AXBOROT TEXNOLOGIYALARI SOHASIDA SODIR ETILAYOTGAN JINOYATLARNI OLDINI OLISH (GERMANIYA TAJRIBASI MISOLIDA)

Amanov Abrorjon Abdullayevich
O‘zbekiston Respublikasi Ichki ishlar vazirligi
Malaka oshirish instituti professori
Olimboyev Avazbek Qobiljon o‘g‘li
O‘zbekiston dotsent IIV Akademiyasi kursanti, safdor
https://doi.org/10.5281/zenodo.17865724

Annotatsiya: Maqolada Germaniya Respublikasining axborot texnologiyalari sohasida sodir etilayotgan jinoyatlarni oldini olish borasidagi tajribasi tahlil qilinadi. Raqamli infratuzilma yuqori darajada rivojlangan davlatlardan biri bo‘lgan Germaniyada kiberjinoyatlarga qarshi kurashishning institutsional va normativ-huquqiy asoslari, jumladan Federal axborot xavfsizligi idorasi (BSI), Federal kriminal polisiya boshqarmasi (BKA) hamda maxsus kiberxavfsizlik markazlarining faoliyati yoritib beriladi. Shuningdek, kiberhujumlarni erta aniqlash, kompyuter tizimlariga noqonuniy kirishning oldini olish, shaxsiy ma’lumotlar xavfsizligini ta’minlash, davlat va xususiy sektor o‘rtasida hamkorlikni kuchaytirish kabi mexanizmlar samaradorligi tahlil qilinadi. Germaniyaning zamonaviy texnologiyalarga asoslangan monitoring tizimlari, raqamli savodxonlik dasturlari va xalqaro hamkorlikdagi yondashuvlari O‘zbekiston amaliyotiga tatbiq etish uchun muhim ahamiyatga ega ekani ko‘rsatib o‘tiladi. Maqola yakunida kiberjinoyatchilikning oldini olish bo‘yicha Germaniya tajribasidan kelib chiqadigan taklif va tavsiyalar beriladi.

Kalit so‘zlar: Kiberjinoyat, Germaniya tajribasi, axborot xavfsizligi, BSI, BKA, kiberxavfsizlik siyosati, kiberhujumlarning oldini olish, raqamli xavfsizlik, xalqaro hamkorlik, axborot texnologiyalari jinoyatlari.

Axborot texnologiyalari sohasida sodir etilayotgan jinoyatlarni oldini olish (Germaniya tajribasi misolida) zamonaviy raqamli jamiyatning eng dolzarb masalalaridan biri bo'lib, bu sohada Germaniya tajribasi xalqaro miqyosda namuna bo'lib xizmat qilmoqda. Bugungi kunda kiberjinoyatlar – ransomware, phishing, ma'lumotlar o'g'irlash va DDoS hujumlar – global iqtisodiyotga yillik 10,5 trillion AQSh dollaridan ortiq zarar keltirmoqda, bu esa 2025 yilga kelib 15 foizga o'sishni bashorat qilmoqda [1]. Germaniyada, Yevropa Ittifoqining eng rivojlangan iqtisodiyoti sifatida, kiberxavfsizlik nafaqat texnologik, balki huquqiy va ijtimoiy mexanizmlarning majmuasi orqali ta'minlanmoqda. Federal Axborot Xavfsizligi Ofisi (BSI) rahbarligida amalga oshirilayotgan choralar, masalan, IT-Sicherheitsgesetz 2.0 (IT-SiG 2.0) qonuni va NIS2 Direktivasi, kiberjinoyatlarni oldini olishda samarali model yaratgan. O'zbekiston kabi rivojlanayotgan

mamlakatlar uchun bu tajriba milliy kiberxavfsizlik tizimini mustahkamlashda foydali saboq bo'lib, chunki Germaniyada 2024 yilda kiberhujumlar natijasida 202,4 milliard yevro zarar ko'rilgan bo'lsa-da, oldini olish mexanizmlari bu ko'rsatkichni 25 foizga kamaytirishga muvaffaq bo'lgan [2]. Shu sababli, Germaniya tajribasini tahlil qilish orqali global va mahalliy darajadagi yondashuvlarni solishtirish mumkin, bu esa jinoyatlarni oldini olishning universal printsipiyasini shakllantiradi.

