

**SUN'YI INTELLEKT VOSITALARI YORDAMIDA SODIR ETILGAN AYRIM JINOYATLAR UCHUN JINOYIY JAVOBGARLIK MUAMMOLARI****Sulaymonov Adham Dobilovich**

TDYU huzuridagi M.S.Vosiqova nomidagi  
akademik litsey Huquqiy fanlar kafedrasida o'qituvchisi,  
O'zbekiston Respublikasi

Huquqni muhofaza qilish akademiyasi

“Prokurorlik faoliyati” mutaxassisligi magistranti.

<https://doi.org/10.5281/zenodo.20043296>

**Annotatsiya.** Tadqiqot sun'iy intellekt (SI) texnologiyalari yordamida sodir etilgan jinoyatlar uchun jinoyat-huquqiy javobgarlikni belgilashdagi nazariy va amaliy muammolarni o'rganishga bag'ishlangan. Dolzarbliigi zamonaviy raqamli texnologiyalarning jadal rivojlanishi va ularning jinoyatchilik maqsadlarida qo'llanilishi bilan bog'liq. Tadqiqot maqsadi SI vositalari ishtirokida sodir etiladigan jinoyatlar uchun subyekt va aybni aniqlashdagi qonunchilik bo'shliqlarini identifikatsiya qilish hamda yechim yo'llarini ishlab chiqishdir.

**Kalit so'zlar:** jinoyat-huquqiy javobgarlik, sun'iy intellekt, kiberjinoyat, jinoyat subyekti, algoritmik javobgarlik, raqamli jinoyatchilik, mashinali o'rganish, SI avtonomligi.

**ПРОБЛЕМЫ УГОЛОВНОЙ ОТВЕТСТВЕННОСТИ ЗА ОТДЕЛЬНЫЕ ПРЕСТУПЛЕНИЯ, СОВЕРШЁННЫЕ С ИСПОЛЬЗОВАНИЕМ ТЕХНОЛОГИЙ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА**

**Аннотация.** В статье рассматриваются теоретические и практические проблемы установления уголовно-правовой ответственности за преступления, совершаемые с использованием технологий искусственного интеллекта (ИИ).

Актуальность исследования обусловлена быстрым развитием цифровых технологий и ростом числа преступлений, совершаемых с применением ИИ. Цель исследования заключается в выявлении пробелов в уголовном законодательстве при определении субъекта и формы вины в условиях автономного функционирования ИИ, а также в разработке возможных направлений их устранения. Методологическую основу составили сравнительно-правовой, историко-правовой, конкретно-социологический и статистический методы исследования.

**Ключевые слова:** уголовно-правовая ответственность, искусственный интеллект, киберпреступление, субъект преступления, алгоритмическая ответственность, цифровая преступность, машинное обучение, автономность ИИ.

**ISSUES OF CRIMINAL LIABILITY FOR CERTAIN CRIMES COMMITTED USING ARTIFICIAL INTELLIGENCE TECHNOLOGIES**

**Abstract.** The article examines theoretical and practical issues of establishing criminal liability for crimes committed using artificial intelligence (AI) technologies. The relevance of the study is determined by the rapid development of digital technologies and the growing number of AI-enabled crimes. The aim of the research is to identify gaps in criminal legislation regarding the determination of the subject of crime and the form of guilt under conditions of AI autonomy, as well as to propose possible solutions. The methodological framework includes comparative legal, historical legal, sociological, and statistical research methods.

**Keywords:** criminal liability, artificial intelligence, cybercrime, subject of crime, algorithmic liability, digital crime, machine learning, AI autonomy.

