O‘ZBEKISTON RESPUBLIKASI QONUNCHILIK PALATASIGA QONUNCHILIK TASHABBUSI TARTIBIDA KIRITILADIGAN TUSHUNTIRISH XATI, ILMIY-EMPIRIK NORMATIV HUJJAT LOYIHASI VA TAQQOSLAMA JADVAL

Ortiqboyev Asadbek Po‘lat o‘g‘li
Jahon Iqtisodiyoti va Diplomatiya Universiteti,
Xalqaro huquq fakulteti talabasi,
Xakimxo‘jayeva Sevdo Kamol qizi
Toshkent davlat yuridik universiteti,
Ommaviy huquq fakulteti talabasi

Annotatsiya. Ushbu ilmiy-amaliy va normativ-huquqiy tadqiqot O‘zbekiston Respublikasining kiberxavfsizlik hamda shaxsga doir ma’lumotlar daxlsizligi sohasidagi qonunchiligini kompleks takomillashtirishga qaratilgan qonunchilik tashabbusi loyihasidir. Ishda JIDU va TDYU tadqiqotchilari tomonidan o‘tkazilgan empirik so‘rovnoma ($N=300$) va ekspert intervyulari ($N=40$) natijalari asosida amaldagi Jinoyat kodeksi, Ma’muriy javobgarlik to‘g‘risidagi kodeks va sohaviy qonunlardagi huquqiy bo‘shliqlar tahlil qilingan. EU GDPR, Budapest Convention va ISO/IEC standartlari asosida kiber-firibgarlik, ijtimoiy muhandislik, dropperlik faoliyati hamda DDoS hujumlarini kriminallashtirish, 24/72 soatlik Data Breach Notification, Unutish huquqi, aylanmadan 1-3% miqdoridagi jarimalar va Bug Bounty (White Hat) kafolatlarini joriy etuvchi to‘liq qonun loyihasi tahriri va taqqoslama jadval taqdim etilgan.

Kalit so‘zlar: qonunchilik tashabbusi, kiberxavfsizlik, shaxsga doir ma’lumotlar, ijtimoiy muhandislik, dropperlik, GDPR, Data Breach, aylanma jarimasi, Bug Bounty, taqqoslama jadval.

Аннотация. Данное исследование представляет собой проект законодательной инициативы, направленный на комплексное совершенствование законодательства Республики Узбекистан в сфере кибербезопасности и защиты персональных данных. На основе эмпирического исследования ($N=300$) и экспертных интервью ($N=40$) выявлены системные пробелы в УК, КоАО и законах “О персональных данных” и “О кибербезопасности”. На базе GDPR, Будапештской конвенции и ISO/IEC разработаны проект закона, криминализирующий социальную инженерию, дропперство и DDoS-атаки, а также вводящий обязательные уведомления об утечках (24/72 часа), “Право на забвение”, оборотные штрафы (1-3%) и правовые гарантии для Bug Bounty.

Ключевые слова: законодательная инициатива, кибербезопасность, персональные данные, социальная инженерия, дропперство, GDPR, утечка данных, оборотный штраф, Bug Bounty, сравнительная таблица.

Abstract. This paper constitutes a comprehensive legislative initiative draft aimed at reforming the cybersecurity and personal data protection framework of the Republic of Uzbekistan. Based on empirical survey data ($N=300$) and 40 expert interviews, the authors identify critical gaps in the Criminal Code, Administrative Code, and primary legislation. Grounded in EU GDPR, the Budapest Convention, and ISO/IEC standards, the work delivers a complete legislative draft criminalizing social engineering, dropper networks, and DDoS attacks on critical infrastructure, while introducing mandatory 24/72h Data Breach notifications, the Right to be Forgotten, 1-3% turnover-based fines, and Bug Bounty legal protections.

Keywords: legislative initiative, cybersecurity, personal data, social engineering, dropper networks, GDPR, data breach, turnover fine, Bug Bounty, comparative table.

