

KIBERJINOYATLAR TERGOVIDA SHAXSGA DOIR MA'LUMOTLARNI MUHOFAZA QILISHDA XORIJ TAJRIBASI

Ergashova Ma'mura Amangeldi qizi

Annotatsiya. Mazkur maqolada xorijiy mamlakatlar qonunchiligida kiberjinoyatlarni tergov qilish jarayonida shaxsga doir ma'lumotlarni muhofaza qilish masalalari tahlil qilingan. AQSH, Germaniya va Yaponiya misolida tergov organlari faoliyatida ma'lumotlarning maxfiyligini ta'minlash, sud ruxsatisiz ma'lumot yig'ishni cheklash va inson huquqlarini kafolatlash tamoyillari o'rganilgan. Shuningdek, xalqaro tajriba asosida O'zbekiston qonunchiligi uchun dolzarb xulosalar va takliflar ishlab chiqilgan.

Kalit so'zlar: kiberjinoyat, shaxsga doir ma'lumotlar, maxfiylik, tergov, inson huquqlari, xalqaro tajriba, GDPR, APPI.

Аннотация. В данной статье анализируются вопросы защиты персональных данных при расследовании киберпреступлений в законодательстве зарубежных стран. На примере США, Германии и Японии исследуются принципы обеспечения конфиденциальности данных в деятельности следственных органов, ограничения сбора информации без судебного разрешения и обеспечения прав человека. Также разработаны соответствующие выводы и предложения по законодательству Узбекистана, основанные на международном опыте.

Ключевые слова: киберпреступность, персональные данные, конфиденциальность, расследование, права человека, международный опыт, GDPR, APPI.

Abstract. This article analyzes the issues of personal data protection in the process of investigating cybercrimes in the legislation of foreign countries. Using the examples of the USA, Germany and Japan, the principles of ensuring the confidentiality of data in the activities of investigative bodies, limiting the collection of information without judicial permission, and guaranteeing human rights are studied. Also, relevant conclusions and proposals for the legislation of Uzbekistan based on international experience are developed.

Keywords: cybercrime, personal data, confidentiality, investigation, human rights, international experience, GDPR, APPI.



Kirish

Raqamli texnologiyalar taraqqiyoti va internet tarmog'ining kengayishi natijasida kiberjinoyatlar zamonaviy jamiyat uchun eng jiddiy xavf-xatarlardan biriga aylandi. Bunday jinoyatlar jismoniy va yuridik shaxslar manfaatlariga zarar yetkazibgina qolmay, davlatlarning milliy xavfsizligi, iqtisodiy barqarorligi va axborot suverenitetiga ham tahdid soladi. Shu bois, xorijiy mamlakatlarda kiberjinoyatlarni tergov qilish va ularning oldini olish masalalari alohida qonuniy mexanizmlar orqali tartibga solinadi. Shu bilan birga, tergov jarayonida fuqarolarning shaxsga doir ma'lumotlari, raqamli izlari va onlayn faoliyati monitoring qilinishi inson huquqlarining muhim tarkibiy qismi — shaxsiy hayot daxlsizligi tamoyiliga zid bo'lmasligi lozim. Mazkur maqolada AQSH, Germaniya va Yaponiya qonunchiligi misolida ushbu muvozanat qanday ta'minlanayotgani tahlil qilinadi.

Asosiy qism

1. AQSH qonunchiligida kiberjinoyatlarni tergov qilish va shaxsga doir ma'lumotlarni himoya qilish

AQSHda kiberjinoyatlarni tergov qilishda shaxsga doir ma'lumotlarni himoya qilish federal va shtat darajasidagi bir qator qonunlar orqali amalga oshiriladi. Ushbu qonunlar tergov jarayonida ma'lumotlarning maxfiyligini, xavfsizligini va ulardan qonuniy foydalanishni ta'minlashga qaratilgan. Eng asosiylari quyidagilardir: Elektron aloqalar maxfiyligi to'g'risidagi qonun (ECPA, 1986) [1], Kompyuter firibgarligi va noqonuniy foydalanish to'g'risidagi qonun (CFAA, 1986) [2], Tibbiy ma'lumotlarni himoya qilish to'g'risidagi qonun (HIPAA, 1996) [3], Federal savdo komissiyasi (FTC) [4] faoliyati hamda Patriot Act (2001) [5] va FISA kabi qonunlar. Shuningdek, har bir shtatda o'ziga xos maxfiylikni himoya qilish qonunlari mavjud. Masalan, Kaliforniya iste'molchilar maxfiyligi qonuni (CCPA) [6] shaxsga doir ma'lumotlar dan foydalanishni qattiq tartibga soladi.

AQSH qonunchiligida shaxsga doir ma'lumotlarni kiberjinoyatlarni tergov qilish jarayonida himoya qilish tizimlashtirilgan bo'lib, federal va shtat qonunlari hamda sud nazorati orqali amalga oshiriladi. Ushbu tartiblar tergov manfaatlarini va shaxsiy maxfiylik huquqlari o'rtasida muvozanatni saqlashga qaratilgan. AQSH tajribasi shuni ko'rsatadiki, kiberjinoyatlarni tergov qilishda davlat xavfsizligi va shaxsiy hayot daxlsizligi o'rtasida qonuniy muvozanat sud ruxsati va nazorat mexanizmlari orqali ta'minlanadi.

