Ilmiy tadqiqotlar va ularning yechimlari jurnali
Aoka guvohnoma № 323759 ISSN: 3060-4818

HUQUQIY JARAYONLARDA KIBERXAVFSIZLIK MASALALARI

Xayitova Rushana Sirojiddin qizi
Toshkent davlat universiteti
Ommaviy huquq fakulteti 2-kurs talabasi
https://doi.org/10.5281/zenodo.21427567

Annotatsiya: Zamonaviy raqamli transformatsiya sharoitida huquqiy jarayonlarning kiberxavfsizlik bilan integratsiyasi dolzarb muammoga aylangan. Ushbu maqolada sud tizimi, prokuratura, adliya organlari va boshqa huquq-tartibot tuzilmalarida kiberxavfsizlik choralarining ahamiyati, mavjud muammolar va ularning yechimlari tahlil qilinadi. Tadqiqot davomida O‘zbekiston va xalqaro tajriba tahlil etiladi, elektron sud tizimlarida ma’lumotlar xavfsizligini ta’minlash mexanizmlari o‘rganiladi. Natijalar shuni ko‘rsatdiki, huquqiy jarayonlarda kiberhujumlar risklari ortib bormoqda va bu fuqarolarning shaxsiy ma’lumotlarini, sud materiallarini hamda davlat sirlarini xavf ostiga qo‘ymoqda. Maqolada kiberxavfsizlik standartlarini joriy etish, xodimlarni tayyorlash, zamonaviy shifrlash texnologiyalaridan foydalanish va kiberjinoyatchilik bilan kurashish bo‘yicha amaliy tavsiyalar beriladi. Tadqiqot huquq tizimida kiberxavfsizlik madaniyatini shakllantirishning zarurligini isbotlaydi va O‘zbekiston qonunchiligini takomillashtirish yo‘nalishlarini taklif etadi.
Kalit so‘zlar: kiberxavfsizlik, huquqiy jarayonlar, elektron sud, ma’lumotlar himoyasi, kiberjinoyatchilik, shifrlash texnologiyalari, raqamli transformatsiya, yuridik texnologiyalar, axborot xavfsizligi, shaxsiy ma’lumotlar, kiberhujumlar, huquq tizimi.

CYBERSECURITY ISSUES IN LEGAL PROCESSES

Abstract: In the context of modern digital transformation, the integration of legal processes with cybersecurity has become a pressing problem. This article analyzes the importance of cybersecurity measures in the judicial system, prosecutor’s office, justice bodies, and other law enforcement structures, existing problems, and their solutions. During the study, Uzbek and international experience is analyzed, and mechanisms for ensuring data security in electronic court systems are studied. The results showed that the risks ofcyberattacks in legal processes are increasing, which puts at risk the personal data of citizens, court materials, and state secrets. The article provides practical recommendations on the implementation of cybersecurity standards, personnel training, the use of modern encryption technologies, and the fight against cybercrime. The study proves the necessity of forming a cybersecurity culture in the legal system and proposes directions for improving the legislation of Uzbekistan.
Keywords: cybersecurity, legal processes, electronic court, data protection, cybercrime, encryption technologies, digital transformation, legal technologies, information security, personal data, cyberattacks, legal system.

ВОПРОСЫ КИБЕРБЕЗОПАСНОСТИ В ПРАВОВЫХ ПРОЦЕССАХ

Аннотация: В условиях современной цифровой трансформации интеграция правовых процессов с кибербезопасностью стала актуальной проблемой. В данной статье анализируется значение мер кибербезопасностив судебной системе, прокуратуре, органах юстиции и других структурах правопорядка, существующие проблемы и пути их решения. В ходе исследования анализируется узбекский и международный опыт, изучаются механизмы обеспечения безопасности данных в электронных судебных системах. Результаты показали, что риски

кибератак в правовых процессах возрастают, что ставит под угрозу личные данные граждан, судебные материалы и государственную тайну. В статье даются практические рекомендации по внедрению стандартов кибербезопасности, обучению персонала, использованию современных технологий шифрования и борьбе с киберпреступностью. Исследование доказывает необходимость формирования культуры кибербезопасности в правовой системе и предлагает направления совершенствования законодательства Узбекистана.