KIRISH VA QONUNCHILIK TASHABBUSI FAKTIK ASOSLARI

Raqamlashtirish sur'atlarining keskin jadallashuvi sharoitida O'zbekiston Respublikasi Konstitutsiyasining 27, 31 va 33-moddalarida kafolatlangan shaxsiy va oilaviy sir, shaxsga doir ma'lumotlar daxlsizligi hamda axborot xavfsizligi huquqlarini ta'minlash milliy xavfsizlik va davlat suverenitetining ustuvor shartiga aylandi. Qonunchilik tashabbusi mualliflari — Ortiqboyev Asadbek Po'lat o'g'li (JIDU) hamda Xakimxo'jayeva Sevdo Kamol qizi (TDYU) tomonidan o'tkazilgan kompleks ilmiy-empirik va kriminologik tadqiqot ($N=300$ so'rovnoma respondentlari va $N=40$ ekspert intervyulari) amaldagi qonunchilik kompleksi zamonaviy kiber-tahdidlar darajasidan sezilarli darajada ortda qolayotganini ko'rsatdi:

Latent kiberjinoyatchilik va jabrlanish: Respondentlarning **31%** bevosita kiberjinoyatlar (bank kartalaridan pul o'g'irlanishi, ijtimoiy tarmoq akkauntlarining egallanishi va h.k.) qurboni bo'lgan.

Ijtimoiy muhandislik va OTP zaifligi: Aholining **85%** psixologik tazyik va manipulyatsiyalar natijasida bir martalik SMS-tasdiqlash kodlarini (OTP) firibgarlarga taqdim etgan. Amaldagi JK 168-moddasi va 278-moddalarida "Ijtimoiy muhandislik" va "Drapperlik" (dropper networks) tushunchalari hamda ularning javobgarlik tarkibi umuman mavjud emas.

Raqamli ishonch inqirozi va Data Breach: Respondentlarning **47%** davlat va xususiy platformalarda shaxsiy ma'lumotlar daxlsizligiga umuman ishonmaydi. Amaldagi O'RQ-547-sonli Qonunda ma'lumotlar sizib chiqqanda (Data Breach) regulyator va fuqaroni majburiy xabardor qilish mexanizmi yo'q, MJTK 46-2-moddasidagi 50-100 BHM jarima esa yirik banklar va korporatsiyalar uchun profilaktik kuchga ega emas.

2.METODOLOGIYA (RESEARCH METHODOLOGY)

Tadqiqotda kompleks aralash metodologik yondashuv (Mixed Methods Research) qo'llanilgan:

Miqdoriy (Quantitative) metod: Google Forms platformasi orqali $N = 300$ respondent o‘rtasida anonim empirik so‘rovnoma o‘tkazildi.

Sifat (Qualitative) metod: Kiberxavfsizlik mutaxassislari va huquqni muhofaza qiluvchi organ xodimlari bilan $N = 40$ chuqurlashtirilgan intervyu o‘tkazildi.

Mantiqiy-huquqiy metodlar:

Induksiya: Xususiy empirik holatlardan mamlakat darajasidagi kiber-zaiflik va huquqiy bo‘shliqlar haqida ilmiy xulosalar chiqarildi.

Deduksiya: EU GDPR (Articles 17, 33, 34, 83), Budapest Convention va ISO/IEC 27001/27701 xalqaro standartlari milliy huquqiy tizimga implementatsiya qilindi.

Sintez va Taqqoslama tahlil: Amaldagi qonun moddalari nuqta-verguligacha so‘zma-so‘z taqqoslanib, yangi normativ tahrir va Taqqoslama jadval ko‘rinishiga keltirildi.

3. MUHOKAMA VA QONUNCHILIK TASHABBUSI ASOSLARI (DISCUSSION)

Jinoyat kodeksi 8-bob, 278^1 va 278^3-moddalar: "Deepfake" va "Drapperlik faoliyati" legal ta’riflanib, kiber-firibgarlik hamda drapperlik guruhlari uchun 5 yildan 8 yilgacha, Critical Infrastructure (MAIO) ob’ektlariga DDoS hujumlari uchun 8 yildan 12 yilgacha ozodlikdan mahrum qilish sanksiyalari kiritilmoqda. **O‘RQ-547 Qonun 24, 31^1, 31^2-moddalar:** Ma’lumotlar sizib chiqqanda (Data Breach) operator tomonidan **24 soat** ichida Regulyatorga va **72 soat** ichida fuqarolarga xabar berish majburiyati, fuqaroning **"Unutish huquqi" (Right to be forgotten)** hamda majburiy kiber-sug‘urta joriy etilmoqda. **MJTK 46^2-modda:** Yirik operatorlar uchun har qanday ma’lumotlar sizib chiqishi holatida kompaniyaning o‘tgan yildagi **yillik oborotining 1% dan 3% gacha miqdorida (Turnover-based fine)** differentsiallashtirilgan jarima belgilanmoqda. **O‘RQ-764 Qonun 28-1-modda:** Zaifliklarni aniqlab, 72 soat ichida mas’uliyatli

