"KIBERHUJUMLARNI AMALGA OSHIRISHDA SUN’IY INTELLEKT TEXNOLOGIYALARINING ROLI VA AVTONOM MUDOFAA (AUTONOMOUS DEFENSE) TIZIMLARINING ILMIY-AMALIY ASOSLARI"

«РОЛЬ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА В РЕАЛИЗАЦИИ КИБЕРАТАК И НАУЧНО-ПРАКТИЧЕСКИЕ ОСНОВЫ СИСТЕМ АВТОНОМНОЙ ЗАЩИТЫ ИНФОРМАЦИИ»

"THE ROLE OF AI IN CYBERATTACKS AND SCIENTIFIC-PRACTICAL FOUNDATIONS OF AUTONOMOUS DEFENSE SYSTEMS"

Jalolov Alisherjon Abduhomid o‘g‘li
O‘zbekiston Respublikasi Jamoat xavfsizligi universiteti,
kafedra katta o‘qituvchisi, mustaqil izlanuvchi
A.A. JALOLOV
O‘zbekiston Respublikasi Jamoat xavfsizligi universiteti

Annotatsiya. *Ushbu maqolada kiberxavfsizlik sohasidagi eng so‘nggi tendensiyalar, xususan, kiberhujumlarni amalga oshirishda sun’iy intellekt (AI) va katta til modellari (LLM) keltirib chiqarayotgan "tezlik paradoksi" hamda zamonaviy dasturiy ta’minot zanjiri (Supply Chain) hujumlari tahlil qilingan. Tadqiqotda 2024–2026-yillar oralig‘ida yangi zaifliklar (CVE) uchun eksploit yaratilish vaqti keskin qisqarganligi hamda an’anaviy qo‘lda boshqariladigan himoya tizimlarining (manual workflow) tanazzuli ko‘rsatib o‘tilgan. Shuningdek, Grafana (TanStack) va GitHub (VS Code) tizimlarida yuz bergan supply chain infeksiyalari misolida zamonaviy kiber-tahdidlar tabiati o‘rganilgan. Maqola yakunida strategik obyektlar va rivojlanayotgan davlatlar infratuzilmasini himoya qilish uchun avtonom mudofaa (Autonomous Purple Teaming) va AI asosidagi faol himoya tizimlarini joriy etishning ilmiy-amaliy asoslari ishlab chiqilgan.*

Kalit so‘zlar: Kiberxavfsizlik, sun’iy intellekt (AI), ta’minot zanjiri hujumi (Supply Chain Attack), avtonom mudofaa, eksploit tezligi, xavfsizlik monitoringi, qo‘lda boshqariladigan tizimlar, xavfsizlik tahlili.

Аннотация. *В данной статье анализируются последние тенденции в области кибербезопасности, в частности «парадокс скорости», вызванный применением искусственного интеллекта (ИИ) и больших языковых моделей (LLM) при осуществлении кибератак, а также современные атаки на цепочки поставок программного обеспечения (Supply Chain Attacks). В исследовании подчеркивается резкое сокращение времени разработки эксплоитов для новых уязвимостей (CVE) в период с 2024 по 2026 годы и рассматривается неэффективность традиционных систем защиты, основанных на ручном управлении (manual workflow). Кроме того, характер современных киберугроз изучен на примере инцидентов безопасности в*

цепочках поставок TanStack-Grafana и компрометации расширения VS Code для GitHub. В заключении статьи разработаны научно-практические основы внедрения систем автономной обороны (Autonomous Purple Teaming) и активной защиты на базе ИИ для обеспечения безопасности инфраструктуры развивающихся стран и стратегических объектов.

Ключевые слова: *Кибербезопасность, искусственный интеллект (ИИ), атака на цепочку поставок (Supply Chain Attack), автономная оборона, скорость эксплоита, мониторинг безопасности, ручное управление, анализ безопасности.*

Annotation. *This paper analyzes the latest trends in cybersecurity, specifically the "speed paradox" driven by Artificial Intelligence (AI) and Large Language Models (LMs) in executing cyberattacks, as well as modern software supply chain attacks. The study highlights the drastic reduction in time-to-exploit for new vulnerabilities (CVEs) between 2024 and 2026 and discusses the failure of traditional manual security workflows. Furthermore, the nature of contemporary cyber threats is examined through recent supply chain security incidents, including the TanStack-Grafana breach and the GitHub VS Code extension compromise. Finally, the paper establishes the scientific and practical foundations for implementing autonomous defense systems (Autonomous Purple Teaming) and AI-assisted active defense to safeguard the infrastructure of developing nations and strategic assets.*