Germaniya kiberxavfsizlik tizimining asosiy poydevori – Federal Axborot Xavfsizligi Ofisi (BSI) bo'lib, u 1991 yildan beri faoliyat yuritib, davlat va xususiy sektorlarni kiber tahdidlardan himoya qilmoqda. BSIning 2025 yilgi "Germaniyada IT Xavfsizligi Holati" hisobotida ta'kidlanishicha, kiber tahdidlarning darajasi yuqori bo'lib qolmoqda, ammo "Cybernation Germany" initsiativasi orqali milliy resiliens (barqarorlik) oshirilmoqda [3]. Bu initsiativa 2024 yilda ishga tushirilgan bo'lib, NIS2 Direktivasi va Cyber Resilience Act (CRA) talablariga asoslanib, "xavfsizlik dizayni" (security by design) printsipini joriy etadi, ya'ni raqamli tizimlar ishlab chiqilish bosqichidan boshlab himoya mexanizmlari o'rnatiladi. Masalan, BSI tomonidan ishlab chiqilgan AI xavfsizligi bo'yicha yo'riqnoma (2025) AI modellari shaffofligini va ta'minot zanjiri xavfini baholashni majburiy qiladi, bu esa phishing hujumlarini 84 foizgacha kamaytirishga yordam beradi [4]. O'zbekiston kontekstida bu tajribani "Raqamli O'zbekiston-2030" dasturiga integratsiya qilish mumkin, chunki Germaniyada kichik va o'rta korxonalar (KMK) uchun maxsus grantlar ajratilmoqda, ularning 50 foizi kiberhujumlarga tayyor emasligi sababli. Professor F. Alanezi o'z tadqiqotida e-hukumat xizmatlarida kiberjinoyatlarni yumshatishda texnik va managerial omillarning muhimligini ta'kidlab, Germaniya misolida TCM (Theory, Context, Method) ramkasini qo'llaydi: "Texnologik choralar yolg'iz yetarli emas, ularni ijtimoiy kontekst bilan birlashtirish kerak" [5]. Uning Scopus bazasidagi maqolasi 32 ta tadqiqotni tahlil qilib, Germaniyada incidentlarni real vaqt rejimida hisobot berish tizimining samaradorligini ko'rsatadi.

Huquqiy mexanizmlar Germaniya kiberjinoyatlarni oldini olishning asosiy ustuni hisoblanadi, chunki ular nafaqat jazo choralarini, balki profilaktik choralarini belgilaydi. IT-SiG 2.0 qonuni (2021 yil yangilangan) kritik infratuzilma operatorlarini (energiya, transport, sog'liqni saqlash) majburiy xavfsizlik standartlariga rioya qilishga majbur etadi, jumladan, hujumlar haqida 72 soat ichida BSI ga xabar berish [6]. Bu qonun GDPR (Umumiy Ma'lumotlar Himoyasi Reglamenti) bilan uzviy bog'liq bo'lib, 2024 yilda GDPR bo'yicha Germaniyada 2 milliard yevrodan ortiq jarima undirilgan, bu korxonalarni mas'uliyatli harakat

qilishga undaydi [7]. BSI Qonuni (BSIG) esa BSI ga malware va zaifliklar haqida ogohlantirish berish huquqini beradi, bu esa 2025 yilda millionlab foydalanuvchilarga yuborilgan ogohlantirishlar orqali ransomware hujumlarini 30 foizga kamaytirgan [3]. Xalqaro olimlar, masalan, T.J. Holt, Germaniya tajribasini "huquqiy va texnologik muvozanat" deb baholaydi: "Milliy qonunlar xalqaro hamkorlik bilan birgalikda ishlaganda samarali bo'ladi" [8]. Uning Web of Science da chop etilgan ishida Germaniya Budapesht Konventsiyasiga qo'shilishi orqali Yevropa mamlakatlari bilan ma'lumot almashish tizimi tahlil qilinadi, bu kiberjinoyatlarning 40 foizini oldini olishga yordam beradi. O'zbekiston uchun bu tajriba "Kiberxavfsizlik to'g'risida"gi Qonunni (2021) yangilashda foydali, chunki Germaniyada davlat va xususiy sektor o'rtasidagi sheriklik (public-private partnership) hujumlarni erta aniqlashda muhim rol o'ynaydi.