oshkor qilgan (Responsible Disclosure) "White Hat" (etik xakerlar) va Bug Bounty ishtirokchilari jinoiy va ma’muriy javobgarlikdan ozod qilinadi.

4. QONUN LOYIHASI TAHRIRI — FULL LEGISLATIVE TEXT O‘ZBEKISTON RESPUBLIKASINING QONUNI

O‘zbekiston Respublikasining ayrim qonun hujjatlariga kiberxavfsizlik va shaxsga doir ma’lumotlar daxlsizligini ta’minlash mexanizmlarini takomillashtirish bo‘yicha o‘zgartish va qo‘shimchalar kiritish to‘g‘risida

1-modda. O‘zbekiston Respublikasining Jinoyat kodeksiga kiber-firibgarlikning zamonaviy shakllarini huquqiy jihatdan aniqlashtirishga qaratilgan o‘zgartish va qo‘shimchalar kiritilsin.

1-modda. O‘zbekiston Respublikasining Jinoyat kodeksiga kiber-firibgarlikning zamonaviy shakllarini huquqiy jihatdan aniqlashtirishga qaratilgan o‘zgartish va qo‘shimchalar kiritilsin.

Jinoyat kodeksining firibgarlikka oid qoidalarida axborot-kommunikatsiya texnologiyalaridan, ijtimoiy muhandislik usullaridan, soxta raqamli identifikatsiya vositalaridan, shu jumladan sun’iy ravishda yaratilgan yoki o‘zgartirilgan audio-vizual kontentdan foydalanib o‘zganing mol-mulki yoki unga bo‘lgan huquqni qo‘lga kiritish alohida og‘irlashtiruvchi holat sifatida nazarda tutilsin.

Bunda mazkur harakatlarni kvalifikatsiya qilishda:

- jabrlanuvchini psixologik manipulyatsiya qilish;
- bir martalik tasdiqlash kodlari (OTP) yoki autentifikatsiya ma’lumotlarini qo‘lga kiritish;
- boshqa shaxs yoki tashkilot nomidan soxta raqamli identifikatsiyadan foydalanish;
- deepfake texnologiyalaridan foydalanish;
- elektron to‘lov vositalari yoki elektron hamyonlardan foydalanish

kabi usullar hisobga olinsin.

2-modda. ***Jinoyat kodeksining asosiy tushunchalariga quyidagi atamalar kiritilsin:***

Ijtimoiy muhandislik — shaxsni psixologik manipulyatsiya qilish, chalg‘itish yoki uning ishonchidan foydalanish orqali axborot tizimlariga noqonuniy kirish, autentifikatsiya ma’lumotlari, bir martalik tasdiqlash kodlari, shaxsga doir ma’lumotlar yoki moliyaviy aktivlarni olishga undashga qaratilgan usullar majmui.

Deepfake — sun’iy intellekt, mashinaviy o‘rganish yoki boshqa raqamli texnologiyalar yordamida shaxsning tasviri, ovozi, harakati yoki boshqa identifikatsiya qiluvchi belgilarini sun’iy ravishda yaratish yoki o‘zgartirish orqali hosil qilingan sintetik raqamli kontent.

Dropperlik faoliyati — jinoiy faoliyat natijasida olingan pul mablag‘lari, kripto-aktivlar yoki boshqa mol-mulkni yashirish, o‘tkazish yoki naqdlashtirish maqsadida o‘ziga tegishli bank hisobvarag‘i, to‘lov vositasi, elektron hamyon yoki boshqa moliyaviy rekvizitlardan boshqa shaxslarning foydalanishiga qasddan va noqonuniy ravishda imkon berish.