Key words: *Cybersecurity, Artificial Intelligence (AI), Supply Chain Attack, Autonomous Defense, time-to-exploit, security monitoring, manual workflows, security analytics.*

Har bir rivojlanayotgan mamlakat va zamonaviy jamiyat uchun davlat xavfsizligi, chegaralar daxlsizligi, fuqarolarning tinch-totuv hayot kechirishi hamda strategik muhim obyektlarning barqaror faoliyat yuritishi eng ustuvor vazifalardan biri hisoblanadi. Bugungi raqamli transformatsiya davrida milliy xavfsizlik tushunchasi faqatgina jismoniy chegaralarni himoya qilish bilan cheklanib qolmay, kiberhudud monitoringi va axborot xavfsizligini ta’minlash tizimlari bilan to‘liq jihozlanganlik darajasini ham o‘z ichiga oladi.

So‘nggi yillarda axborot texnologiyalarining rivojlanishi kiberhududdagi tahdidlar xarakterini tubdan o‘zgartirdi. Ayniqsa, Sun’iy Intellekt (AI) va Katta Til Modellari (LLM) ning hujumchilar tomonidan faol qo‘llanilishi an’anaviy himoya tizimlarining samaradorligini shubha ostiga qo‘ymoqda. Kiberhujumlarning tezlashishi va **Ta’minot Zanjiri Hujumlari (Supply Chain Attacks)** deb ataluvchi uchinchi tomon dasturiy vositalari orqali tizimlarga sizib kirish holatlari bugungi kunda global xavfsizlikning eng zaif nuqtalariga aylanib ulgurdi.

Ushbu maqolaning maqsadi — 2024–2026-yillarda kiberhududda sodir bo‘layotgan keskin o‘zgarishlar, AI texnologiyalarining hujum jarayonlariga ta’siri va ta’minot zanjiri xavfsizligi bilan bog‘liq global hodisalarni ilmiy-amaliy jihatdan tahlil qilish hamda zamonaviy himoya konseptlarini asoslab berishdan iborat.

2024-yilda yangi CVE e'lon qilingandan keyin unga mos exploit yozilishigacha o'rtacha 56 kun vaqt ketgan. Bu vaqt oralig'ida ko'plab tashkilotlar tizimlarni patch qilishga va himoyani moslashtirishga ulgurardi.2025-yilda bu 23 kunga tushgan. 2026-yilda esa atigi 10 soat.Bunga asosiy sabab esa AI va avtomatlashtirish texnologiyalarining hujum jarayonlarini keskin tezlashtirayotganidir. Oldin exploit yozish, reconnaissance qilish yoki payload tayyorlash uchun ko'proq vaqt va tajribali mutaxassis kerak bo'lardi. Hozir esa LLM va automation vositalari bu jarayonlarni bir necha baravar tezlashtirmoqda.Maqoladagi yana bir qiziq statistika: AI-assisted attackerlar ayrim holatlarda tizimga 73 sekund ichida kirishga muvaffaq bo'lyapti.Sababi AI: — exploit yozishda — reconnaissance'da — phishing tayyorlashda — avtomatik scanning'da — privilege escalation'da hujumchilarni keskin tezlashtiryapti.Xo'sh, himoya tomoni bu tezlikka mos javob bera olyaptimi?

Ko'plab tashkilot va kompaniyalarning axborot xavfsizligi xizmatlari hali ham juda sekin manual workflow bilan ishlaydi. Ya'ni hujumchilar allaqachon AI va automation'dan foydalanayotgan bir paytda, ko'plab himoya jarayonlari hali ham qo'lda boshqariladi.Ko'plab joylarda oddiy patch jarayoni shunday ko'rinadi:zaiflik aniqlanadi → ticket ochiladi → approval kutiladi → adminlarga uzatiladi → test qilinadi → maintenance window belgilanadi → production'ga deploy qilinadiBa'zi hollarda esa himoya tomoni zaiflik mavjudligidan umuman xabardor ham bo'lmaydi — chunki alert yo'qoladi, ticket o'qilmaydi, yoki jamoalar o'rtasida ma'lumot yetib bormaydi. Bu jarayon kunlar, haftalar olishi mumkin. Hujumchi esa 73 soniyada tizimda.Maqolaning asosiy g'oyasini shunday ifodalash mumkin: "Cybersecurity'dagi asosiy muammo endi exploit emas. Muammo — tezlik."Shu sabab industry'da "Autonomous Purple Teaming" va AI-assisted defense tushunchalari tez rivojlanmoqda.[18]