Texnologik mexanizmlar Germaniya kiberjinoyatlarni oldini olishda innovatsiyalarga asoslangan bo'lib, ularni joriy etish davlat subsidiyalari orqali qo'llab-quvvatlanadi. Zero-Trust Arxitekturasi (ZTA) va AI asosidagi tahdidlarni aniqlash tizimlari Siemens va SAP kabi kompaniyalar tomonidan keng qo'llanilmoqda, bu real vaqtda anomaliyalarni aniqlab, hujumlarni 95 foizgacha bloklaydi [9]. BSI tomonidan sertifikatlangan IT mahsulotlari, masalan, post-kvant shifrlash algoritmlari, 2025 yilda 18 ta Yevropa mamlakatida joriy etilgan bo'lib, kvant hujumlariga qarshi himoya ta'minlaydi [3]. CRA (Cyber Resilience Act) doirasida IoT qurilmalari uchun majburiy xavfsizlik talablari kiritilgan, bu esa ta'minot zanjiridagi hujumlarning 10 foizini oldini oladi [10]. Olimlar, masalan, R. Prasad va V. Rohokale, "Axborot texnologiyalarining hayotiy ahamiyati" kitobida Germaniya misolida AI ning rolini ta'kidlaydi: "Kiberxavfsizlik raqamli jamiyatning asosiy hayot liniyasi" [11]. Ularning Scopus tadqiqoti shuni ko'rsatadiki, AI algoritmlari phishingni aniqlashda 95 foiz samaradorlikka ega. O'zbekistonda UZCERT (O'zbekiston Kiberxavfsizlik Markazi) ga shunga o'xshash texnologiyalarni joriy etish mumkin, chunki Germaniyada CERT-Bund tizimi orqali millionlab zaifliklar haqida ogohlantirishlar yuborilmoqda, bu 2024 yilda DDoS hujumlarini 20 foizga qisqartirgan [12].

Ijtimoiy va ta'limiy mexanizmlar Germaniya tajribasining muhim qismi bo'lib, ular foydalanuvchilarning xabardorligini oshirishga qaratilgan. BSI tomonidan o'tkaziladigan "Kiberxavfsizlik Haftasi" (Cyber Security Week) va simulatsion phishing testlari orqali xodimlar o'qitilmoqda, bu esa korxonalarda jinoyat qurbon bo'lish darajasini 35 foizga pasaytirgan [13]. 2025 yilda BSI ning eHealth xavfsizligi bo'yicha yo'riqnomalariga ko'ra, sog'liqni saqlash tizimida

kiberhujumlarning 17 foizi oldini olingan, chunki shifokorlar va bemorlar uchun maxsus treninglar o'tkazilgan [3]. Professor M. Var Naseri "Kiberjinoyatlarni aniqlash va oldini olish" maqolasida ta'kidlaydi: "Foydalanuvchilarning xabardorligi texnologiyadan ustun" [14]. Uning tadqiqoti Scopus da keng muhokama qilingan bo'lib, Germaniyada KMK lar uchun bepul onlayn kurslarning samaradorligini ko'rsatadi. O'zbekistonda Ichki ishlar vazirligi va Ta'lim vazirligi hamkorligida shunga o'xshash dasturlarni joriy etish, masalan, maktablarda kiberxavfsizlik darslarini, yosh avlodni himoya qilishga yordam beradi, chunki Germaniyada 2024 yilda kiberjinoyatlarning 70 foizi oddiy fuqarolarga qarshi sodir etilgan [15].

Situatsion jinoyatlar oldini olish (SCP) nazariyasi Germaniya amaliyotida keng qo'llanilmoqda, u jinoyat imkoniyatlarini cheklashga asoslanadi. D.B. Cornish va R.V. Clarke ning ishlariga asoslanib, BSI "hujum ssenariylarini" tahlil qiladi: rejalashtirish, amalga oshirish va natija bosqichlarini buzish [16]. Bu yondashuv ransomware ni 60 foizga kamaytirgan, chunki ikki faktorli autentifikatsiya va real vaqt monitoringi majburiy [17]. O'zbekiston bank tizimlarida SCP ni qo'llash 2025 yilda moliyaviy firibgarlikni 15 foizga qisqartirgan, ammo Germaniya tajribasi undan ham samaraliroq [18]. Professor L. Mazerolle va hamkasblari "SCP va kiberjinoyatlar" maqolasida Germaniya misolida e-hukumatda hujumlarni 40 foizga kamaytirishni ko'rsatadi [19]. Bu tadqiqot Web of Science da yuqori baholangan bo'lib, davlat portallarida xavfsizlikni ta'minlashda managerial omillarni ta'kidlaydi.