3-modda. ***O‘zbekiston Respublikasining 2019-yil 2-iyuldagi O‘RQ-547-son “Shaxsga doir ma’lumotlar to‘g‘risida”gi Qonuniga quyidagi mazmundagi norma kiritilsin:***

“Shaxsga doir ma’lumotlar xavfsizligi buzilishi haqida xabar berish” Mulkdor va (yoki) operator shaxsga doir ma’lumotlarning yo‘qolishi, noqonuniy oshkor etilishi, tarqalishi, o‘zgartirilishi yoki ularga ruxsatsiz kirish bilan bog‘liq xavfsizlik buzilishini aniqlagan taqdirda, bu haqda vakolatli davlat organini hodisa aniqlangan paytdan e’tiboran 24 soatdan kechiktirmay xabardor qilishi shart. Agar mazkur xavfsizlik buzilishi shaxslarning huquq va qonuniy manfaatlariga jiddiy xavf tug‘dirsa, mulkdor va (yoki) operator tegishli shaxsga doir ma’lumotlar subyektlarini ham xabardor qilishi shart.

Xabarnomada xavfsizlik buzilishining xususiyati, ta’sir ko‘rsatgan ma’lumotlar toifalari, ehtimoliy oqibatlar hamda buzilish oqibatlarini bartaraf etish va kamaytirish bo‘yicha ko‘rilayotgan choralar to‘g‘risidagi ma’lumotlar ko‘rsatiladi.

4-modda. ***O‘RQ-547-son Qonun quyidagi mazmundagi norma bilan to‘ldirilsin:***

“Shaxsga doir ma’lumotlarni o‘chirishni talab qilish huquqi” Shaxsga doir ma’lumotlar subyekti ma’lumotlar dastlab yig‘ilgan yoki qayta ishlangan maqsadlar uchun zarur bo‘lmay qolgan, noqonuniy ravishda qayta ishlangan yoki ularni saqlash uchun qonuniy asos mavjud bo‘lmagan hollarda mulkdor va (yoki) operatordan o‘ziga tegishli shaxsga doir ma’lumotlarni o‘chirishni yoki yo‘q qilishni talab qilish huquqiga ega. Mazkur huquq qonunchilikda belgilangan majburiyatlarni bajarish, sudlovni amalga oshirish, jamoat manfaatlarini ta’minlash yoki qonuniy da’volarni amalga oshirish va himoya qilish uchun ma’lumotlarni saqlash zarur bo‘lgan hollarda cheklanishi mumkin.

5-modda. *Yirik hajmdagi shaxsga doir ma’lumotlarni qayta ishlovchi mulkdor va (yoki) operatorlar uchun kiberxavflarni boshqarish bo‘yicha qo‘shimcha talablar belgilanadi.*

Bunday subyektlar:

- kiberxavflarni muntazam baholashi;
- shaxsga doir ma’lumotlarni himoya qilish choralarini hujjatlashtirishi;
- xavfsizlik buzilishlarini aniqlash va ularga javob berish mexanizmlarini joriy etishi;
- zarur hollarda kiberxavflardan sug‘urtalanish choralarini ko‘rishi shart.

Majburiy kiber-sug‘urta qo‘llaniladigan subyektlar, sug‘urta summasi va boshqa talablar alohida qonunchilik hujjatlari bilan belgilanadi.

6-modda. ***O‘zbekiston Respublikasining 2022-yil 15-apreldagi O‘RQ-764-son “Kiberxavfsizlik to‘g‘risida”gi Qonuniga zaifliklarni mas’uliyatli oshkor qilish mexanizmini nazarda tutuvchi norma kiritilsin:***

“Zaifliklarni mas’uliyatli aniqlash va xabar berish”

Axborot tizimlari yoki dasturiy ta’minotdagi zaifliklarni qonuniy va mas’uliyatli ravishda aniqlagan shaxs, agar u:

- tizimga ruxsatsiz kirishni kengaytirmagan;
- aniqlangan ma’lumotlardan shaxsiy yoki boshqa noqonuniy manfaatlar uchun foydalanmagan;
- tizim faoliyatiga qasddan zarar yetkazmagan;
- aniqlangan zaiflik to‘g‘risida tizim egasiga yoki vakolatli davlat organiga belgilangan muddatda xabar bergan

bo‘lsa, uning harakatlari tegishli qonuniy shartlar mavjud bo‘lgan taqdirda jinoyat yoki ma’muriy huquqbuzarlik sifatida baholanmasligi mumkin.

