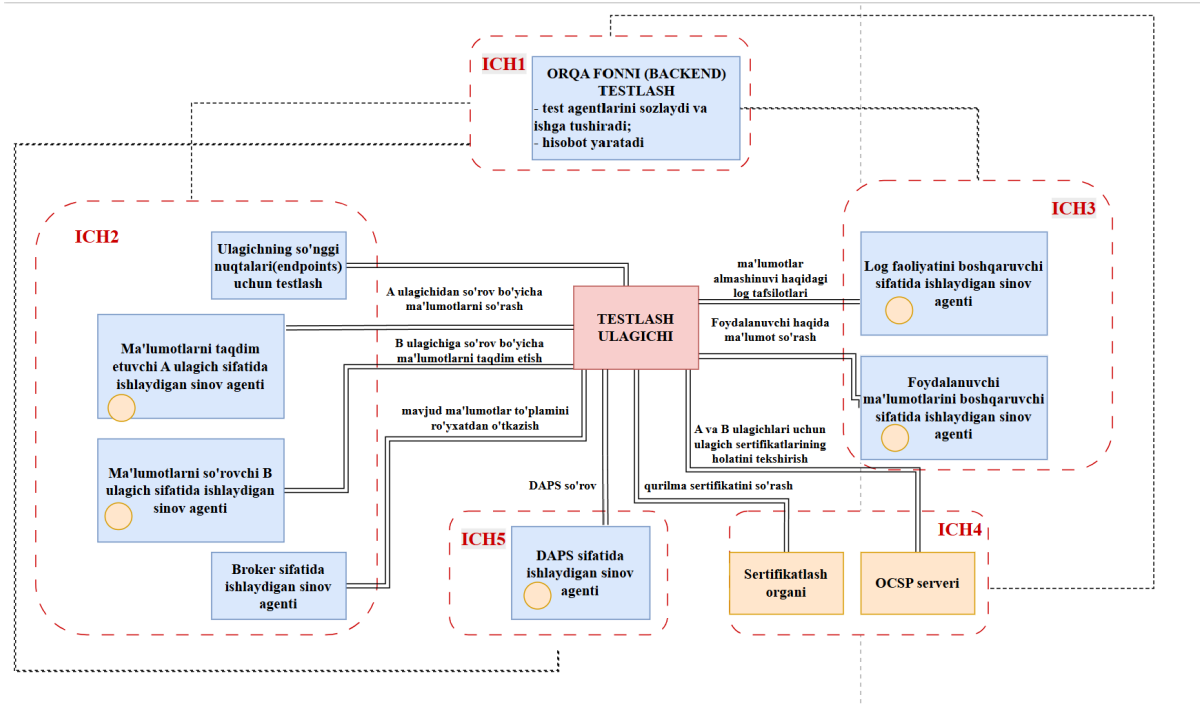
Tizim dekompozitsiyasini yaratishda IDS sinov muhitidan foydalanilgan bo‘lib, bunda markazda testlash ulagichi joylashtirilgan va u IDS muhitidagi xavfsiz ma’lumotlar almashinuvini ta’minlovchi funksiya sifatida baholanadi. Ushbu ulagich Broker, Log faoliyati va ma’lumotlarni boshqarish, dinamik atribut provayderi (DAPS) kabi komponentlar bilan o‘zaro ta’sir ostida bo‘ladi. Ushbu sinov muhitining ishlashi 2-rasmda batafsil keltirilgan.

Quyida IDS turli komponentalarga bo‘lingan va ishonch darajalari yoki chegaralari (ICH) ta’rifi 3-jadvalda keltiriladi.

3-jadval. IDS sinov maydonchasidagi ishonch darajalari (ICH)

ICH	Tavsifi	IDSdagi roli
ICH1: Orqa fonni testlash	Test muhiti va **operatsion** komponentlarni ajratadi. Testdagi xatoliklar yoki zaifliklar **jonli** tizimni buzmasligini ta’minlaydi.	IDS algoritmlari va test modullarini izolyatsiya qiladi, haqiqiy tizim xavfsizligini saqlaydi.