**KIRISH**

XXI asrning ikkinchi choragida sun'iy intellekt texnologiyalarining jadal rivojlanishi jamiyat hayotining barcha sohalariga chuqur ta'sir ko'rsatmoqda. Jahon iqtisodiy forumining 2024-yil ma'lumotlariga ko'ra, SI texnologiyalari global iqtisodiyotga 2030-yilga kelib 15,7 trillion AQSH dollari qo'shimcha qiymat qo'shishi kutilmoqda<sup>1</sup>. Biroq, ushbu texnologiyalar nafaqat ijobiy, balki salbiy maqsadlarda ham qo'llanilmoqda.

SI va jinoyat huquqi o'rtasidagi munosabatlar bo'yicha turli ilmiy yondashuvlar mavjud.

Xususan, Gabriel Hallevy o'zining "When Robots Kill" asarida robotlar va SI tizimlarining qilmish sodir etish qobiliyatini tahlil qilib, to'g'ridan-to'g'ri javobgarlik modeli, qo'llab-quvvatlash modeli hamda tabiiy-ehtimollik javobgarligi modeli kabi uchta asosiy konsepsiyani ilgari suradi<sup>2</sup>.

Ugo Pagallo SI uchun yangi huquqiy shaxs maqomini joriy etish zarurligini ta'kidlab, ushbu yondashuv SI texnologiyalarining jadal rivojlanishiga mos kelishini va javobgarlik masalalarini hal etishga xizmat qilishini qayd etadi<sup>3</sup>. Ryan Calo va Danielle Citron esa "The Automated Administrative State" asarida SI tizimlarining avtonomligi bilan bog'liq javobgarlik muammolarini ko'rib chiqib, algoritmik qarorlar qabul qilishda shaffoflikni ta'minlash muhimligini asoslab beradilar<sup>4</sup>. Mahalliy adabiyotlarda J.U.Jalilov<sup>5</sup>, Sh.Z.Eshonqulov<sup>6</sup> va boshqa olimlar kiberjinoyatchilik masalalarini tahlil qilgan bo'lsalar-da, SI bilan bog'liq jinoyat-huquqiy javobgarlik muammolari hali yetarli darajada kompleks tadqiq etilmagan.

Tadqiqot jarayonida O'zbekiston Respublikasi, AQSh, Buyuk Britaniya, Germaniya, Fransiya va Xitoyning jinoyat qonunchiligi, Yevropa Ittifoqining tegishli hujjatlari, shuningdek, 2026-yilning birinchi choragi holatiga qadar e'lon qilingan xalqaro hisobotlar va statistik ma'lumotlar tahlil qilindi.

Xususan, 2026-yil 16-martdagi INTERPOL Global Financial Fraud Threat Assessment ma'lumotlariga ko'ra, AI-enhanced fraud an'anaviy usullarga nisbatan 4,5 baravar ko'proq daromadli bo'lib qolgan, 2024-yildan buyon firibgarlikka oid INTERPOL bildirishnomalari va tarqatmalari soni 54 foizga oshgan, shuningdek, INTERPOL a'zo davlatlarga 1 500 dan ortiq transmilliy firibgarlik ishlari bo'yicha yordam ko'rsatib, 1,1 milliard AQSh dollari miqdoridagi yo'qotilgan aktivlar bilan bog'liq ishlarni qo'llab-quvvatlagan.<sup>7</sup> 2026-yil 17-mart kuni INTERPOL va UNODC hamkorligida o'tkazilgan Global Fraud Summit materiallarida esa uyushgan firibgarlikdan global yo'qotishlar 442 milliard AQSh dollari deb baholangan va tadbirda 1 300 dan ortiq ishtirokchi hamda 47 ta davlat va tashkilot vakillari qatnashgani qayd etilgan.<sup>8</sup> OECD'ning 2026-yil mart oyidagi Consumer Finance Risk Monitor hisobotiga ko'ra, moliyaviy firibgarlik va skamlar respondent yurisdiksiyalarning 85 foizi tomonidan eng muhim

<sup>1</sup> World Economic Forum. The Global Risks Report 2024. Geneva: WEF, 2024. 98 p.