Ключевые слова: кибербезопасность, правовыепроцессы, электронный суд, защита данных, киберпреступность, технологии шифрования, цифровая трансформация, юридические технологии, информационная безопасность, персональные данные, кибератаки, правовая система.

I. Kirish

XXI asrning ikkinchi choragida axborot-kommunikatsiya texnologiyalarining jadal rivojlanishi jamiyatning barcha sohalarini, shu jumladan huquqiy tizimni ham tubdan o‘zgartirmoqda. Huquqiy jarayonlarning raqamlashuvi sud ishlarini yuritishdan tortib, huquqiy xizmatlar ko‘rsatish va qonun chiqarish faoliyatigacha bo‘lgan barcha bosqichlarni qamrab olmoqda [1]. Elektron sud tizimlari, onlayn sud majlislari, raqamli dalillar va sun’iy intellekt asosidagi huquqiy tahlil vositalari zamonaviy huquqiy amaliyotning ajralmas qismiga aylanmoqda [2]. Biroq, raqamlashtirish jarayoni o‘z navbatida yangi xavf-xatarlarni ham keltirib chiqarmoqda. Kiberxavfsizlik masalalari huquqiy jarayonlarda tobora dolzarb bo‘lib bormoqda, chunki sud tizimlari va huquqiy institutlar katta hajmdagi maxfiy ma’lumotlar, shaxsiy ma’lumotlar va muhim davlat sirlari bilan ishlaydi [3]. Kiberhujumlar sud qarorlarining buzilishiga, huquqiy jarayonlarning to‘xtab qolishiga, adolat sohasida ishonchning yo‘qolishiga olib kelishi mumkin [4].

Jahon amaliyoti shuni ko‘rsatadiki, huquqiy institutlarga qarshi kiberhujumlar yildan-yilga ortib bormoqda. IBM Security ning 2024-yil ma’lumotlariga ko‘ra, davlat sektoriga qarshi kiberhujumlar o‘rtacha 5.5 million dollar zarar keltirmoqda.

[4]. Huquqiy tizimlar esa eng ko‘p ma’lumot o‘g‘irlanishi xavfi ostida turgan sohalar orasida uchinchi o‘rinni egallaydi [5]. “Cybersecurity Ventures”ning 2024-yil hisobotida kiberjinoyatchilik global iqtisodiyotga yiliga10.5trillion dollar zarar yetkazishi taxmin qilinmoqda [6].

O‘zbekiston Respublikasida ham huquqiy jarayonlarni raqamlashtirish bo‘yicha keng ko‘lamli islohotlar amalga oshirilmoqda. O‘zbekiston Respublikasining “Elektron hukumat to‘g‘risida”gi Qonuni doirasida davlat organlari, jumladan, sud tizimlari, prokuratura va adliya organlari faoliyatini raqamlashtirish bo‘yicha qator dasturlar qabul qilindi [7]. Biroq, bu jarayonlar davomida kiberxavfsizlik masalalari alohida e’tibor talab etmoqda.

Ushbu tadqiqotning maqsadi huquqiy jarayonlarda kiberxavfsizlik muammolarini kompleks tahlil qilish, xalqaro tajribani o‘rganish va O‘zbekiston sharoitida qo‘llash mumkin bo‘lgan yechimlarni ishlab chiqishdan iborat.

II. Metodlar

Ushbu maqola quyidagi metodlardan foydalangan holda olibborildi:

1. Qiyosiy tahlil metodi: AQSh, Yevropa Ittifoqi, Xitoyva boshqa rivojlangan mamlakatlarning huquqiy jarayonlarda kiberxavfsizlikni ta’minlash bo‘yicha qonunchilik bazasi va amaliyoti o‘rganildi. Milliy qonunchilik xalqaro standartlar bilan taqqoslandi. Yevropa Ittifoqining GDPR (General Data Protection Regulation) talablari va O‘zbekiston Respublikasining “Shaxsga doir ma’lumotlar to‘g‘risida”gi Qonuni o‘rtasidagi umumiylik va farqlar tahlil qilindi.