ICH2: Tugash nuqtalari va ulagichlar	Ma’lumot manbalari, iste’molchilar, brokerlar va test agentlarini o‘rab oladi. Interfeyslar xavfsiz bo‘lishini kafolatlaydi.	Sensorlar va log yig‘uvchi modullar orasidagi ma’lumot oqimini himoyalaydi.
ICH3: Log faoliyati va ma’lumotlarni boshqarish	Loglar va ishtirokchi ma’lumotlarini boshqaradigan infratuzilmani o‘z ichiga oladi.	IDS tizimida log yozuvlari va ma’lumotlarni qayta ishlashni izolyatsiya qiladi.
ICH4: Sertifikatlash organi (CA)	Sertifikatlar chiqarish, boshqarish va tasdiqlash jarayonini izolyatsiya qiladi.	IDS tizimida shifrlash va autentifikatsiya ishonchliligini ta’minlaydi.
ICH5: Dinamik atribut provayderi (DAPS)	Dinamik identifikatsiya atributlari va tokenlarni boshqarish jarayonini ajratadi.	IDSda foydalanuvchi va qurilma autentifikatsiyasini mustahkamlaydi, boshqaruv jarayonini asosiy tizimdan izolyatsiya qiladi.



2-rasm. IDS kontekst diagrammasi

TAHLIL VA NATIJALAR

Tahdid modelini baholashda har bir ICH uchun STRIDE+DREAD usulidan foydalanilgan bo‘lib, bunda **STRIDE** IDSda mavjud tahdid va zaifliklarni aniqlashda, DREAD esa xavfni baholashda ishlatiladi. STRIDE usuliga ko‘ra bir nechta zaifliklar aniqlangan bo‘lib, **4–8-jadvallarda** keltiriladi va zaifliklar **vXX** tartibida sanab o‘tiladi.

4-jadval. ICH1 uchun STRIDE tahlili: Orqa fonni testlash

STRIDE kategoriyasi	Kuchli tomonlari	Zaif tomonlari
Soxtalashtirish (Spoofing)	Sinov orqa fonning izolyatsiyasi taqlid qilishni cheklaydi.	-
Buzib ko‘rsatish (Tampering)	TLS orqali shifrlangan aloqa uzatish paytida ma’lumotlar yaxlitligini himoya qiladi.	v_{01}: Ochiq kodli vositalardagi mumkin bo‘lgan orqa tomon buzib kirishga yo‘l qo‘yishi mumkin.
Rad edish (Repudation)	Jurnal mexanizmlari operatsiyalarni kuzatib boradi va rad etmaslikni ta’minlaydi.	-

Ma'lumotni oshkor qilish (Information Disclosure)	TLS va xavfsiz sertifikatlar ma'lumotlar uzatish jarayonida maxfiylikni ta'minlaydi. Maxfiy ma'lumotlarni shifrlash ruxsatsiz kirishning oldini oladi.	v_{02}: Shikastlangan oxirgi foydalanuvchi qurilmalari maxfiy ma'lumotlarni oshkor qilishi mumkin.
Xizmat ko'rsatishdan bosh tortish (Denial of Service)	-	-
Imtiyozlarni oshirish (Elevation of Privelege)	Rolga asoslangan kirishni boshqarish (RBAC) tegishli imtiyozlarni ta'minlaydi.	-