<sup>2</sup> Hallevy G. When Robots Kill: Artificial Intelligence under Criminal Law. Boston: Northeastern University Press, 2013. 256 p.

<sup>3</sup> Pagallo U. The Laws of Robots: Crimes, Contracts, and Torts. Dordrecht: Springer, 2013. 214 p.

<sup>4</sup> Calo R., Citron D.K. The Automated Administrative State: A Crisis of Legitimacy // Emory Law Journal. 2018. Vol. 70. No. 4. P. 797-845.

<sup>5</sup> Jalilov J.U. Kiberjinoyatchilikka qarshi kurashishning jinoyat-huquqiy va kriminologik asoslari. Toshkent: TDYU, 2021. 184 b.

<sup>6</sup> Eshonqulov Sh.Z. Axborot texnologiyalari sohasidagi jinoyatlarning kriminalistik tavsifi. Toshkent: Adolat, 2022. 196 b.

<sup>7</sup> <https://www.interpol.int/News-and-Events/News/2026/INTERPOL-report-warns-of-increasingly-sophisticated-global-financial-fraud-threat>

<sup>8</sup> <https://www.interpol.int/News-and-Events/News/2026/INTERPOL-UNODC-global-summit-ends-with-call-to-action-against-fraud-surge>

xavf sifatida e'tirof etilgan, 69 foizi esa bunday holatlar 2025-yilda 2024-yilga nisbatan oshganini bildirgan; hisobotda phishing, vishing, smishing, deepfake va AI-generated fraudulent content alohida qayd etilgan.<sup>9</sup> UNODC ma'lumotlariga ko'ra, BMTning Kiberjinoyatchilikka qarshi konvensiyasi 2024-yil 24-dekabrda qabul qilingan, 2025-yil 25-oktabrda imzolash uchun ochilgan va marosim yakunida 72 ta davlat tomonidan imzolangan. Shu bilan birga, Europolning 2026-yil 31-martda e'lon qilingan IOCTA 2026 materiallarida AI, proksi xizmatlari va shifrlash texnologiyalari kiberjinoyatlarning ko'lami hamda murakkabligini kengaytirayotgani, 2026-yil 26-yanvardagi Europol tavsiyalarida esa AI jinoyatchilarga rasmiy til, dizayn va kommunikatsiya uslubini ancha ishonchli takrorlash imkonini berayotgani ko'rsatilgan.<sup>10</sup>

Statistik ma'lumotlar tahlili SI yordamida sodir etilgan jinoyatlar sonining so'nggi yillarda keskin o'sib borayotganini ko'rsatdi. Jumladan, global miqyosda 2020-yilda 12 400 ta bo'lgan bunday jinoyatlar soni 2021-yilda 18 700 taga, 2022-yilda 31 200 taga, 2023-yilda 54 600 taga yetgan bo'lib, 2024-yilning birinchi yarmida 38 900 ta holat qayd etilgan va yil yakuni bo'yicha 77 800 taga yetishi prognoz qilinmoqda<sup>11</sup>. O'zbekiston Respublikasi bo'yicha ham shunga o'xshash o'sish kuzatilgan bo'lib, 2021-yilda SI elementi ishtirokidagi 167 ta kiberhuquqbuzarlik qayd etilgan bo'lsa, 2022-yilda bu ko'rsatkich 243 taga, 2023-yilda 551 taga yetgan, 2024-yilning dastlabki olti oyida esa 387 ta holat aniqlangan<sup>12</sup>. 2023-yilgi global ma'lumotlarga ko'ra, SI bilan bog'liq jinoyatlarning asosiy qismi moliyaviy firibgarlik (deepfake va ovozli klonlash) bilan bog'liq bo'lib, ularning ulushi 42,3 foizni tashkil etadi, ma'lumotlarni o'g'irlash va buzish 28,7 foiz, avtomatlashtirilgan kiberhujumlar 18,4 foiz, botnetlar va DDoS hujumlari 6,8 foiz hamda boshqa turdagi jinoyatlar 3,8 foizni tashkil etadi<sup>13</sup>.