Shu kunlarda Grafana bilan bog'liq bir nechta muhim hodisalar sodir bo'ldi, shu haqida qisqacha ma'lumot bermoqchiman.Avval eng shovqinlisi — **TanStack npm supply chain hujumi**[19] orqali Grafana'ning GitHub workflow tokeni o'g'irlangan va bir nechta xususiy repozitoriya yuklab olingan. O'g'ri xabar berish o'rniga, kodlarni ommaga chiqarmaslik evaziga to'lov talab qilgan. Keyinchalik ma'lum bo'ldiki, hujum ortida **CoinbaseCartel** deb nomlangan xakerlar guruhi turgan. Hozircha o'g'irlangan ma'lumotlar ommaga chiqarilmagan. Grafana jamoasi xakerlarning tahdidiga qaramasdan ularga pul to'lamaslikka qaror qilgan va buni rasmiy sahifalarida e'lon qildi. Shu voqealar fonida yana bir yangilik — Grafana Final Scanner yangi versiyasi chiqarildi.Scanner Grafana infratuzilmasini skanerlash va zaifliklarni aniqlash uchun mo'ljallangan

TanStack npm supply chain hujum haqida ham qisqacha: TanStack — React, Vue kabi frameworklar uchun mashhur JavaScript kutubxonalari to'plami. Ko'plab dasturchilar uni loyihalarida ishlatadi.

[18] Elektron manba: https://thehackernews.com/2026/05/your-purple-team-isnt-purple-its-just.html

[19] Elektron manba: https://github.com/Zierax/Grafana-Final-Scanner

Bu jarayon kunlar yoki haftalar talab qilishi mumkin. Agar jamoalar o‘rtasida aloqa yaxshi bo‘lmasa, muhim bildirishnomalar (alertlar) umuman o‘qilmay qolib ketishi ham odatiy holga aylangan. Natijada xaker 73 soniyada ichkariga kirgan tizimda xavfsizlik xizmati haftalab zaiflikni yopish bilan band bo‘ladi. Shu sababli sohada an’anaviy himoyadan voz kechib, **"Autonomous Purple Teaming"** (avtonom tarzda ham hujum, ham himoya simulyatsiyalarini o‘tkazuvchi AI tizimlar) va **AI-assisted defense** (AI asosidagi faol mudofaa) konsepsiyalariga o‘tish zarurati paydo bo‘ldi.

Bugungi kunda xakerlar to‘g‘ridan-to‘g‘ri yaxshi himoyalangan server yoki bulutli infratuzilmaga hujum qilish o‘rniga, o‘sha kompaniya foydalanadigan uchinchi tomon (third-party) kutubxonalari, plaginlari yoki ochiq kodli paketlarini zararlashni afzal ko‘rishmoqda. Bu usul dasturiy ta’minot zanjiri hujumi (Supply Chain Attack) deb ataladi. 2026-yilda yuz bergan ikkita yirik keys buni yaqqol isbotlaydi.

Supply chain hujumi — bevosita nishonga hujum qilish o'rniga, u ishlatadigan uchinchi tomon kutubxonasiga zararli kod kiritish.