5-jadval. ICH2 uchun STRIDE tahlili: Tugash nuqtalari va ulagichlar

STRIDE kategoriyasi	Kuchli tomonlari	Zaif tomonlari
Soxtalashtirish (Spoofing)	Mijoz sertifikatini tekshirishda soxtalashtirish cheklovlari	v_{03}: SIM-kartani almashtirish ko'p joylarda ko'p faktorli autentifikatsiya (MFA) dan o'tishi va potensial maxfiy ma'lumotlarga kirish imkonini beradi. v_{04}: Oxirgi foydalanish qurilmalari buzilgan xakerlarga MFAni chetlab o'tishga imkon beradi. v_{05}: MitM hujumlari sessiyani o'g'irlashga imkon beradi.
Buzib ko'rsatish (Tampering)	TLS orqali shifrlangan aloqa uzatish paytida ma'lumotlar yaxlitligini himoya qiladi.	v_{06}: Ochiq kodli vositalardagi mumkin bo'lgan orqa fon buzib kirishga yo'l qo'yishi mumkin.
Rad edish (Repudation)	Jurnal mexanizmlari operatsiyalarni kuzatib boradi va rad etmaslikni ta'minlaydi.	-
Ma'lumotni oshkor qilish (Information Disclosure)	TLS va xavfsiz sertifikatlar ma'lumotlar uzatish jarayonida maxfiylikni ta'minlaydi. Maxfiy ma'lumotlarni shifrlash ruxsatsiz kirishning oldini oladi.	v_{07}: Shikastlangan oxirgi foydalanuvchi qurilmalari maxfiy ma'lumotlarni oshkor qilishi mumkin.
Xizmat ko'rsatishdan bosh tortish (Denial of Service)	-	v_{08}: DDoS hujumlari tizimning kirish nuqtalarini nishonga olishi mumkin.
Imtiyozlarni oshirish (Elevation of Privelege)	RBAC tegishli imtiyozlarni ta'minlaydi.	-

6-jadval. ICH3 uchun STRIDE tahlili: Log faoliyati va ma'lumotlarni boshqarish

STRIDE kategoriyasi	Kuchli tomonlari	Zaif tomonlari
Soxtalashtirish (Spoofing)	Tizim bilan o'zaro aloqada bo'lgan barcha obyektlar uchun X.509 sertifikat autentifikatsiyasi.	-
Buzib ko'rsatish (Tampering)	TLS orqali shifrlangan aloqa uzatish paytida ma'lumotlar yaxlitligini himoya qiladi. Shifrlangan saqlash ma'lumotlar yaxlitligini ta'minlaydi.	v_{09}: Ochiq kodli dasturiy ta'minotdagi backdoor buzib kirishga imkon berishi mumkin. v_{10}: Kalitlarni noto'g'ri boshqarish.
Rad edish (Repudation)	Jurnal mexanizmlari operatsiyalarni kuzatib boradi va rad etmaslikni ta'minlaydi.	-
Ma'lumotni oshkor qilish (Information Disclosure)	TLS va xavfsiz sertifikatlar ma'lumotlar uzatish jarayonida maxfiylikni ta'minlaydi. Maxfiy ma'lumotlarni shifrlash ruxsatsiz kirishning oldini oladi.	v_{11}: Kalitlarni noto'g'ri boshqarish shifrlangan ma'lumotlarning oshkor bo'lishiga olib kelishi mumkin.

Xizmat ko‘rsatishdan bosh tortish (Denial of Service)	Obyektlarni ajratish DDoS hujumlarining zararini cheklaydi.	v_{12}: DDoS hujumlari xizmatni o‘chirib qo‘yishi va tizimda rad etishga imkon berishi mumkin.
Imtiyozlarni oshirish (Elevation of Privelege)	RBAC tegishli imtiyozlarni ta’minlaydi.	-

7-jadval. ICH4 uchun STRIDE tahlili: Sertifikatlash organi

STRIDE kategoriyasi	Kuchli tomonlari	Zaif tomonlari
Soxtalashtirish (Spoofing)	Ochiq kalit infratuzilmasi soxtalashtirishni cheklaydi.	-
Buzib ko‘rsatish (Tampering)	CA faqat shifrlangan sertifikatlar bilan ishlaydi, bu esa ma’lumotlarni oshkor qilishni cheklaydi.	-
Rad edish (Repudation)	Sertifikat berish jarayonlarini batafsil qayd etish	-
Ma’lumotni oshkor qilish (Information Disclosure)	Sertifikatlarni saqlash va uzatishni shifrlash.	v_{13}: Kalitlarni noto‘g‘ri boshqarish shifrlangan ma’lumotlarning oshkor bo‘lishiga olib kelishi mumkin.
Xizmat ko‘rsatishdan bosh tortish (Denial of Service)	-	v_{14}: CA ga qaratilgan DoS hujumlari sertifikat xizmatlarini blokirovka qilishi mumkin.
Imtiyozlarni oshirish (Elevation of Privelege)	Imtiyozli kirish faqat bir nechta vakolatli xodimlar bilan cheklangan.	v_{15}: Xavf ostida qolgan oxirgi foydalanuvchi qurilmalari v_{16}: MitM hujumlari xakerlarga imtiyozli kirish huquqini olish imkonini berishi mumkin. v_{17}: SIM-kartani almashtirish xakerlarga imtiyozli kirish huquqini olish imkonini berishi mumkin.

