AMERICAN JOURNAL OF MULTIDISCIPLINARY BULLETIN
ISSN: 2996-511X (online) | ResearchBib (IF) = 9.512 IMPACT FACTOR
Volume-4| Issue-6| 2025 Published: |30-06-2026|

PLASTIK KARTAGA OID JINOYATLARINI ANIQLASHNING INTEGRATSIYALASHGAN YONDASHUVI

https://doi.org/10.5281/zenodo.20947040

Nabiev Inomjon Ayubxon o‘g‘li
Ichki Ishlar Vazirligi Akademiyasi Raqamli texnologiyalar va axborot xavfsizligi kafedrasi katta o‘qituvchisi

Annotatsiya

Maqolada karding – bank kartalari ma’lumotlarini o‘g‘irlash va ularni firibgarlik maqsadlarida qo‘llash bilan bog‘liq jinoyatlarni aniqlash va fosh etishda o‘quv platformalaridan tizimli foydalanish masalalari yoritilgan. Tadqiqotda ushbu jarayonni samarali tashkil etish uchun kiberpoligon asosidagi integratsiyalashgan o‘quv muhiti taklif etiladi. Mazkur muhit SIEM tizimlari, tranzaksiya tahlili, raqamli kriminalistika, OSINT/Darknet monitoring hamda mashinali o‘qitish modullarini yagona laboratoriya doirasida birlashtirish orqali mutaxassislarning amaliy ko‘nikmalarini rivojlantirishga xizmat qiladi.

Kalit so‘zlar

Karding; raqamli kriminalistika; o‘quv platformalari; OSINT; Darknet; SIEM; tranzaksiya tahlili; mashina o‘rganish; dalilga yaroqlilik.

Аннотация

В статье рассматриваются вопросы систематического использования обучающих платформ для выявления и раскрытия преступлений, связанных с кардингом — кражей данных банковских карт и их использованием в мошеннических целях. В исследовании предлагается интегрированная обучающая среда на основе киберполигона для эффективной организации этого процесса. Эта среда служит для развития практических навыков специалистов путем объединения систем SIEM, анализа транзакций, цифровой криминалистики, мониторинга OSINT/Darknet и модулей машинного обучения в рамках единой лаборатории.

Ключевые слова

Кардинг; цифровая криминалистика; обучающие платформы; OSINT; Darknet; SIEM; анализ транзакций; машинное обучение; достоверность доказательств.

Abstract

AMERICAN JOURNAL OF MULTIDISCIPLINARY BULLETIN
ISSN: 2996-511X (online) | ResearchBib (IF) = 9.512 IMPACT FACTOR
Volume-4| Issue-6| 2025 Published: |30-06-2026|

The article discusses the issues of systematic use of training platforms in identifying and exposing crimes related to carding - theft of bank card data and their use for fraudulent purposes. The study proposes an integrated training environment based on cyber polygon for the effective organization of this process. This environment serves to develop the practical skills of specialists by combining SIEM systems, transaction analysis, digital forensics, OSINT/Darknet monitoring and machine learning modules within a single laboratory.

Keywords

Carding; digital forensics; training platforms; OSINT; Darknet; SIEM; transaction analysis; machine learning; evidence validity.

Raqamli iqtisodiyotning jadal rivojlanishi bilan birga kiberjinoyatlar, xususan karding bilan bog‘liq huquqbuzarliklar soni va murakkabligi ortib bormoqda [1]. Zamonaviy karding ekotizimi phishing, skimming, web-skimming, POS-malware, credential stuffing, BIN-range hujumlari hamda bot-tarmoqlar orqali amalga oshiriladigan avtomatlashtirilgan operatsiyalarni o‘z ichiga olgan ko‘p bosqichli tizim sifatida namoyon bo‘ladi. Ushbu jarayonlarning har biri o‘ziga xos raqamli izlar, vaqt dinamikasi va jinoyatchi aktorlar tarmog‘i bilan tavsiflanadi.