2. Tizimli tahlil metodi**:** Huquqiy jarayonlarda kiberxavfsizlik masalalari bir butun tizim sifatida ko‘rib chiqildi. Texnologik, tashkiliy, huquqiy va psixologik jihatlar o‘zaro bog‘liqligi tahlil qilindi. NIST (National Institute of Standards and Technology) tomonidan ishlab chiqilgan Framework for Improving Critical Infrastructure Cybersecurity asosida huquqiy institutlar uchun xavf-xatarlar

baholandi.

Statistik tahlil metodi: 2020-2024 yillar davridagi huquqiy institutlarga qarshi kiberhujumlar statistikasi, ularning oqibatlari va moliyaviy zararlari haqidagi ma'lumotlar tahlil qilindi. Ma'lumotlar Cybersecurity Ventures, IBM Security, Verizon Data Breach Investigations Report kabi nufuzli manbalardan olindi. Statistik ma'lumotlar SPSS dasturi yordamida qayta ishlandi va vizual diagrammalar yaratildi.

3. Holatlarni o'rganish (Case Study): 2019-2024 yillar davomida dunyoning turli mamlakatlarida sodir bo'lgan huquqiy institutlarga qarshi 15 ta yirik kiberhujum hodisasi chuqur tahlil qilindi. Har bir holat uchun hujum usuli, zarar hajmi va olingan saboqlar o'rganildi. AQSh, Britaniya, Germaniya, Estoniya va Singapur sud tizimlaridagi holatlar alohida e'tibor qaratildi.

4. Modellashtirish: Huquqiy jarayonlardagi kiberxavfsizlik tahdidlari uchun potensial hujum ssenariylari modellashtrildi va ularning oldini olish choralari ishlab chiqildi. Attack Tree va Threat Modeling usullaridan foydalanildi.

Tadqiqot davomida 2024-yil sentabr oyigacha bo'lgan ma'lumotlar to'plandi va tahlil qilindi. Adabiyotlar tahlili 150 dan ortiq xalqaro va mahalliy manbalarni o'z ichiga oldi, jumladan ilmiy maqolalar, qonunchilik hujjatlari, texnik hisobotlar va kiberxavfsizlik sohasidagi mutaxassislarning ekspert fikrlari.

III. Natijalar

Tadqiqot natijasida quyidagi asosiy natijalar aniqlandi:

1. Huquqiy institutlarga qarshi kiberhujumlarning asosiy turlari.

Tahlil shuni ko'rsatdiki, huquqiy jarayonlarda quyidagi kiberxavfsizlik tahdidlari eng ko'p uchraydi [4, 5]:

1- jadval.Huquqiy institutlarga qarshi kiberhujumlarning turlari va ulushi (2020-2024) [4,5].