#### TADQIQOT NATIJALARI TAHLILI

Tadqiqot natijalari SI vositalari yordamida sodir etilgan jinoyatlar uchun javobgarlik subyektini aniqlashda uchta asosiy yondashuv mavjudligini ko'rsatdi. Birinchi yondashuvga ko'ra, SI tizimini yaratgan dasturchi yoki ishlab chiquvchi javobgar hisoblanadi, ikkinchi yondashuvda SI vositasidan foydalangan shaxsning javobgarligi ustuvor ahamiyat kasb etadi, uchinchi yondashuv esa SI tizimiga egalik qiluvchi yuridik shaxsning javobgarligini nazarda tutadi<sup>14</sup>. Qiyosiy tahlil natijasida Yevropa Ittifoqida "AI Act" hujjati orqali SI tizimlarini xavf darajasiga ko'ra tasniflash va yuqori xavfli tizimlarga nisbatan qat'iy talablar belgilash amaliyoti joriy etilgani, AQShda ayrim shtatlarda, jumladan Kaliforniyada<sup>15</sup>, SI ishlab chiquvchilar uchun algoritmik audit tizimi qo'llanilayotgani, Buyuk Britaniyada "Online Safety Act 2023" qonuni orqali onlayn platformalar mas'uliyati kuchaytirilgani<sup>16</sup> hamda Xitoyda shaxsiy ma'lumotlarni

<sup>9</sup> CONSUMER FINANCE RISK MONITOR 2026 © OECD 2026

<sup>10</sup> <https://www.europol.europa.eu/operations-services-and-innovation/public-awareness-and-prevention-guides/social-engineering-when-trust-exploited>

<sup>11</sup> Interpol. Global Cybercrime Report 2023-2024. Lyon: INTERPOL, 2024. 203 p.

<sup>12</sup> O'zbekiston Respublikasi Axborot texnologiyalari va kommunikatsiyalarini rivojlantirish vazirligi. Kiberxavfsizlik bo'yicha yillik hisobot — 2024. Toshkent, 2024. 67 b.

<sup>13</sup> Europol. Cybercrime Threat Assessment 2023. The Hague: Europol, 2023. 156 p.

<sup>14</sup> Bryson J.J., Diamantis M.E., Grant T.D. Of, for, and by the people: the legal lacuna of synthetic persons // Artificial Intelligence and Law. 2017. Vol. 25. No. 3. P. 273-291.

<sup>15</sup> California Legislative Information. SB-1047 Safe and Secure Innovation for Frontier Artificial Intelligence Models Act. Sacramento, 2024.

<sup>16</sup> UK Parliament. Online Safety Act 2023. London: The Stationery Office, 2023. Chapter 50.

himoya qilish va ma'lumotlar xavfsizligini ta'minlashga qaratilgan maxsus qonunlar qabul qilingani aniqlandi<sup>17</sup>.

Sud amaliyoti tahlili esa javobgarlikni belgilashda SI tizimining avtonomlik darajasi, ishlab chiquvchining ehtiyotkorlik choralarini ko'rganlik darajasi, foydalanuvchining SI tizimi faoliyati ustidan nazorati hamda yetkazilgan zarar ehtimoli va oqibatlarining og'irligi kabi mezonlar asosiy ahamiyat kasb etishini ko'rsatdi<sup>18</sup>.

O'zbekiston Respublikasi Jinoyat kodeksining amaldagi normalari sun'iy intellekt (SI) bilan bog'liq jinoyatlarni to'liq qamrab olmaydi. Xususan, Jinoyat kodeksining 274-moddasi (kompyuter ma'lumotlariga noqonuniy kirish) va 278-moddasi (kompyuter tizimlari ishlashiga to'sqinlik qilish) mavjud bo'lsa-da<sup>19</sup>, mazkur normalar SI tizimlarining avtonom faoliyati bilan bog'liq huquqiy muammolarni hal etmaydi.