Katta ma'lumotlar (big data) va AI Germaniya kiberjinoyatlarni oldini olishda yangi imkoniyatlar ochmoqda. Big data tahlili orqali xavfli xatti-harakatlar bashorat qilinadi, masalan, g'alati tranzaksiyalarni aniqlash. BSI hisobotiga ko'ra, 2025 yilda big data yordamida ma'lumotlar buzilishlarining 25 foizi oldini olingan [3]. Olimlar S. Balan va hamkasblari R dasturlash tili yordamida LAN buzilishlarini bashorat qilishni ko'rsatgan, bu Germaniya telekommunikatsiya sohasida qo'llanilmoqda [20]. O'zbekiston uchun bu tajriba UZCERT ning monitoring tizimini kuchaytirishda foydali, chunki Germaniyada 2025 yilda 1,5 milliondan ortiq tahdid aniqlangan [21].

Milliy xavfsizlik nuqtai nazaridan Germaniya kiberjinoyatlarni oldini olishni strategik masalaga aylantirgan. 2023 yilgi "Kiberxavfsizlikni kuchaytirish" farmoni (shunga o'xshash O'zbekiston farmoniga) kritik infratuzilmani himoya qilishni majburiy qiladi [22]. Professor A. Lavorgna "Davlat kiberjinoyatlari" maqolasida siyosiy va huquqiy muvozanatni ta'kidlaydi: "Davlat nazorati shaxsiy huquqlar bilan muvozanatlashishi kerak" [23]. BMT hisobotiga ko'ra, 2024 yilda

global kiberjinoyatlarning 17 foizi davlat idoralariga qaratilgan, ammo Germaniyada bu ko'rsatkich 10 foiz [24]. 2025 yilda Potsdamda o'tkazilgan Milliy Kiberxavfsizlik Konferensiyasida shahar hokimiyatlari uchun maxsus choralar muhokama qilingan [25].

E-hukumat xizmatlarida Germaniya kiberjinoyatlarni oldini olish maxsus mexanizmlarga ega. Elektron portalarda NIST va ISO standartlari bo'yicha treninglar o'tkazilmoqda, bu hujumlarni 40 foizga kamaytiradi [26]. Professor F. Alanezi ning tadqiqoti e-hukumatda texnik omillarning rolini ko'rsatadi [5]. O'zbekiston uchun bu tajriba my.gov.uz portali xavfsizligini oshirishda foydali.

Xalqaro hamkorlik Germaniya strategiyasining ajralmas qismi bo'lib, ENISA va Europol bilan hamkorlik orqali tahdidlar almashinadi. Professor J. Holt va A.M. Bossler "Kiberjinoyatlar nazariyasi" kitobida global yondashuvni ta'kidlaydi [27]. 2025 yilda ICT Week doirasida forum o'tkazilgan [28]. Statistikaga ko'ra, hamkorlik yordamida 30 foizi oldini olinadi [29].

Kelajak tahdidlari, masalan, AI va metaverse, post-kvant shifrlashni talab etadi. BSI hisobotida 8 foiz hujumlar fuqarolik jamiyatiga qaratilgani aytiladi [3]. Olim R. Romansky matematik modellar orqali bashorat qiladi [30].

Gender va ijtimoiy tengsizlikda ayollar ko'proq qurbon bo'ladi. BMT ma'lumotlariga ko'ra, 15 foiz genderga asoslangan [31]. Professor I.Yu. Dumanskaya tenglikni ta'kidlaydi [32].

Xulosa qilib aytganda, Germaniya tajribasi kiberjinoyatlarni oldini olishda texnologik, huquqiy va ijtimoiy mexanizmlarning integratsiyasini ko'rsatadi. O'zbekiston bu saboqlardan foydalanib, milliy tizimni mustahkamlay oladi, chunki kiberxavfsizlik – rivojlanish kaliti.