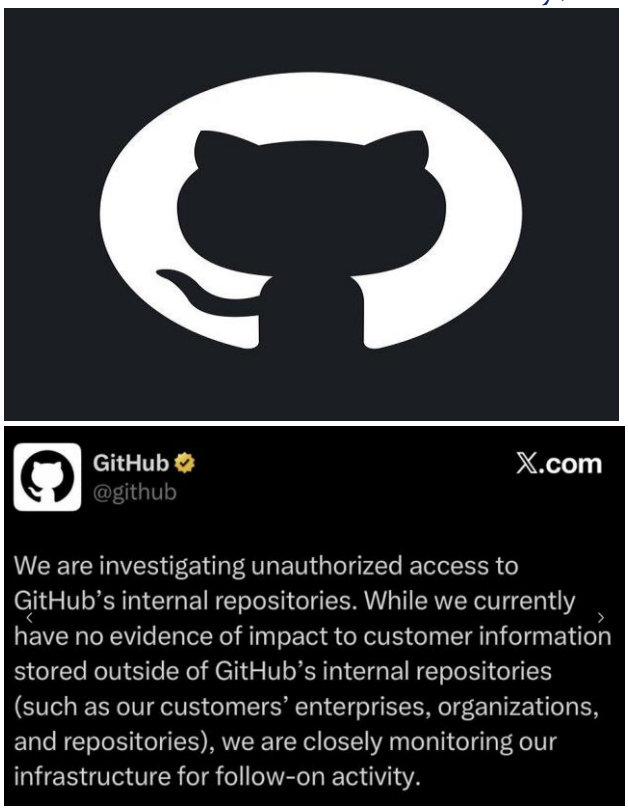
TanStack'ning npm paketlari ichiga zararli kod kiritilgan. Grafana ham o'z CI/CD pipeline'ida TanStack ishlatgan. Zararli paket ishga tushganda GitHub workflow'dagi maxfiy tokenlarni o'g'irlab yuborgan. O'g'irlangan token orqali esa Grafana'ning xususiy repozitoriyalariga kirish imkoni hosil bo'lgan.

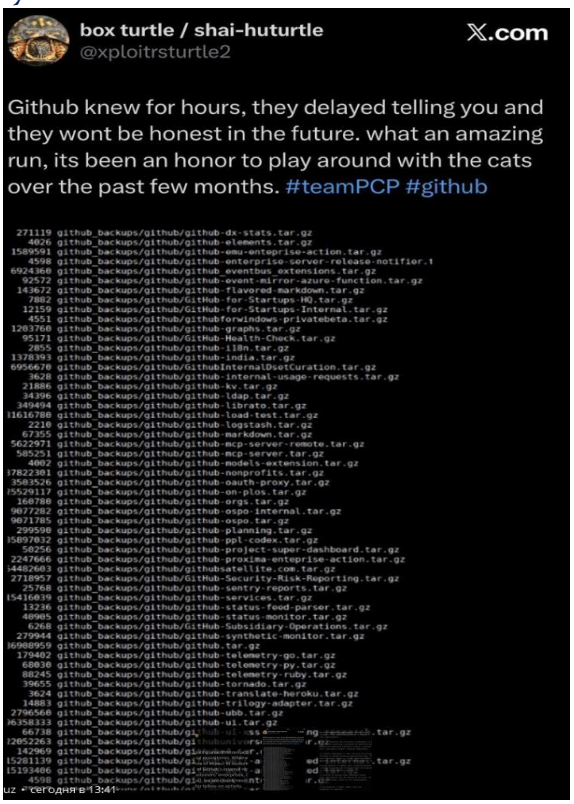
Yana bir supply chain attack bu safar GitHub VS Code kengaytmasi orqali buzildi. Minglab ichki repozitoriyalar sizib chiqdi. GitHub kompaniya xodimlaridan birining kompyuteri kompromitatsiya qilinganligini xabar qildi.

TanStack npm paketi va grafana hodisasi

React, Vue kabi mashhur dasturlash freymvorklari uchun eng ommabop JavaScript kutubxonalar to‘plami hisoblangan **TanStack** npm paketlari ichiga zararli kod kiritilgan. Dunyodagi eng yirik monitoring va vizualizatsiya platformalaridan biri bo‘lgan **Grafana** o‘zining CI/CD (doimiy integratsiya va yetkazib berish) konveyerida aynan ushbu kutubxonadan foydalangan.

Zararli paket avtomatik ravishda ishga tushib, Grafana platformasining GitHub muhitidagi maxfiy workflow tokenlarini (kirish kalitlarini) o‘g‘irlagan. Ushbu o‘g‘irlangan tokenlar yordamida **CoinbaseCartel** deb nomlangan kiberjinoyatchilar guruhi Grafana’ning bir nechta maxfiy (private) repozitoriyalarini to‘liq yuklab olgan va shantaj yo‘li bilan pul talab qilgan. Grafana jamoasining xakerlar bilan muzokaraga kirmasdan, hodisani ochiq e’lon qilgani va infratuzilmani skanerlash uchun maxsus *Grafana Final Scanner* yangi avlod vositasini ishga tushirgani sohadagi inqirozli vaziyatlarni boshqarishga namuna bo‘la oladi.