Amaliyot shuni ko‘rsatadiki, tezkor xodimlar va tergovchilar uchun ushbu murakkab tizimlarni tushunish ko‘pincha qiyinchilik tug‘diradi. Buning asosiy sababi — nazariy bilimlar va amaliy ko‘nikmalar o‘rtasidagi uzilishdir. Shu nuqtai nazardan, real holatlarga yaqinlashtirilgan, boshqariladigan va xavfsiz muhitda o‘qitishni ta’minlovchi kiberpoligon texnologiyasi muhim ahamiyat kasb etadi [7]. Kiberpoligon yordamida turli kiberhujum ssenariylari modellashtiriladi va foydalanuvchilar ularni tahlil qilish, aniqlash hamda ularga javob berish ko‘nikmalarini shakllantiradi.

Adabiyotlar tahlili. Xalqaro manbalarda (IOCTA, NIST, ISO/IEC 27001 hamda ilmiy maqolalar) karding bozorlarining raqamli ijtimoiy arxitekturasi, dalil to‘plash standartlari, hodisalarga javob berish (IR) mexanizmlari batafsil yoritilgan. O‘quv platformalari bo‘yicha esa masofaviy MOOC, amaliy lablar, CTF, simulyatorlar va SIEM-treninglar kompetensiya asosida loyihalanishi ta’kidlanadi hamda onlayn qora bozorlarning sotsiologik tadqiqotlari karding bozorlarining narx mexanizmlari, ishtirokchilar roli (seller, broker, ‘mule’), escrow tizimi va reklamalar strukturasini ochib beradi. Mazkur ish ana shu yo‘nalishlarni karding kontekstida birlashtiruvchi metodik yechimni taklif etadi. Karding - plastik karta rekvizitlari (PAN, CVV/CVC, trek ma’lumotlari), hisob egalari haqidagi identifikatorlar hamda autentifikatsiya ma’lumotlarini noqonuniy yig‘ish va moliyaviy o‘zlashtirishda qo‘llash, kardingga oid dalillar bilan ishlashda shaxsiy

AMERICAN JOURNAL OF MULTIDISCIPLINARY BULLETIN
ISSN: 2996-511X (online) | ResearchBib (IF) = 9.512 IMPACT FACTOR
Volume-4| Issue-6| 2025 Published: |30-06-2026|

ma’lumotlarni himoya qilish, dalilga yaroqlilik, zanjirli saqlash (chain of custody) tamoyillari alohida ahamiyatga ega.[5] Xalqaro darajada Budapest konvensiyasi prinsiplari, institutsional darajada esa axborot xavfsizligi boshqaruv tizimlari (ISMS) talablariga rioya qilish lozim.

Amaliyotda tezkor xodim va tergovchilar uchun bilimlar tartibsiz (tushunarsiz) holda yetkaziladi (nazariya bir tomonda, laboratoriya mashg‘ulotlari va SIEM simulyatsiyalari boshqa tomonda qoladi). O‘quv platformalari asosida integratsiyalashgan karkas yaratilsa, kompetensiyalar bir yo‘lakda tizimlashtiriladi va natijalar baholash mezonlari orqali ko‘rsatkichga aylantiriladi.

Biroq mavjud adabiyotlarda o‘quv platformalarini aynan kiberpoligon asosida integratsiyalashgan holda qo‘llash masalasi yetarlicha yoritilmagan. Shu bois ushbu maqolada nazariya, amaliyot va texnologik vositalarni yagona tizimga birlashtirishga qaratilgan metodik yondashuv ishlab chiqiladi.