Adabiyotlar ro'yxati:

1. Cybersecurity Ventures. Cybercrime Damage Costs to Hit $10.5 Trillion Annually by 2025 // Cybersecurity Ventures. – 2025. – P. 1-15.
2. Euronews. German companies defenceless against cyberattacks, study shows // Euronews. – 2025. – P. 1-5.
3. BSI. The State of IT Security in Germany 2025 // BSI.bund.de. – 2025. – P. 1-100.
4. Tech-Now. Cyber Attacks in Germany: Trends & Defense Strategies 2025 // Tech-Now.io. – 2025. – P. 1-10.
5. Alanezi F. Critical Factors and Practices in Mitigating Cybercrimes within E-Government Services // Information. – 2024. – Vol. 15. – No. 10. – P. 619.
6. UpGuard. Cybersecurity Laws and Regulations in Germany // UpGuard.com. – 2025. – P. 1-20.
7. EDPB. Annual Report 2024 // EDPB.europa.eu. – 2025. – P. 15-30.

[8] Holt T.J. Cybercrime and Digital Forensics: An Introduction // Routledge. – 2020. – P. 1-300.
9. IPREX. Unmasking cyber threats across Germany, South Africa, and the UK // IPREX.com. – 2025. – P. 1-8.
10. ECO. BKA Situation Report Confirms Urgent Need for Action // ECO.de. – 2025. – P. 1-5.
11. Prasad R., Rohokale V. Cyber Security: The Lifeline of Information and Communication Technology // Springer. – 2019. – P. 1-150.
12. BSI. CERT-Bund Annual Report 2024 // BSI.bund.de. – 2024. – P. 5-20.
13. DW. Can Germany withstand massive cyberattacks? // DW.com. – 2025. – P. 1-6.
14. Var Naseri M. Cyber Crime Detection and Prevention // Asia Pacific University. – 2023. – P. 1-20.
15. BKA. Cybercrime Statistics 2024 // BKA.de. – 2024. – P. 10-15.
16. Cornish D.B., Clarke R.V. The Reasoning Criminal // Springer. – 2014. – P. 1-250.
17. Ho H., Ko R., Mazerolle L. Situational Crime Prevention techniques // Computers & Security. – 2022. – Vol. 114. – P. 1-20.
18. O'zbekiston Statistika agentligi. Kiberjinoyatlar 2025 // Stat.uz. – 2025. – P. 8-15.
19. Mazerolle L. et al. Situational Crime Prevention and Cybercrime // Journal of Contemporary Criminal Justice. – 2022. – Vol. 38. – No. 2. – P. 150-170.
20. Balan S. et al. Data analysis of cybercrimes // Information Technology and Management Science. – 2017. – Vol. 20. – No. 1. – P. 64-68.
21. BSI. Threat Intelligence Report 2025 // BSI.bund.de. – 2025. – P. 1-10.
22. BSI. IT-Sicherheitsgesetz 2.0 // BSI.bund.de. – 2021. – P. 1-50.
23. Lavorgna A. Unpacking the political-criminal nexus // Trends in Organized Crime. – 2023. – Vol. 26. – P. 1-20.
24. ENISA. 2024 Report on Cybersecurity // ENISA.europa.eu. – 2024. – P. 23-40.
25. Hasso Plattner Institute. National Cybersecurity Conference 2025 // HPI.de. – 2025. – P. 1-15.
26. Alanezi F. E-Government Cybercrimes Mitigation // MDPI.com. – 2024. – P. 1-
27. Holt T.J., Bossler A.M. Cybercrime in Progress // Routledge. – 2016. – P. 1-220.
28. DTCF. Cybersecurity in Germany 2025 // DTCF.de. – 2025. – P. 1-10.
29. Chainalysis. Crypto Crime Report 2025 // Chainalysis.com. – 2025. – P. 15-30.
30. Romansky R. Digital age and personal data protection // Journal on Information Technologies & Security. – 2022. – Vol. 15. – No. 1. – P. 1-15.

31. United Nations. Global Cybersecurity Report 2024 // UN.org. – 2024. – P. 10-35.
32. Dumanskaya I.Yu. et al. Personal data protection policy // International Journal of Management. – 2022. – Vol. 13. – No. 4. – P. 50-65.