8-jadval. ICH5 uchun STRIDE tahlili: Dinamik atributlar provayderi (DAPS)

STRIDE kategoriyasi	Kuchli tomonlari	Zaif tomonlari
Soxtalashtirish (Spoofing)	X.509 sertifikatlari bilan o‘zaro autentifikatsiya.	-
Buzib ko‘rsatish (Tampering)	Token imzosi ma’lumotlarni buzib kirishdan himoya qiladi.	-
Rad edish (Repudation)	DAPS barcha token bilan bog‘liq faoliyatlarni qayd qiladi.	-
Ma’lumotni oshkor qilish (Information Disclosure)	Sertifikatlarni saqlash va uzatishni shifrlash.	v_{18}: Kalitlarni noto‘g‘ri boshqarish shifrlangan ma’lumotlarning oshkor bo‘lishiga olib kelishi mumkin.
Xizmat ko‘rsatishdan bosh tortish (Denial of Service)	-	v_{19}: DAPS DDoS hujumlarida tokenlarni taqdim etishni o‘chirib qo‘yish uchun mo‘ljallangan bo‘lishi mumkin.
Imtiyozlarni oshirish (Elevation of Privelege)	Imtiyozli kirish faqat bir nechta vakolatli xodimlar bilan cheklangan.	v_{20}: Oxirgi foydalanish qurilmalari buzilgan v_{21}: MitM hujumlari v_{22}: SIM-kartani almashtirish xakerlarga imtiyozli kirish huquqini olish imkonini berishi mumkin..

Yuqorida STRIDE yordamida aniqlangan tahdidlar DREAD usuliga ko‘ra 5 ta toifa bo‘yicha baholanadi va quyidagi formula yordamida hisoblanadi:

$$DREAD = (D + R + E + A + Di) / 5 \quad (1)$$

Bu yerda:

D (Damage Potential) – zarar darajasi;

R (Reproducibility) – hujumni takrorlash imkoniyati;
E (Exploitability) – ekspluatatsiya qilish osonligi;
A (Affected Users) – ta'sir qiluvchi foydalanuvchilar soni;
Di (Discoverability) – zaiflikni aniqlash osonligi.

Baholash 0–3 oralig'ida amalga oshirilib, 0–1,0 qiymat past, 1,1–2,0 oralig'i o'rta darajani, 2,1–3,0 oralig'idagi qiymatlar esa yuqori risk darajasini belgilaydi. Ishlab chiqilgan tahdid modelida riskni baholash bo'yicha natijalar har bir ICH darajasi uchun alohida hisoblangan bo'lib, 9–13-jadvallarda keltiriladi.

9-jadval. ICH1 uchun DREAD usulida xavfni baholash: Orqa fonni testlash

Tahdid toifasi	D	R	E	A	Di	Xavf bali	Xavf
v_{01}: Ochiq kodli vositalardagi orqa eshiklar(backdoor)	2	2	2	2	1.8	1.8	o'rta
v_{02}: Buzilgan foydalanuvchi qurilmasi orqali ma'lumot sizib chiqishi	2	2	2	2	2	2	o'rta

10-jadval. ICH2 uchun DREAD usulida xavfni baholash: Tugash nuqtalari va ulagichlar

Tahdid toifasi	D	R	E	A	Di	Xavf bali	Xavf
v_{03}: SIM swapping	2	2	2	2	2	2	o'rta
v_{04}: MFA bypass orqali ruxsatsiz kirish	3	2	2	3	2	2.4	yuqori
v_{05}: MiTM sessiyani o'g'irlash	2	2	2	2	2	2	o'rta
v_{06}: Ochiq kodli komponentdagi orqa eshiklar	2	2	2	2	1	1.8	o'rta
v_{07}: Endpoint orqali ma'lumot sizishi	2	2	2	2	2	2	o'rta
v_{08}: DDoS hujumi	3	3	3	3	2	2.8	yuqori