Dastlabki ma'lumotlarga ko'ra, hujum zararlangan VS Code kengaytmasi orqali amalga oshirilgan. Natijada xakerlar taxminan 4 000 ta ichki repozitoriyaga kirish imkoniga ega bo'ldi. Voqea allaqachon "ichki hodisa" doirasidan chiqib ketdi: xakerlar o'g'irlangan ma'lumotlarni $50 000 ga sotuvga qo'ydi.GitHub keyinroq batafsil hisobot va tekshiruv natijalarini e'lon qilishga va'da berdi. Bu holat ham ko'p narsani ko'rsatib turibdi: bugun supply chain hujumi server, CI/CD yoki bulutdan emas — balki kod muharriridagi oddiy kengaytmadan boshlanishi mumkin.

Kiberhududda 2024–2026-yillar oralig‘idagi dinamika va yirik kiberhujumlar tahlili shuni ko‘rsatadiki, axborot xavfsizligini ta’minlashning an’anaviy, inson omili boshqaradigan va qo‘lda bajariladigan usullari o‘z umrini o‘tab bo‘ldi. Kiberjinoyatchilar AI yordamida soniyalar ichida harakat qilayotgan davrda, himoya tizimlari ham to‘liq avtomatlashtirilgan bo‘lishi shart.

Har qanday rivojlanayotgan davlat va strategik tashkilot o‘z xavfsizligini ta’minlashda quyidagi ilmiy va amaliy tavsiyalarga tayanishi lozim:

1. **Avtonom Himoyaga O‘tish:** Zaifliklarni aniqlash va ularni bartaraf etish (patching) jarayonlarini inson aralashuvisiz bajaruvchi *Autonomous Purple Teaming* texnologiyalarini tatbiq etish.

2. **Ta’minot Zanjiri Monitoringi:** Loyihalarda ishlatilayotgan uchinchi tomon kutubxonalari (npm, pip, nuget va h.k.) va hattoki dasturchilar foydalanadigan IDE kengaytmalarini har kuni avtomatik audit qiluvchi tizimlarni (masalan, *Final Scanner* turidagi vositalarni) joriy etish.

3. **Token va Maxfiy Kalitlar xavfsizligi:** CI/CD tizimlarida qisqa muddatli va cheklangan huquqli tokenlardan foydalanish, GitHub Workflow’larni qat’iy izolyatsiya qilish.

Xulosa qilib aytganda, bugungi kiber-makonda g‘oliblikni faqatgina texnologik jihatdan eng ilg‘or va eng asosiysi — **eng tezkor qaror qabul qila oladigan** tomon qo‘lga kiritadi.

FOYDALANILGAN ADABIYOTLAR RO‘YXATI:

1. Elektron manba: Your Purple Team Isn't Purple, It's Just Slow: How AI-Assisted Attackers Broke the 73-Second Barrier. The Hacker News. May, 2026. Manba: https://thehackernews.com/2026/05/your-purple-team-isnt-purple-its-just.html
2. Elektron manba: Grafana Infrastructure Vulnerability Report and the CoinbaseCartel Ransom Case. Cyber Security Review, 2026.
3. Elektron manba: Zierax. Grafana-Final-Scanner: Automated Infrastructure and Supply Chain Security Auditing Tool. GitHub Repository, 2026. Manba: [https://github.com/Zierax/Grafana-Final-Scanner](https://github.com/Zierax /Grafana-Final-Scanner)
4. Elektron manba: GitHub Internal Incident Report: VS Code Extension Compromise and Repository Leak. GitHub Security Blog, 2026.
5. Elektron manba: National Cyber Security Strategies for Developing Countries: Infrastructure and Automation Needs. International Journal of Cyber Warfare and Terrorism, 14(2), 2025.
6. Elektron manba: www.video-control.ru, www.secnews.ru, www.aamsystems.ru, www.sigma-is.ru, (murojaat sanasi: 25.01.2026-y.)
7. Elektron manba: www.guardtec.ru, www.hitsec.ru, , www.itv.com, www.smartec-cctv.ru, (murojaat sanasi: 25.01.2026-y.)