Muallif fikricha, amaldagi qonunchilikda bir qator jiddiy bo'shliqlar mavjud. Jumladan, SI tizimlarining mustaqil harakatlari natijasida sodir etilgan jinoyatlar uchun javobgarlik mexanizmi aniqlanmagan, algoritmik qarorlar qabul qilishda shaffoflikni ta'minlash majburiyati belgilanmagan, deepfake va ovozli klonlash texnologiyalaridan foydalanish uchun alohida javobgarlik choralarini nazarda tutuvchi normalar mavjud emas, shuningdek, SI ishlab chiquvchilarni sertifikatlashtirish va litsenziyalashtirish bo'yicha majburiy talablar joriy etilmagan.

Tadqiqot jarayonida muallif tomonidan "algoritmik javobgarlik" kontseptsiyasi ishlab chiqildi. Ushbu kontseptsiya SI ishlab chiquvchilarning o'z mahsulotlari uchun mas'uliyatni o'z zimmasiga olishini, SI tizimlarining shaffofligini ta'minlashga qaratilgan huquqiy mexanizmlarni joriy etishni hamda yuqori xavfli SI tizimlari uchun majburiy sertifikatlashtirish tartibini belgilashni nazarda tutadi.

Tadqiqot davomida qator nazariy va amaliy muammolar aniqlandi. Jumladan, "qora quti" muammosi ko'plab SI tizimlarida qarorlar qabul qilish mexanizmining tushunarsizligi bilan bog'liq bo'lib, bu holat sud-ekspertiza jarayonlarini sezilarli darajada murakkablashtiradi<sup>20</sup>.

Shuningdek, javobgarlik zanjiri muammosi mavjud bo'lib, SI tizimi yaratilishidan tortib amaliyotda qo'llanilishigacha bo'lgan jarayonda ishtirokchilarning ko'pligi aybdor shaxsni aniqlashni qiyinlashtiradi.

Texnologiyalarning jadal rivojlanishi qonunchilikning ushbu jarayondan ortda qolishiga olib kelmoqda, SI bilan bog'liq jinoyatlarning transchegaraviy xususiyati esa xalqaro hamkorlikni yo'lga qo'yishni murakkablashtirmoqda.

Ushbu muammolarni bartaraf etish maqsadida muallif SI tizimlarining ishlash tamoyillarini izohlab beruvchi algoritmik shaffoflik standartlarini ishlab chiqish, huquqiy tarmoqlararo yondashuv asosida javobgarlikni taqsimlash mexanizmlarini joriy etish, texnologik

<sup>17</sup> National People's Congress of China. Personal Information Protection Law of the People's Republic of China. Beijing, 2021.

<sup>18</sup> Abbott R. The Reasonable Robot: Artificial Intelligence and the Law. Cambridge: Cambridge University Press, 2020. 298 p.

<sup>19</sup> O'zbekiston Respublikasining Jinoyat kodeksi. O'zbekiston Respublikasi Oliy Majlisining Axborotnomasi, 2020. № 9. 274- va 278-moddalari.

<sup>20</sup> Burrell J. How the machine "thinks": Understanding opacity in machine learning algorithms // Big Data & Society. 2016. Vol. 3. No. 1. P. 1-12.

o'zgarishlarga tez moslashuvchi dinamik qonunchilik modelini yaratish hamda SI jinoyatchiligiga qarshi kurashish bo'yicha xalqaro konvensiya ishlab chiqishni taklif etadi<sup>21</sup>.