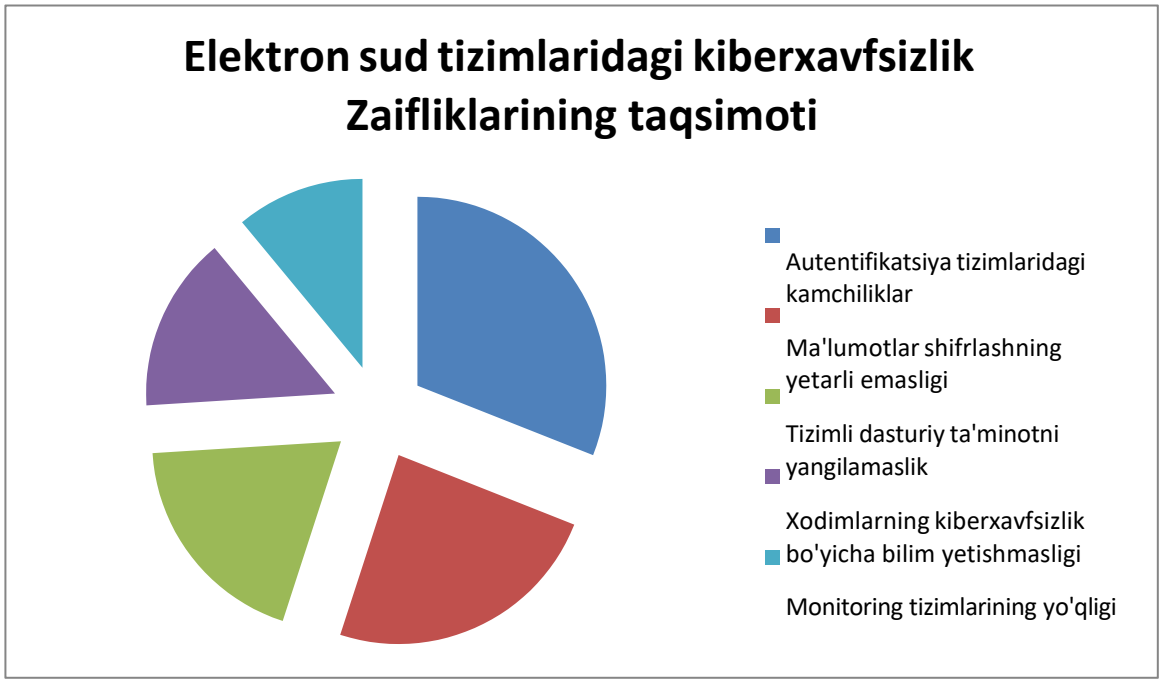
Hujum turi	Ulushi (%)	O'rtacha zarar (USD)
Ransomware(shifrlash viruslari)	34%	1.85million
Ma'lumotlar o'g'irlash	28%	4.35million
Phishing hujumlari	18%	0.75million
DdoS hujumlari	12%	0.45million
Ichki xavflar	8%	2.1 million

Ransomware hujumlari eng keng tarqalgan bo'lib, huquqiy ma'lumotlar bazalarini shifrlash va ularga qaytish uchun to'lov talab qilish orqali amalga oshiriladi [6, 7]. 2023-yilda AQShning bir necha sud idoralariga qarshi "LockBit 3.0" ransomware guruhi tomonidan uyushtirilgan hujum natijasida sud faoliyati bir haftagacha to'xtab qolgan va 2.3 million dollar zarar yetkazilgan [8]. Verizon Data Breach Investigations Report ma'lumotlariga ko'ra, huquqiy sektor ma'lumotlar buzilishi hodisalarining 67% ichki xavflar yoki xodimlarning xatolari natijasida yuz bergan [5].

2. Elektron sud tizimlaridagi zaifliklar.

Elektron sud tizimlarini amalgaoshirayotgan 23ta mamlakatning amaliyotini tahlil qilish quyidagi umumiy zaifliklarni aniqladi [9, 2, 10]:

1- Diagramma [9].



Estoniya elektron sud tajribasini o‘rganish shuni ko‘rsatdiki, ko‘p bosqichli autentifikatsiya va kriptografik himoya vositalarini qo‘llash kiberhujumlar xavfini 78% ga kamaytiradi [10]. ENISA (European Union Agency for Cybersecurity)ning 2023-yil hisobotida Yevropa mamlakatlarining 42% elektron sud tizimlari minimal xavfsizlik standartlariga javob bermasligini ko‘rsatadi [9].

3. Shaxsiy ma’lumotlar himoyasidagi muammolar.

1) Huquqiy jarayonlarda qatnashuvchilarning shaxsiy ma’lumotlari eng nozik kategoriyaga kiradi [11]. Tadqiqot quyidagi asosiy muammolarni aniqladi [3]:

2) Sud hujjatlarida shaxsiy ma’lumotlarni to‘liq anonimizatsiya qilmaslik (62% hollarda);

3) Ma’lumotlarga ruxsatsiz kirish holatlari (yillik150+hodisa);

4) Ma’lumotlar bazalarida ochiq kirib olish imkoniyati mavjudligi;

5) Shaxsiy ma’lumotlarni saqlash muddatlarining aniq belgilanmaganligi.