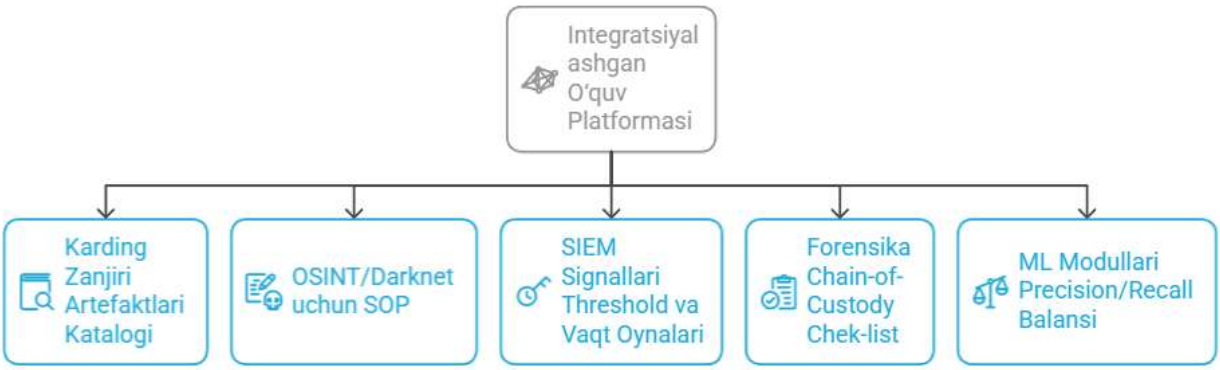
Tadqiqot uch xil (aralash) tipda olib borildi: nazariy tahlil, amaliy modellashtirish va ekspert baholash.

Nazariy tahlilda karding ekotizimi, huquqiy-chegaraviy talablar, dalil standartlari (hash, xronologiya, ruxsatnomalar) va o‘quv dizayni (kompetensiya matritsasi, kapsulalangan ko‘nikmalar) tahlil qilindi. Amaliy modellashtirishda OSINT/Darknet monitoring, SIEM signal korrelyatsiyasi, tranzaksiya naqshlari, malware/forensika tahlili hamda ML anomaliya aniqlash modullari loyihalandi. Ekspert baholash bosqichida tergovchi, tezkor xodim, ekspert-kriminalist va prokurorlar uchun alohida kompetensiya matritsalari tuzildi[5].

Kiberpoligon asosidagi o‘quv jarayoni bosqichma-bosqich tashkil etilib, unda huquqiy va etik asoslardan boshlab, karding zanjiri, OSINT tahlili, SIEM monitoringi, forensika va mashinali o‘qitishgacha bo‘lgan jarayonlar uzviy bog‘langan holda o‘qitiladi. Har bir bosqich real ssenariylar asosida tashkil etilib, unda dalillar to‘plami, tahlil vazifalari va baholash mezonlari aniq belgilab qo‘yiladi.

Ko‘nikma keyslari (aniq natija beruvchi topshiriqlar) quyidagilardan iborat: Dalilga yaroqlilik (xesh, xronologiya, ruxsat), insidentga javob tezligi (MTTD/MTTRga o‘xshash ko‘rsatkichlar), takrorlanish/audit, etik/opsec mosligi, ML modellarida izohlanish va oqilona threshold boshqaruvi (precision/recall/F1, AUC/ROC).

AMERICAN JOURNAL OF MULTIDISCIPLINARY BULLETIN
ISSN: 2996-511X (online) | ResearchBib (IF) = 9.512 IMPACT FACTOR
Volume-4| Issue-6| 2025 Published: |30-06-2026|



Yaratalishi taklif etilayotgan integratsiyalashgan o'quv platformasi quyidagilarni ta'minlaydi:

O'quv yo'lagini (curriculum) ishlab chiqish quyidagi ketma-ketlikda amalga oshiriladi:

1-modulda huquqiy va etik asoslar, 2-modulda karding zanjiri va artefaktlar 3-modulda OSINT/Darknet, 4-modulda SIEM va tranzaksiya tahlili, 5-modulda Malware/forensika, 6-modulda ML va risk bali, 7-modulda dalilga yaroqlilik va protsessual hujjatlar, 8-modulda yakuniy integratsion amaliyotni tashkil etishni amalga oshirish lozim.