Zaifliklarni aniqlash va xabar berish tartibi, xabardor qilish muddati hamda bug bounty dasturlarini tashkil etish talablari vakolatli davlat organi tomonidan belgilanadi.

7-modda. *Muhim axborot infratuzilmasi obyektlariga qarshi kiberhujumlar uchun javobgarlikni belgilashda hujumning oqibati, yetkazilgan zarar, xizmatlarning to‘xtatilishi, hujumning takroriyligi va boshqa og‘irlashtiruvchi holatlar hisobga olinsin.*

Muhim axborot infratuzilmasi obyektlariga nisbatan DDoS-hujumlarni qasddan tashkil etish, axborotni noqonuniy yo‘q qilish, bloklash, o‘zgartirish yoki tizim faoliyatini izdan chiqarish uchun javobgarlik tegishli jinoyat tarkiblarida og‘irlashtiruvchi holat sifatida belgilansin.

8-modda. *O‘zbekiston Respublikasining Ma’muriy javobgarlik to‘g‘risidagi kodeksida shaxsga doir ma’lumotlar to‘g‘risidagi qonunchilikni buzish uchun javobgarlik choralarini ma’lumotlar hajmi, huquqbuzarlikning takroriyligi, yetkazilgan zarar va subyektning maqomini hisobga olgan holda tabaqalashtirish nazarda tutilsin.*

Yirik ma’lumot operatorlari tomonidan qonunchilik talablarini muntazam yoki qo‘pol ravishda buzish uchun yuridik shaxslarning iqtisodiy javobgarligi mexanizmlari qonunchilikda belgilangan tartibda kuchaytirilishi mumkin.

9-modda. *O‘zbekiston Respublikasi Vazirlar Mahkamasi va vakolatli davlat organlari ushbu Qonundan kelib chiqadigan qonunchilik hujjatlarini uch oy muddatda ushbu Qonunga muvofiqlashtirsin.*

10-modda. *Ushbu Qonun rasmiy e’lon qilingan kundan e’tiboran uch oy o‘tgach kuchga kiradi.*

5. TAKLIF ETILAYOTGAN YANGI TAHRIR VA QO‘SHIMCHALARNING ASOSLANISHI

5.1. Jinoyat qonunchiligini takomillashtirish

Amaldagi holat: O‘zbekiston Respublikasi Jinoyat kodeksida firibgarlik uchun javobgarlik nazarda tutilgan bo‘lib, axborot tizimlari va axborot texnologiyalaridan foydalanish bilan bog‘liq holatlar ham mavjud. Shu bilan birga, ijtimoiy muhandislik, deepfake va boshqa zamonaviy texnologiyalardan foydalanib sodir etiladigan firibgarlik shakllarini huquqiy kvalifikatsiya qilishda qo‘shimcha aniqlik zarur. Jinoyat kodeksining $278^1–278^9$-moddalari esa allaqachon kompyuter va telekommunikatsiya sohasidagi turli jinoyat tarkiblarini qamrab oladi.
Taklif: Jinoyat kodeksida ijtimoiy muhandislik, deepfake va dropperlik bilan bog‘liq usullarni mavjud jinoyat tarkiblari doirasida aniq kvalifikatsiya qilish hamda zarur hollarda og‘irlashtiruvchi holat sifatida belgilash.

Xalqaro asos: *Budapest Convention on Cybercrime* kompyuter tizimlari va ma'lumotlariga qarshi noqonuniy xatti-harakatlarni kriminalizatsiya qilish uchun xalqaro huquqiy asos yaratadi.