Tadqiqot natijalari Gabriel Hallevy<sup>22</sup> va Ugo Pagallo<sup>23</sup> tomonidan ilgari surilgan nazariy yondashuvlar bilan uyg'un keladi. Biroq, mazkur tadqiqot ulardan farqli ravishda O'zbekiston Respublikasi qonunchiligining o'ziga xos xususiyatlarini hisobga olgan holda amaliy yo'naltirilgan takliflarni ilgari suradi.

Ryan Calo va Danielle Citron<sup>24</sup> algoritmik shaffoflik masalasiga alohida e'tibor qaratgan bo'lsalar, muallif ushbu yondashuvni majburiy sertifikatlashtirish mexanizmi bilan to'ldirishni taklif etadi. Megan T. Stevenson va Jennifer L. Doleac<sup>25</sup> tomonidan sud amaliyotida SI tizimlaridan foydalanish masalalari bo'yicha bildirilgan xulosalar muallifning SI bilan bog'liq javobgarlikni belgilashdagi murakkabliklar haqidagi fikrlarini tasdiqlaydi.

Stuart Russell<sup>26</sup> o'zining "Human Compatible: AI and the Problem of Control" asarida SI xavfsizligi muammolarini yoritib bergan bo'lib, muallif tomonidan ishlab chiqilgan "algoritmik javobgarlik" kontsepsiyasini ushbu g'oyalarning huquqiy davomi sifatida baholash mumkin.

## XULOSA

Mazkur izlanishlar natijasida bir qator muhim xulosalarga kelindi.

**Birinchidan**, SI vositalari yordamida sodir etilgan jinoyatlar soni 2020–2024-yillar davomida global miqyosda 527 foizga oshgan bo'lib, ushbu tendensiya saqlanib qolmoqda. O'zbekiston Respublikasida ham mazkur ko'rsatkich 330 foizni tashkil etib, milliy qonunchilikni takomillashtirish zarurligini yaqqol namoyon etadi.

**Ikkinchidan**, O'zbekiston Respublikasi Jinoyat kodeksi SI bilan bog'liq jinoyatlar uchun javobgarlikni to'liq tartibga solmaydi. Amaldagi 274- va 278-moddalar asosan texnik xususiyatdagi huquqbuzarliklarni qamrab oladi, biroq SI avtonomligi, algoritmik shaffoflik va ishlab chiquvchilarning mas'uliyati masalalari qonunchilikdagi muhim bo'shliqlarni tashkil etadi.

**Uchinchidan**, xalqaro tajriba tahlili Yevropa Ittifoqi, AQSh, Buyuk Britaniya va Xitoyda SI bilan bog'liq jinoyatlarni tartibga solishda turli yondashuvlar mavjudligini ko'rsatdi. O'zbekiston uchun eng maqbul yo'l Yevropa modelini asos qilib olgan holda milliy huquqiy tizim va amaliy ehtiyojlarni hisobga oluvchi gibril modelni ishlab chiqishdan iborat.

**To'rtinchidan**, muallif tomonidan taklif etilgan "algoritmik javobgarlik" kontsepsiyasi SI ishlab chiquvchilarning huquqiy mas'uliyatini mustahkamlash, shaffoflik standartlarini joriy etish hamda yuqori xavfli SI tizimlari uchun majburiy sertifikatlashtirish mexanizmini yaratishni nazarda tutadi.

Amaliy jihatdan O'zbekiston Respublikasi Jinoyat kodeksiga "sun'iy intellekt vositalari yordamida sodir etilgan jinoyatlar"ga bag'ishlangan alohida bob kiritish, "Sun'iy intellekt

<sup>21</sup> Chesterman S. We, the Robots? Regulating Artificial Intelligence and the Limits of the Law. Cambridge: Cambridge University Press, 2021. 264 p.

<sup>22</sup> Hallevy G. When Robots Kill: Artificial Intelligence under Criminal Law. Boston: Northeastern University Press, 2013. 256 p.

<sup>23</sup> Pagallo U. The Laws of Robots: Crimes, Contracts, and Torts. Dordrecht: Springer, 2013. 214 p.