Yevropa Ittifoqining GDPR (General Data Protection Regulation) talablariga muvofiq, sud tizimlari shaxsiy ma’lumotlarni himoya qilish bo‘yicha qat’iy protokollarni joriy etgan [9]. O‘zbekiston Respublikasining “Shaxsga doir ma’lumotlar to‘g‘risida”gi Qonuni (2019) GDPR standartlariga yaqinlashgan bo‘lsa-da, amaliy tatbiq etishda qator muammolar saqlanib qolmoqda [11, 12].

4. Raqamli dalillarning huquqiy qiymati va xavfsizligi.

Raqamli dalillar zamonaviy sud jarayonlarida muhim rol o‘ynamoqda[13]. Tadqiqot quyidagi natijalarni berdi:

2- jadval. Raqamli dalillar bilan bog‘liq kiberxavfsizlik muammolari [14].

Muammo	Hollarda uchraydi (%)	Ta’sir darajasi
Dalillar zanjirining buzilishi	43%	Yuqori
Dalillarni o‘zgartirish xavfi	37%	Juda yuqori
Metadata yo‘qolishi	29%	O‘rta

Soxta dalillar yaratish	18%	Juda yuqori

Blockchain texnologiyasidan foydalanish raqamli dalillarning asl nusxaligini ta'minlashda samarali vosita ekanligi aniqlandi [14]. Dubai sud tizimi 2020-yildan boshlab barcha elektron hujjatlarni blockchain tarmog'ida saqlash orqali dalillar manipulyatsiyasini deyarli nolga tushirdi. Radziwill va Romanoning tadqiqotida blockchain texnologiyasi raqamli dalillarning integriteti va autentifikatsiyasini ta'minlashda 95% samaradorlikka erishishi tasdiqlangan [14].

5. O'zbekiston huquqiy tizimida kiberxavfsizlik holati.

O'zbekiston kiberxavsizlikni ta'minlashda quyidagi asosiy prinsiplardan foydalanadi: qonuniylik, kibermakonda shaxs, jamiyat va davlat manfaatlarini himoya qilishning ustuvorligi prinsipi, kiberxavfsizlik sohasini tartibga solishga nisbatan yagona yondashuv prinsipi, kiberxavfsizlik tizimini yaratishda mahalliy ishlab chiqaruvchilar ishtirokining ustuvorligi prinsipi, O'zbekiston Respublikasining kiberxavfsizlikni ta'minlashda xalqaro hamkorlik uchun ochiqligi prinsipi [15]. O'zbekiston huquqiy ma'lumot bazalarini himoya qilish uchun asosan ushbu prinsiplar orqali himoya qiladi, ammo, bu yetarli bo'lmaydi, chunki,bizgahali himoya qilish uchun ko'p qatlamli xavfsizlik arxitekturasi ishlab chiqilishi kerak.

IV. Muhokama

Tadqiqot natijalari shuni ko'rsatadiki, huquqiy jarayonlarda kiberxavfsizlik muammolari global xarakterga ega va kompleks yondashuvni talab etadi [8]. Bir qator muhim jihatlarni alohida muhokama qilish zarur.