5.2. Ijtimoiy muhandislik va deepfake tushunchalarini huquqiy aniqlashtirish

Amaldagi holat: Amaldagi shaxsga doir ma'lumotlar va kiberxavfsizlik qonunchiligida "ijtimoiy muhandislik" va "deepfake" tushunchalari mustaqil huquqiy ta'rif sifatida yetarlicha aniqlashtirilmagan. **Taklif:** Mazkur tushunchalarni qonunchilikka kiritish orqali huquqni qo'llash organlariga yangi texnologik usullardan foydalanilgan huquqbuzarliklarni bir xil mezonlar asosida kvalifikatsiya qilish imkoniyatini yaratish.

5.3. Shaxsga doir ma'lumotlar xavfsizligi buzilishi haqida xabar berish

Amaldagi holat: O'RQ-547-sonli Qonunning 24-moddasi avtomatlashtirilgan tarzda ishlov berishga bag'ishlangan. Qonunning 27-moddasi shaxsga doir ma'lumotlarni himoya qilish kafolatlarini, 28-moddasi esa ularning maxfiyligini belgilaydi.

Taklif: Shaxsga doir ma'lumotlar xavfsizligi buzilishi aniqlangan hollarda vakolatli organga tezkor xabar berishning alohida huquqiy mexanizmini joriy etish. Tadqiqot doirasida taklif etilayotgan modelda vakolatli organga 24 soat ichida xabar berish, yuqori xavf mavjud bo'lgan hollarda esa ma'lumotlar subyektlarini ham xabardor qilish nazarda tutiladi.

Xalqaro asos: *GDPR*ning 33-moddasi shaxsiy ma'lumotlar buzilishi haqida nazorat organini xabardor qilish, 34-moddasi esa ayrim hollarda ma'lumotlar subyektlarini xabardor qilish mexanizmini belgilaydi.

5.4. "Unutish huquqi"ni joriy etish

Amaldagi holat: O'RQ-547-sonli Qonunda shaxsga doir ma'lumotlar subyektining huquqlari va ma'lumotlarni yo'q qilish bilan bog'liq qoidalar mavjud

bo‘lsa-da, GDPRdagi “right to erasure” modeliga o‘xshash, ma’lumotni o‘chirishni talab qilishning yaxlit mexanizmini yanada aniq shakllantirish mumkin. **Taklif:** Ma’lumotlar dastlabki maqsad uchun zarur bo‘lmay qolgan yoki ularni saqlashning qonuniy asosi mavjud bo‘lmagan hollarda subyektga ma’lumotlarini o‘chirishni talab qilish huquqini berish.

Xalqaro asos: *GDPR*ning 17-moddasi “right to erasure” mexanizmini nazarda tutadi.

5.5. Yirik operatorlarning kiberxavflarini boshqarish

Amaldagi holat: Katta hajmdagi shaxsga doir ma’lumotlarni qayta ishlovchi tashkilotlarda yuzaga keladigan kiberxavfsizlik hodisalari ko‘proq shaxslarning huquq va manfaatlariga ta’sir qilishi mumkin. **Taklif:** Yirik operatorlar uchun risklarni baholash, xavfsizlik choralarini hujjatlashtirish, hodisalarga javob berish rejalarini ishlab chiqish va tegishli hollarda kiber-sug‘urta mexanizmlaridan foydalanish talablarini bosqichma-bosqich joriy etish.

Xalqaro asos: *ISO/IEC 27001* axborot xavfsizligini boshqarish tizimlariga, *ISO/IEC 27701* esa privacy information management tizimlariga oid xalqaro standartlarni belgilaydi.

5.6. White Hat va Responsible Disclosure

Amaldagi holat: O‘RQ-764-sonli “Kiberxavfsizlik to‘g‘risida”gi Qonunning 22-moddasi kiberxavfsizlik hodisalarini tekshirishni, 23-moddasi esa hodisalarga javob berish va zaifliklarni bartaraf etish choralarini nazarda tutadi. **Taklif:** Zaifliklarni qonuniy aniqlaydigan xavfsizlik tadqiqotchilari uchun Responsible Disclosure mexanizmini joriy etish. Bunda javobgarlikdan himoya faqat oldindan belgilangan shartlarga rioya qilingan hollarda qo‘llanadi. **Xalqaro asos:** *ISO/IEC 29147* zaifliklarni aniqlash va oshkor qilish jarayonlarini tashkil etish bo‘yicha xalqaro yondashuvni belgilaydi.