11-jadval. ICH3 uchun DREAD usulida xavfni baholash: Log faoliyati va ma'lumotlarni boshqarish

Tahdid toifasi	D	R	E	A	Di	Xavf bali	Xavf
v_{09}: Orqa eshiklar orqali tizimga kirish	2	2	2	2	1	1.8	o'rta
v_{10}: Kalitlarni noto'g'ri boshqarish	2	2	2	3	1	2	o'rta
v_{11}: Shifrlangan ma'lumotlarning oshkor bo'lishi	3	2	2	3	1	2.2	yuqori
v_{12}: DDoS hujumi	3	3	3	3	2	2.8	yuqori

12-jadval. ICH4 uchun DREAD usulida xavfni baholash: Sertifikatlash organi

Tahdid toifasi	D	R	E	A	Di	Xavf bali	Xavf
v_{13}: Kalitlarni noto'g'ri boshqarish	3	2	2	3	1	2.2	yuqori
v_{14}: DoS hujumi	3	3	3	3	2	2.8	yuqori
v_{15}: Buzilgan foydalanuvchi qurilmasi	2	2	2	2	2	2	o'rta
v_{16}: MitM orqali imtiyoz oshirish	3	2	2	3	2	2.4	yuqori
v_{17}: SIM swapping orqali imtiyoz oshirish	2	2	2	3	2	2.2	yuqori

13-jadval. ICH5 uchun DREAD usulida xavfni baholash: Dinamik atributlar provayderi (DAPS)

Tahdid toifasi	D	R	E	A	Di	Xavf bali	Xavf
v_{18}: Kalitlarni noto‘g‘ri boshqarish	3	2	2	3	1	2.2	yuqori
v_{19}: DAPSga qarshi DDoS	3	3	3	3	2	2.8	yuqori
v_{20}: Buzilgan Endpoint	2	2	2	2	2	2	o‘rta
v_{21}: MitM hujumi	2	2	2	3	2	2.2	yuqori
v_{22}: SIM swapping	2	2	2	3	2	2.2	yuqori

Yuqorida DREAD metodologiyasi asosida o‘tkazilgan xavfni baholash natijalari shuni ko‘rsatadiki, har bir **ID (ishonch darajasi)** uchun STRIDE yordamida aniqlangan tahdidlar DREAD usuli yordamida baholandi va ular orasida eng yuqori xavf ko‘rsatkichi sifatida **2,8** natija qayd etildi. Ushbu xavf **DoS/DDoS** hujumlariga to‘g‘ri keladi va IDS tizimining uzluksiz ishlashiga bevosita ta’sir qiladi. Shuningdek, **MFA bypass**, **MitM** hujumlari, kalitlarni noto‘g‘ri boshqarish hamda imtiyozlarni oshirish bilan bog‘liq tahdidlar ham yuqori xavf darajasiga kiradi.

Ushbu natijalarga ko‘ra, IDS tizimlarida xizmat uzluksizligi va barqarorligini ta’minlash hamda ma’lumotlar yaxlitligini himoya qilish bo‘yicha chora-tadbirlar strategiyasini ishlab chiqish maqsadga muvofiq bo‘ladi. Yuqoridagi tahdid modeli aniqlagan tahdidlar uchun bir qator yumshatish strategiyalari taklif qilingan bo‘lib, ular **14-jadvalda** to‘liq keltiriladi.