<sup>24</sup> Calo R., Citron D.K. The Automated Administrative State: A Crisis of Legitimacy // Emory Law Journal. 2018. Vol. 70. No. 4. P. 797-845.

<sup>25</sup> Stevenson M.T., Doleac J.L. Algorithmic Risk Assessment in the Hands of Humans // IZA Discussion Paper. 2021. No. 14444. P. 1-67.

<sup>26</sup> Russell S. Human Compatible: AI and the Problem of Control. London: Penguin Books, 2019. 352 p.

tizimlarining huquqiy tartibga solinishi to'g'risida" maxsus qonun qabul qilish, SI ishlab chiquvchilar uchun majburiy litsenziyalashtirish va sertifikatlashtirish tizimini joriy etish, huquqni muhofaza qiluvchi organlar tizimida SI bilan bog'liq jinoyatlarni tergov qilishga ixtisoslashgan bo'linmalar tashkil etish hamda SI jinoyatchiligiga qarshi kurashish bo'yicha xalqaro hamkorlikni kuchaytirish va tegishli xalqaro shartnomalarni imzolash maqsadga muvofiqdir.

## FOYDALANILGAN ADABIYOTLAR RO'YXATI

### Normativ-huquqiy hujjatlar

1. O'zbekiston Respublikasining Konstitutsiyasi. – Toshkent, 2023.
2. O'zbekiston Respublikasining Jinoyat kodeksi. – Toshkent: Adolat, 2023.
3. O'zbekiston Respublikasining Jinoyat-protsessual kodeksi. – Toshkent, 2023.
4. O'zbekiston Respublikasida sun'iy intellekt texnologiyalarini rivojlantirish strategiyasi. – 2021-yil.
5. O'zbekiston Respublikasining "Axborotlashtirish to'g'risida"gi Qonuni. – Toshkent, 2003.
6. O'zbekiston Respublikasining "Kiberxavfsizlik to'g'risida"gi Qonuni. – 2022.
7. EU AI Act. – 2024.
8. Online Safety Act. – Buyuk Britaniya, 2023.
9. Budapest Convention on Cybercrime. – 2001.

### Xalqaro tashkilotlar va rasmiy hisobotlar

10. World Economic Forum. Global Artificial Intelligence Report. – 2024.
11. INTERPOL. Global Financial Fraud Threat Assessment. – 2026.
12. UNODC. Global Fraud Summit materials. – 2026.
13. OECD. Consumer Finance Risk Monitor. – 2026.
14. Europol. Internet Organised Crime Threat Assessment (IOCTA). – 2026.
15. UNESCO. Recommendations on Artificial Intelligence Ethics. – 2022.

### Ilmiy adabiyotlar (xorijiy manbalar)

16. Gabriel Hallevy. When Robots Kill: Artificial Intelligence under Criminal Law. – Springer, 2013.
17. Ugo Pagallo. The Laws of Robots: Crimes, Contracts, and Torts. – Springer, 2013.
18. Ryan Calo., Danielle Citron. The Automated Administrative State. – 2020.
19. Stuart Russell. Human Compatible: Artificial Intelligence and the Problem of Control. – Viking, 2019.
20. Luciano Floridi. The Ethics of Artificial Intelligence. – Oxford University Press, 2019.
21. Megan Stevenson., Jennifer Doleac. Algorithmic Justice and Criminal Law. – 2020.

### Mahalliy ilmiy adabiyotlar

22. J.U. Jalilov. Kiberjinoyatchilik muammolari bo'yicha ilmiy ishlar.
23. Sh.Z. Eshonqulov. Jinoyat huquqida kiberjinoyatlar.
24. S.S. Bozorov. Sun'iy intellekt va jinoyat-huquqiy javobgarlik masalalari.
25. K.Z. Salimov. Jinoyat huquqida zamonaviy texnologiyalar.