Modelga ko'ra, qaror qabul qilish "ma'lumot>gipoteza>tekshiruv>xulosa" ketma-ketligida quriladi va hujjatlashtiriladi. Platformadagi har bir keysda ssenariy, dalillar to'plami, tahlil vazifalari va baholash rubrikasi mavjud bo'lishi shart.

Normativ-huquqiy hujjatlar kadrlar tayyorlash va malaka oshirish tizimini institutsional jihatdan mustahkamlaydi. Jinoyat sxemasini tiklashda vaqt shkalasi (timeline) va graf-bog'lanishlar (nodelink) vizuallashtirishi katta yordam beradi. Tranzaksiya loglari, 3DS holati, qurilma identifikatori va IP-ma'lumotlar korrelyatsiyasi fosh etishda muhim ahamiyatga ega. Mazkur bobda masalaning nazariy va amaliy jihatlari izchil bayon etiladi. Ishda simulyatsion platforma uchun modulli arxitektura taklif qilinib, u ta'lim, monitoring va baholash funksiyalarini birlashtiradi. Interaktiv pedagogik texnologiyalar kursantning analitik fikrlashini va qaror qabul qilish tezligini oshiradi. Karding jinoyatlari ko'p bosqichli bo'lib, har bir bosqichda alohida raqamli izlar shakllanadi.

Shuningdek, axborot xavfsizligi talablari — rollar bo'yicha huquqlar, jurnallash, dalillarning xesh-nazorati — alohida belgilanadi. Normativ-huquqiy hujjatlar kadrlar tayyorlash va malaka oshirish tizimini institutsional jihatdan mustahkamlaydi. Raqamli dalillar bilan ishlashda to'liqlik, haqqoniylik va uzluksizlik tamoyillari ustuvor hisoblanadi.

Pilot mashg'ulotlarda credential stuffing va BIN-rangega yo'naltirilgan hujumlar ketma-ketligi bo'yicha anomaliya indikatorlari ishlab chiqilishi, login

AMERICAN JOURNAL OF MULTIDISCIPLINARY BULLETIN
ISSN: 2996-511X (online) | ResearchBib (IF) = 9.512 IMPACT FACTOR
Volume-4| Issue-6| 2025 Published: |30-06-2026|

muvaffaqiyatsizliklari burstlari, IP/ASN o‘zgaruvchanligi, geolokatsiya sakrashlari kabi ko‘rsatkichlar risk ballini sozlashda samaradorlilikni oshiradi.

Kiberpoligon muhitida amalga oshirilgan pilot mashg‘ulotlar credential stuffing va BIN-range hujumlari misolida anomaliya indikatorlarini aniqlash va risk ballini baholash tizimining samaradorligini oshirdi. Tahlillar natijasida login urinishlaridagi keskin o‘zgarishlar, IP manzillarning tez-tez almashinuvi va geolokatsiya sakrashlari kabi ko‘rsatkichlar kiberhujumlarni erta aniqlashda muhim ahamiyat kasb etishi aniqlandi.[12]

Ishda simulyatsion platforma uchun modulli arxitektura taklif qilinib, u ta’lim, monitoring va baholash funksiyalarini birlashtiradi. Interaktiv pedagogik texnologiyalar kursantning analitik fikrlashini va qaror qabul qilish tezligini oshiradi. Carding jinoyatlari ko‘p bosqichli bo‘lib, har bir bosqichda alohida raqamli izlar shakllanadi. IIV Akademiyasi tomonidan 1-jadvalda keltirilgan **Kompetensiya matritsasi** ishlab chiqildi.