5.7. Muhim axborot infratuzilmasini himoya qilish

Amaldagi holat: O‘RQ-764-sonli Qonun kiberxavfsizlik hodisalarini tekshirish va ularga javob berishning huquqiy mexanizmlarini belgilagan.

Taklif: Muhim axborot infratuzilmasi obyektlariga qarshi DDoS va boshqa jiddiy kiberhujumlarni baholashda hujum oqibatlari, xizmatlarning uzilishi, zarar miqdori, takroriylik va boshqa og‘irlashtiruvchi holatlarni hisobga oladigan tabaqalashtirilgan javobgarlik tizimini yaratish.

5.8. Takliflarning umumiy huquqiy ahamiyati

Taklif etilayotgan o‘zgartishlar O‘zbekistonning mavjud kiberxavfsizlik va shaxsga doir ma’lumotlarni himoya qilish tizimini uchta asosiy yo‘nalishda rivojlantirishga qaratilgan:

kiberjinoyatlarning yangi shakllarini huquqiy aniqlashtirish;

shaxsga doir ma’lumotlar buzilganda ma’lumotlar subyektlarining huquqlarini kuchaytirish;

kiberxavfsizlikning profilaktik va mas’uliyatli disclosure mexanizmlarini rivojlantirish.

Shu tariqa, qonun loyihasi faqat jinoyat sodir etilgandan keyingi jazolash mexanizmiga emas, balki kiberxavflarni oldindan aniqlash, ma’lumotlar buzilishiga tezkor javob berish, shaxs huquqlarini himoya qilish va qonuniy kiberxavfsizlik tadqiqotlarini rag‘batlantirishga yo‘naltirilgan kompleks yondashuvni taklif etadi.

6. FOYDALANILGAN ADABIYOTLAR RO‘YXATI (BIBLIOGRAFIYA)

1. European Union. (2016). *Regulation (EU) 2016/679 of the European Parliament and of the Council (General Data Protection Regulation - GDPR)*. Official Journal of the European Union, L 119.

URL: https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679

2.Council of Europe. (2001). *Convention on Cybercrime (Budapest Convention)*, ETS No. 185.

URL: https://www.coe.int/en/web/cybercrime/the-budapest-convention

3.European Parliament and Council of the European Union. (2022). *Directive (EU) 2022/2555 on measures for a high common level of cybersecurity across the Union (NIS2 Directive)*. Official Journal of the European Union.

URL: https://eur-lex.europa.eu/eli/dir/2022/2555/oj

4.ISO/IEC. (2022). *ISO/IEC 27001:2022 — Information security, cybersecurity and privacy protection — Information security management systems*. Geneva: International Organization for Standardization.

5.ISO/IEC. (2019). *ISO/IEC 27701:2019 — Security techniques — Extension to ISO/IEC 27001 and ISO/IEC 27002 for privacy information management*. Geneva: International Organization for Standardization.

6.ISO/IEC. (2018). *ISO/IEC 29147:2018 — Information technology — Security techniques — Vulnerability disclosure*. Geneva: International Organization for Standardization.

7.O‘zbekiston Respublikasi. (1994). *O‘zbekiston Respublikasining Jinoyat kodeksi*. LexUZ. URL: https://lex.uz/docs/-111453

8.O‘zbekiston Respublikasi. (1994). *O‘zbekiston Respublikasining Ma’muriy javobgarlik to‘g‘risidagi kodeksi*. LexUZ.

URL: https://lex.uz/docs/-97664

9.O‘zbekiston Respublikasi. (2019). *“Shaxsga doir ma’lumotlar to‘g‘risida”gi Qonun*, O‘RQ-547-son. LexUZ.

URL: https://lex.uz/docs/-4396419

10.O‘zbekiston Respublikasi. (2022). *“Kiberxavfsizlik to‘g‘risida”gi Qonun*, O‘RQ-764-son. LexUZ.

URL: https://lex.uz/docs/-5957900

11.O‘zbekiston Respublikasi. (2023). *O‘zbekiston Respublikasi Konstitutsiyasi*. Toshkent: “O‘zbekiston” NMIU.