14-jadval. Tahdidlar va ularni yumshatish strategiyalari

Zaifliklar	Yumshatish strategiyasi
v_{01}, v_{06}, v_{09}: Ochiq kodli vositalardagi orqa eshiklar (ID1, ID2, ID3)	Kodlarni puxta tekshirish, kodlash amaliyotini xavfsiz bajarish va ochiq kodli komponentlar uchun avtomatlashtirilgan zaifliklarni skanerlash vositalarini birlashtirish. Qattiq bog‘liqlikni boshqarishni o‘rnatish va uchinchi tomon dasturiy ta’minot komponentlarining yaxlitligini tekshirish.
v_{02}, v_{04}, v_{07}, v_{20}: Xavf ostida qolgan oxirgi foydalanuvchi qurilmalari maxfiy ma’lumotlarni oshkor qiladi yoki autentifikatsiyani chetlab o’tadi (ID1, ID2, ID5)	Endpoint Detection va Response (EDR) tizimlarini joriy eting, ilovaga asoslangan MFA yoki apparat tokenlarini joriy eting va saqlangan va uzatilgan ma’lumotlar uchun kuchli shifrlashni qo‘llang. Sessiya cookie-fayllarining amal qilish muddatini belgilang. Ish uchun alohida qurilmalardan foydalanishni majburiy qiling. Zaifliklarga duchor bo‘lishni minimallashtirish uchun foydalanuvchi qurilmalarini muntazam ravishda yangilash kerak.
v_{01}, v_{17}, v_{22}: SIM-swamming ruxsatsiz kirishga ruxsat beradi (ID2, ID4, ID5)	Mobil hisoblarni noodatiy faoliyatlar uchun kuzatib borish va raqamni o‘tkazishdan oldin qat’iy shaxsni tasdiqlashni amalga oshirish. SIM-karta almashtiruvchilari odatda raqamni o‘tkazish uchun telefon qo‘ng‘iroqlari orqali ijtimoiy muhandislikka tayanadilar. Shuning uchun, jarayon xakerlar osongina qo’lga kirita olmaydigan ma’lumotlarni bilishni talab qilishi kerak.Faqat SMS asosidagi MFA va parolni qayta tiklashdan saqlanish kerak.
v_{05}, v_{16}, v_{21}: MitM hujumlari sessiyani o‘g‘irlash yoki imtiyozlarni oshirishga imkon beradi (ID2, ID4, ID5)	O‘zaro TLS autentifikatsiyasidan, sertifikatlarni pinlashdan foydalanish va shifrlash kalitlari va sertifikatlarini muntazam ravishda almashtirish kerak. MitM hujumlarini ko‘rsatadigan shubhali faoliyatni aniqlash uchun buzg‘unchilikni aniqlash tizimlarini joriy qilish talab qilinadi. Sessiya cookie-fayllarining amal qilish muddatini belgilash kerak (masalan, har bir ish smenasi boshida bitta kirishni talab qilish uchun 8 soat).
v_{08}, v_{12}, v_{14}, v_{19}: Tizimga kirish nuqtalari va xizmatlariga qaratilgan DDoS hujumlari (ID2, ID3, ID4, ID5)	Tezlikni cheklash, trafikni filtrlash va yukni muvozanatlash kabi DDoS himoya mexanizmlarini joriy qilish. Hujumlar paytida xizmatlarning mavjudligini saqlab qolish uchun ortiqcha tizimlar va ishdan chiqish strategiyalaridan foydalanish. Faqat ishonchli foydalanuvchilarga kirishga ruxsat berish uchun IP oq ro‘yxatlaridan foydalanish kerak.
v_{10}, v_{11}, v_{13}, v_{18}: Kalit noto‘g‘ri boshqaruv maxfiy va shifrlangan ma’lumotlarning oshkor bo‘lishiga olib keladi (ID3, ID4, ID5)	Xavfsiz saqlash, muntazam kalitlarni almashtirish va qat’iy kirish nazorati kabi mustahkam kalitlarni boshqarish amaliyotlarini joriy etish kerak. Muddati o‘tgan yoki buzilgan kalitlardan foydalanish xavfini kamaytirish uchun sertifikat berish va bekor qilish jarayonlarini avtomatlashtirish talab qilinadi.

XULOSA VA TAKLIFLAR

Mazkur ishda hujumlarni aniqlash tizimlari va ularning asosiy turlari tahlil qilindi hamda tahdidlarni modellashtirish yondashuvi asoslab berildi. STRIDE metodologiyasi yordamida ishlab chiqilgan tahdid modeli orqali tizimdagi mavjud zaifliklar aniqlanib, ularning xavfsizlikka ta'siri baholandi hamda aniqlangan tahdidlarning xavfi DREAD metodi yordamida baholandi.

Natijalar shuni ko'rsatadiki, tahdidlarni modellashtirishni IDS tizimlariga integratsiya qilish hujumlarni aniqlash samaradorligini oshirish va ehtimoliy xavflarni oldindan kamaytirishga xizmat qiladi. Kelgusida ushbu yondashuvni amaliy tizimlarda qo'llash va uni sun'iy intellekt asosidagi usullar bilan boyitish maqsadga muvofiq hisoblanadi.