Tizim boshqaruvi rollari va vazifalari

Olingan natijalar shuni ko‘rsatadiki, kiberpoligon asosidagi yondashuv nazariya va amaliyot o‘rtasidagi uzilishni bartaraf etadi hamda mutaxassislarning analitik fikrlashini rivojlantiradi. Bunday muhitda o‘quvchilar real vaziyatlarga maksimal darajada yaqinlashtirilgan sharoitda ishlash imkoniyatiga ega bo‘lib, bu esa ularning kasbiy tayyorgarligini sezilarli darajada oshiradi.

Shu bilan birga, kiberpoligonlardan foydalanishda etik me’yorlarga rioya qilish, shaxsiy ma’lumotlarni himoya qilish va dalillarning yuridik kuchini ta’minlash masalalari alohida e’tibor talab etadi. Ayniqsa, mashinali o‘qitish modellarining izohlanishi va ularning sud jarayonlarida qo‘llanishi dolzarb

AMERICAN JOURNAL OF MULTIDISCIPLINARY BULLETIN
ISSN: 2996-511X (online) | ResearchBib (IF) = 9.512 IMPACT FACTOR
Volume-4| Issue-6| 2025 Published: |30-06-2026|

muammolardan biri hisoblanadi. Shu sababli, izohlanuvchi sun'iy intellekt yondashuvlarini joriy etish muhim ahamiyatga ega.

ML modellarining izohlanishi (LIME/SHAP turkumidagi yondashuvlar, minimal izoh talablariga moslik) tergov va sud jarayonlarida qarorlarni asoslash uchun muhim. Modelni yaratishda drift va adversarial misollarga chidamliligini doimiy monitoring qilib borish quyidagicha talablar asosida yaratilishi lozim:

Amaliy laboratoriya va uni joriy etish yo'l xaritasi bo'yicha:

– kompetensiya matritsasida rol va darajalar aniq belgilanishi;

– modul dizaynida nazariya→ laboratoriya→ osint → siem/ml → huquqiy ketma-ketligida ishlashi;

– baholashda ko'nikma kapsulalari va audit skriptlarini hisobga olishi;

– xavfsizlikni ta'minlashda opsec, etik va pii himoyasini tashkil qilishi;

– institutsionalizatsiyalashda akademiya – amaliy bo'linma hamkorligi, muntazam yangilanish va lessons learned larni muntazam amalga oshirish.

SOP — SIEM/tranzaksiya tahlili bo'yicha:

– ma'lumot manbalari va vaqt oynalari;

– normal bazaviy chiziq (baseline) hisoblash;

– korrelyatsiya qoidalari (failed logins, bin-range urinishlari, qurilma/foydalanuvchi nisbatlari);

– alertlar uchun threshold va eskalatsiya;

– voqea sahnalashtirish va qayta ijro;

– natijalar hisobotini dalilga yaroqli tarzda rasmiylashtirish.

Etika va xatarlarni boshqarish bo'yicha:

–haqiqiy shaxsiy ma'lumotlar bilan ishlash taqiqlanishi;

AMERICAN JOURNAL OF MULTIDISCIPLINARY BULLETIN
ISSN: 2996-511X (online) | ResearchBib (IF) = 9.512 IMPACT FACTOR
Volume-4| Issue-6| 2025 Published: |30-06-2026|

– barcha ma’lumotlar anonimlashtirilgan va yopiq resurslarga kirish faqat qonuniy doirada va ruxsat asosida ta’minlash.

Kiberpoligon asosida tashkil etilgan integratsiyalashgan o‘quv platformasi karding jinoyatlarini aniqlash, tahlil qilish va fosh etish jarayonlarini sezilarli darajada takomillashtiradi. Ushbu yondashuv nafaqat tezkor-tergov faoliyatining samaradorligini oshiradi, balki kiberxavfsizlik sohasida malakali mutaxassislarni tayyorlashda ham muhim vosita bo‘lib xizmat qiladi. Kelgusida ushbu tizimni yanada rivojlantirish, real ma’lumotlar bilan boyitish va sun’iy intellekt asosidagi tahlil usullarini takomillashtirish muhim ilmiy-amaliy yo‘nalishlardan biri bo‘lib qoladi.