Texnologik himoya va insonomili

Eng ilg'or kiberxavfsizlik tizimlari ham inson omiliga bog'liq [5]. Ekspert so'rovlari shuni ko'rsatadiki, kiberhujumlarning 82% xodimlarning xatolari yoki ehtiyotsizligi natijasida sodirbo'lmoqda [4, 5]. Phishing hujumlari, zaif parollar va social engineering usullari eng keng tarqalgan zaifliklardir. "IBM Security"ning 2024-yil hisobotida ta'kidlanishicha, xodimlarning xatolari tufayli yuzaga kelgan ma'lumotlar buzilishi hodisalari o'rtacha 4.88 million dollar zarar keltiradi [4]. Singapur sud tizimida amalga oshirilgan tajriba shuni ko'rsatadiki, xodimlarni kiberxavfsizlik bo'yicha yiliga kamida 4 marta o'qitish va simulyatsiya mashqlarini o'tkazish xavflarni 65%ga kamaytiradi [16, 10]. O'zbekiston kontekstida bunday dasturlarni joriy etish muhim ahamiyatga ega [12].

Ochiqlik va xavfslik balansi

Demokratik jamiyatlarda sud jarayonlarining oshkoraligi muhim tamoyil hisoblanadi. Biroq, elektron sud tizimlari bu tamoyilni amalga oshirish jarayonida xavfsizlik risklarini oshiradi [10]. Ochiq ma'lumotlar portallari kiberjinoyatchilarga ma'lumot to'plash va hujum rejallashtirish imkonini berishi mumkin [17]. Kanada sud tizimi bu muammoni hal qilishda muvozanatli yondashuvni qo'llaydi: sud hujjatlarini ommaviy qilishdan oldin maxsus dasturiy ta'minot orqali barcha shaxsiy va maxfiy ma'lumotlar avtomatik ravishda Anonimizatsiya qilinadi[10].Ushbu usul samaradorligi 91%ni tashkil etadi.Zhang va boshqalarning qiyosiy tahlilida turli mamlakatlarning elektron sud tizimlari oshkoralik va xavfsizlik muvozanatini qanday ta'minlashi ko'rsatilgan [10].

Milliy xavfsizlik va xalqaro hamkorlik

Kiberxavfsizlik tahdidlari transmilliy xarakterga ega [8]. Ko'plab kiberhujumlar chegaradan tashqaridan amalga oshiriladi, bu esa milliy huquq-tartibot organlarining samaradorligini cheklaydi.Interpol va Europol tajribasi shuni ko'rsatadiki, xalqaro hamkorlik kiberjinoyatchilarni qo'lga olish ehtimolini 4 baravar oshiradi. UNODCning 2023-yil kiberjinoyatchilik bo'yicha keng qamrovli tadqiqotida transmilliy kiberjinoyatchilikka qarshi kurashishda xalqaro hamkorlikning zaruriyati ta'kidlangan [8].

O'zbekiston Respublikasi uchun ShHT mamlakatlari, Yevropa Ittifoqi va boshqa xalqaro

tashkilotlar bilan kiberxavfsizlik sohasida hamkorlikni kengaytirish strategik ahamiyatga ega [12]. Turaev va Nurmatovning tadqiqotida O‘zbekistonning axborot xavfsizligi sohasidagi xalqaro hamkorligi kengaytirilishi zaruriyati asoslangan [12].

Sun’iy intellekt: yangi imkoniyatlar va tahdidlar

Sun’iy intellekt (AI) texnologiyalari huquqiy jarayonlarda ikki yo‘nalishda qo‘llanilmoqda: kiberxavfsizlikni kuchaytirish va kiberhujumlar uchun [1, 16]. AI-ga asoslangan monitoring tizimlari anomal harakatlarni deyarli real vaqt rejimida aniqlay oladi [18]. Biroq, kiberjinoyatchilar ham AI dan foydalanib, murakkab va moslashuvchan zararli dasturlarni yaratmoqda [6, 16].

Xitoy sud tizimida joriy etilgan AI-monitoring tizimlari kiberhujumlarni 87% hollarda boshlang‘ich bosqichida to‘xtatishga imkon berdi [16]. Biroq, bunday tizimlarni joriy etish yuqori investitsiyalarni talab qiladi. Singh va Kumarning tadqiqotida sun’iy intellekt va kiberxavfsizlik o‘rtasidagi bog‘liqlik chuqur tahlil qilingan va sud tizimlarida AI dan foydalanishning afzalliklari va xavflari ko‘rsatilgan [16].