FOYDALANILGAN ADABIYOTLAR RO'YXATI

1. Lekidis, A.; Mavroeidis, V.; Fysarakis, K. *Towards Incident Response Orchestration and Automation for the Advanced Metering Infrastructure.* In Proceedings of the 2024 IEEE 20th International Conference on Factory Communication Systems (WFCS), Toulouse, France, 17–19 April 2024; pp. 1–8. [CrossRef]
2. Babu, P.R.; Kumar, S.A.P.; Reddy, A.G.; Das, A.K. *Quantum Secure Authentication and Key Agreement Protocols for IoT-Enabled Applications: A Comprehensive Survey and Open Challenges.* Comput. Sci. Rev. 2024, 54, 100676. [CrossRef]
3. Wijesundara, W.M.A.B.; Lee, J.-S.; Tith, D.; Aloupogianni, E.; Suzuki, H.; Obi, T. *Security-Enhanced Firmware Management Scheme for Smart Home IoT Devices Using Distributed Ledger Technologies.* Int. J. Inf. Secur. 2024, 23, 1927–1937. [CrossRef]
4. Zhang, H.; Li, Z.; Xue, Y.; Chang, X.; Su, J.; Wang, P.; Guo, Q.; Sun, H. *A Stochastic Bi-Level Optimal Allocation Approach of Intelligent Buildings Considering Energy Storage Sharing Services.* IEEE Trans. Consum. Electron. 2024, 70, 5142–5153. [CrossRef]
5. Zhai, X.; Li, Z.; Li, Z.; Xue, Y.; Chang, X.; Su, J.; Jin, X.; Wang, P.; Sun, H. *Risk-Averse Energy Management for Integrated Electricity and Heat Systems Considering Building Heating Vertical Imbalance: An Asynchronous Decentralized Approach.* Appl. Energy 2025, 383, 125271. [CrossRef]
6. Hassan, Q.; Viktor, P.; Al-Musawi, T.J.; Mahmood Ali, B.; Algburi, S.; Alzoubi, H.M.; Khudhair Al-Jiboory, A.; Zuhair Sameen, A.; Salman, H.M.; Jaszczur, M. *The Renewable Energy Role in the Global Energy Transformations.* Renew. Energy Focus 2024, 48, 100545. [CrossRef]
7. Blog, M.S. *STRIDE Chart.* Available online: https://www.microsoft.com/en-us/security/blog/2007/09/11/stride-chart/ (accessed on 2 October 2024).
8. Cloudflare. *DDoS Threat Report for Q3 2024.* Available online: https://blog.cloudflare.com/ddos-threat-report-for-2024-q3/ (accessed on 2 October 2024).
9. **MITRE ATT&CK Framework Version 9.** Available online: https://attack.mitre.org/versions/v9/ (accessed on 2 October 2024).
10. Eichler, R.; Gröger, C.; Hoos, E.; Stach, C.; Schwarz, H.; Mitschang, B. *Introducing the Enterprise Data Marketplace: A Platform for Democratizing Company Data.* J. Big Data 2023, 10, 173. [CrossRef]

muhandislik & iqtisodiyot

ijtimoiy-iqtisodiy, innovatsion texnik,
fan va ta'limga oid ilmiy-amaliy jurnal

Ingliz tili muharriri: Feruz Hakimov

Musahhih: Zokir Alibekov

Sahifalovchi va dizayner: Abdurahmon Qurbonov

2026. № 7

"Muhandislik va iqtisodiyot" jurnali 26.06.2023-yildan
O'zbekiston Respublikasi Prezidenti Adminstratsiyasi huzuridagi
Axborot va ommaviy kommunikatsiyalar agentligi tomonidan
№S–5669245 reyestr raqami tartibi bo'yicha ro'yxatdan o'tkazilgan.
Litsenziya raqami: №095310.

Manzilimiz: Toshkent shahri Yunusobod tumani 15-mavze 19-uy

+998 93 718 40 07 https://muhandislik-iqtisodiyot.uz/index.php/journal t.me/yait_2100