Simulyatsiya va model ma’lumotlariga tayanish real dunyo murakkabligini to‘liq aks ettirmasligi mumkin. Kelgusida banklar va to‘lov provayderlari bilan ma’lumot almashuvini kuchaytirgan holda indikatorlar bazasi (IOC) boyitiladi, federativ o‘qitish yondashuvlari sinovdan o‘tkaziladi va sud-ekspertiza uchun izohlanadigan AI standartlari ustida tadqiqotlar olib borilishi kutilmoqda.

FOYDALANILGAN ADABIYOTLAR RO‘YXATI:

1. European Union Agency for Law Enforcement Cooperation. Internet Organised Crime Threat Assessment (IOCTA). – Hague: Europol, 2023.
2. National Institute of Standards and Technology. Guide to Integrating Forensic Techniques into Incident Response (NIST SP 800-86). – Gaithersburg, 2012.

3. International Organization for Standardization. ISO/IEC 27001:2022 Information Security Management Systems – Requirements. – Geneva, 2022.

4. Council of Europe. Convention on Cybercrime (Budapest Convention). – Budapest, 2001.

5. Casey, E. Digital Evidence and Computer Crime: Forensic Science, Computers and the Internet. – Academic Press, 2011.

6. Behl, A., Behl, K. Cybersecurity and Cyberwar: What Everyone Needs to Know. – Oxford University Press, 2017.

7. SANS Institute. Digital Forensics and Incident Response (DFIR) White Papers. – 2020–2024.

8. MITRE Corporation. MITRE ATT&CK Framework. – https://attack.mitre.org

9. Holt, T. J., Smirnova, O., Chua, Y. T. Exploring and Estimating the Revenues of Cybercrime Markets. – Social Science Computer Review, 2016.

10. Krebs on Security. Carding and Payment Fraud Investigations Reports. – 2018–2024.

11. OWASP Foundation. OWASP Top 10: Web Application Security Risks. – 2021.

12. Aggarwal, C. C. Machine Learning for Cybersecurity. – Springer, 2019.

13. Ribeiro, M. T., Singh, S., Guestrin, C. "Why Should I Trust You?" Explaining the Predictions of Any Classifier (LIME). – KDD, 2016.

14. Lundberg, S. M., Lee, S.-I. A Unified Approach to Interpreting Model Predictions (SHAP). – NIPS, 2017.

15. Interpol. Cybercrime: Payment Card Fraud Reports. – 2022–2024

16. Мирзаева, М. Б., & Абдазимов, С. З. (2022). Использование технологий искусственного интеллекта в сфере высшего образования.

17. Abdazimov, S., & Mustafa, D.. (2026). Zamonaviy axborot xavfsizligi tizimlarini loyiihalash: ai va iot yondashuvlari ASOSIDA. *Научный Фокус*, *3*(34), 313-321.

18. Abdazimov, S., & Mustafa, D.. (2026). Simmetrik kriptotizimlarda o ‘rniga qo ‘yish algoritmlarining qiyosiy tahlili va amaliy ahamiyati. *Научный Фокус*, *3*(34), 231-237.

19. Abdazimov, S., & Mustafa, D. (2026). Biometric authentication: modern methods of ensuring information security. *Научный Фокус*, *3*(34), 222-230.

20. Saidaminxo'Dja Zoirxo'Dja, O. G., & Abdazimov, L. (2022). Ijtimoiy tarmoqlarda axborot xurujlarini tarqalish ehtimolligini bashoratlash va ulardan himoyalash usuli va modellari. *Central Asian Research Journal for Interdisciplinary Studies (CARJIS)*, *2*(5), 109-115.