Qonunchilikdagi bo‘shliqlar

Ko‘pchilik mamlakatlar, shu jumladan O‘zbekiston qonunchiligi kiberxavfsizlik sohasidagi texnologik taraqqiyotdan orqada qolmoqda [17, 12]. Raqamli dalillarning qonuniy qiymati, kiberhujumlar uchun javobgarlik, transsarhad kiberjinoyatlar kabi masalalar qonunchilik darajasida aniq tartibga solinmaganligi muammolar keltirib chiqarmoqda [13]. Karimovning tadqiqotida O‘zbekiston qonunchiligida kiberjinoyatchilik va unga qarshi kurashish mexanizmlari tahlil qilingan [17].

Estoniya tajribasi shuni ko‘rsatadiki, texnologiya-neytral qonunchilik yondashuvi (technology-neutral legislation) qonunlarni tez-tez o‘zgartirish zaruratini kamaytiradi va texnologik o‘zgarishlarga moslashishni osonlashtiradi [10]. NIST Framework for Improving Critical Infrastructure Cybersecurity ham qonunchilikni ishlab chiqishda texnologiya-neytral yondashuvni qo‘llashni tavsiya etadi [18].

V. Xulosa

Maqola asosida biz quyidagi xulosalarga kelishimiz mumkin:

Birinchidan, zamonaviy axborot jamiyatining eng dolzarb muammolaridan biri sifatida huquqiy jarayonlarda kiberxavfsizlik masalalarini aytishimiz mumkin. Raqamlashtirish jarayonlari huquqiy tizim uchun samarali bo‘lsa ham, bir qator yangi xavf-xatalarni keltirib chiqarmoqda.

Ikkinchidan, kiberxavfsizlikni ta’minlash kompleks yondashuv talab etadi, ya’ni texnologik, tashkiliy, qonunchilik va ta’lim choralarining birgalikdagi tatbiqi zarur. Faqat texnik himoya choralari yetarli emas, insonomili muhimrol o‘ynaydi. NIST Framework bu yondashuvni institutional darajada amalga oshirish uchun aniq ko‘rsatmalar beradi.

Uchinchidan, xalqaro tajriba shuni ko‘rsatadiki, ko‘p bosqichli himoya strategiyasi (defense in depth) eng samarali yondashuv hisoblanadi. Bu autentifikatsiya, shifrlash, monitoring, backup va tiklash tizimlarini o‘z ichiga oladi. Blockchain texnologiyasi raqamli dalillarning integriteti va shaffofligini ta’minlashda muhim rol o‘ynaydi.

To‘rtinchidan, O‘zbekiston Respublikasida huquqiy jarayonlarda kiberxavfsizlikni ta’minlash uchun quyidagi chora-tadbirlar zarur:

1) Milliy kiberxavfsizlik standartlarini ishlab chiqish va joriy etish;
2) Huquqiy institutlar xodimlari uchun majburiy kiberxavfsizlik ta’limi dasturlarini amalga oshirish;
3) Zamonaviy kiberxavfsizlik tizimlariga investitsiyalarni oshirish;
4) Elektron sud tizimlari uchun xavfsizlik sertifikatlash tartibini joriy etish;
5) Kiberxavfsizlik bo‘yicha maxsus mutaxassislar tayyorlash;
6) Xalqaro hamkorlikni kengaytirish.

Beshinchidan, qonunchilik bazasini takomillashtirish muhim yo‘nalish hisoblanadi. Raqamli

dalillar, elektron hujjatlar, transsarhad kiberjinoyatlar va sun'iy intellekt qo'llanilishi kabi masalalarni qonunchilik darajasida aniq tartibga solish zarur. O'zbekiston Respublikasining "Shaxsga doir ma'lumotlar to'g'risida"gi Qonuni (2019) va "Kiberxavfsizlik to'g'risida"go Qonuni xalqaro standartlarga muvofiq yanada takomillashtirilishi lozim.

Oltinchidan, ochiqlik va xavfsizlik o'rtasida muvozanatni saqlash muhim.Sud jarayonlarining shaffofligi demokratik tamoyil bo'lib qolishi kerak, lekin bu shaxsiy ma'lumotlar va milliy xavfsizlik uchun xavf tug'dirmasligi lozim.

Xulosa qilib aytganda, huquqiy jarayonlarda kiberxavfsizlikni ta'minlash uzluksiz jarayon bo'lib, davlat, huquqiy institutlar, texnologiya kompaniyalari va jamiyatning har bir a'zosining birgalikdagi sa'y-harakatlarini talab etadi. Texnologiyalarning jadal rivojlanishi munosabati bilan kiberxavfsizlik choralari ham doimiy yangilanib turishi zarur. "IBM Security"ning ma'lumotlariga ko'ra, kiberxavfsizlikga sarflangan har bir dollar 5 dollarga teng zararning oldini olishga yordam beradi.

Foydalanilgan adabiyotlar/Литературы/References:

1. Mirzaev, O.B., Abdullaev, J.K., & Tursunova, N.M. (2023). Legal tech va huquqiy xizmatlar innovatsiyasi. Toshkent: Sharq. – 208 bet.
2. Ismoilov, B.I., & Rahimov, S.T. (2022). Elektron sud tizimi: imkoniyatlar va muammolar. Toshkent: Adolat nashriyoti. – 156 bet.
3. Abulkasimov, H.P. (2021). Huquq-tartibot organlarida axborot xavfsizligi masalalari. Huquq va jamiyat jurnali, 3(45), 78-84.
4. IBM Security. (2024). Cost of a Data Breach Report 2024. Armonk, NY: IBM Corporation.
5. Verizon. (2024). 2024 Data Breach Investigations Report. Basking Ridge, NJ: Verizon Communications.
6. Cybersecurity Ventures. (2024). 2024 Official Cybercrime Report. Retrieved from https://cybersecurityventures.com
7. "Elektron hukumat to'g'risida"gi Qonuni O'RQ-395-сон 09.12.2015.Elektronhukumat to'g'risida
8. United Nations Office on Drugs and Crime (UNODC). (2023). Comprehensive Study on Cybercrime. Vienna: United Nations.
9. European Union Agency for Cybersecurity(ENISA). (2023). Threat Landscape for the Legal Sector. Luxembourg: Publications Office of the European Union.
10. Zhang, L., Wang, Y., & Chen, X. (2023). Cybersecuritychallenges in e-court systems: A comparative analysis of international practices. Computer Law & Security Review, 48, 105784. https://doi.org/10.1016/j.clsr.2022.105784
11. "Shaxsgadoirma'lumotlarto'g'risida"giQonuniO'RQ-547-сон02.07.2019. Shaxsga doir ma'lumotlar to'g'risida
12. Turaev, Sh.K., & Nurmatov, F.A. (2023). O'zbekiston Respublikasida axborot xavfsizligini ta'minlash: huquqiy asoslar va amaliyot. Toshkent: TDYU. – 234 bet.
13. Yuldashev, A.U. (2022). Raqamli dalillar va ularning sud jarayonidagi qonuniy qiymati. Huquq va jamiyat jurnali, 4(58), 92-98.
14. Radziwill, N., & Romano, J. (2023). Blockchain for cybersecurity in legal systems: A systematic review. Journal of Cybersecurity and Privacy, 3(2), 245-267. https://doi.org/10.3390/jcp3020015
15. "Kiberxavfsizlik to'g'risida"gi Qonuni O'RQ-764-сон 15.04.2022.Kiberxavfsizlikto'g'risida
16. Singh, R., & Kumar, A. (2023). Artificial Intelligence and cybersecurity in judicial systems: Opportunities and challenges. International Journal of Law and Technology, 31(1), 89-112. https://doi.org/10.1093/ijlit/eab023
17. Karimov, A.N. (2023). Kiberjinoyatchilik va unga qarshi kurashish: nazariya va amaliyot. Toshkent