2. Germaniya qonunchiligida shaxsga doir ma'lumotlarni himoya qilish tizimi

Germaniyada kiberjinoyatlarni tergov qilish jarayonida shaxsga doir ma'lumotlarni muhofaza qilish qat'iy huquqiy tartiblarga asoslanadi. Ushbu tizim Yevropa Ittifoqining Umumiy ma'lumotlarni himoya qilish nizomi (GDPR, 2018) [7] va Federal ma'lumotlarni himoya qilish qonuni (BDSG, 2018) [8] asosida shakllangan. Bu tizimda shaxsiy hayotni himoya qilish ustuvor ahamiyatga ega bo'lib, har qanday tergov faoliyati inson huquqlariga zid bo'lmazligi kerak. Germaniya qonunchiligida kiberjinoyatlarni tergov qilishda shaxsga doir ma'lumotlarni himoya qilish juda qat'iy tartibga solingan. GDPR va BDSG shaxsga doir ma'lumotlarning noqonuniy yig'ilishi va ishlatilishini cheklaydi. Tergov jarayonida faqat sud ruxsati bilan shaxsga doir ma'lumotlar olinishi mumkin. Telekommunikatsiya ma'lumotlariga faqat og'ir jinoyatlar bo'yicha ruxsat beriladi.

3. Yaponiya qonunchiligida kiberjinoyatlar va shaxsiy ma'lumotlarni himoya qilish

Yaponiyada kiberjinoyatlarni tergov qilish Shaxsga doir ma'lumotlarni himoya qilish to'g'risidagi qonun (APPI, 2003, 2017-yil tahriri) [9], Telekommunikatsiya to'g'risidagi qonun (1984) [10] hamda Jinoyat kodeksi va boshqa kiberjinoyatga qarshi qonunlar asosida tartibga solinadi. Yaponiya tajribasida kiberjinoyatlarni tergov qilishda inson huquqlarini ta'minlash hamda xalqaro hamkorlik mexanizmlarini kuchaytirish muhim o'rin tutadi. APPI va telekommunikatsiya qonunlari shaxsga doir ma'lumotlar ning noqonuniy ishlatilishini cheklaydi. Tergovchilar shaxsga doir ma'lumotlarga faqat sud ruxsati bilan kirishlari mumkin. Elektron kuzatuv va monitoring qat'iy nazorat ostida olib boriladi.

Xulosa va takliflar

Kiberjinoyatlar bilan kurashish va ularni tergov qilish jarayoni zamonaviy huquqiy tizimlar oldida murakkab vazifalarni qo'yimoqda. Xususan, tergov organlari jinoyatlarni aniqlash va oldini olish uchun shaxsga doir ma'lumotlardan foydalanishga ehtiyoj sezadi, biroq bu jarayon inson huquqlari, ayniqsa, shaxsiy hayot daxlsizligi prinsipiga zid kelmasligi lozim. Shu sababli, xorijiy mamlakatlar qonunchiligida ushbu ikki muhim jihat – jamoat xavfsizligi va shaxsga doir ma'lumotlarni himoya qilish o'rtasidagi muvozanatni ta'minlashga alohida e'tibor qaratilmoqda.

Xalqaro tajribadan ko'rinib turibdiki, kiberjinoyatlarni tergov qilishda shaxsga doir ma'lumotlarni muhofaza qilish bo'yicha turli huquqiy mexanizmlar joriy etilgan. Ayrim davlatlar maxsus qonunlar orqali shaxsga doir ma'lumotlarni himoya qilish choralarini kuchaytirgan bo'lsa, boshqalari xalqaro tashkilotlar bilan hamkorlikda



kiberjinoatlarga qarshi kurash strategiyalarini ishlab chiqmoqda. Shunday qilib, kiberjinoatlarni tergov qilish jarayonida shaxsga doir ma'lumotlarni muhofaza qilishga oid xalqaro tajribani o'rganish va uni milliy qonunchilikka moslashtirish dolzarb vazifalardan biri hisoblanadi. Kelajakda texnologik taraqqiyot va huquqiy normalar uyg'unligini ta'minlash, inson huquqlarini poymol qilmagan holda kiberjinoatlarga qarshi samarali kurashish yo'nalishida izchil islohotlar amalga oshirilishi zarur.

Xalqaro tajriba tahlili shuni ko'rsatadiki, kiberjinoatlarni tergov qilishda shaxsga doir ma'lumotlarni himoya qilish har bir demokratik davlatda inson huquqlari tizimining ajralmas qismi hisoblanadi. O'zbekiston uchun quyidagi xulosalar muhim ahamiyatga ega: 1) tergov organlari faoliyatida shaffoflikni oshirish; 2) shaxsga doir ma'lumotlarni himoya qilish qonunchiligini takomillashtirish; 3) sud nazoratini kuchaytirish; 4) xalqaro hamkorlikni kengaytirish. Xorijiy tajriba O'zbekiston uchun kiberjinoatlar bilan kurashishda inson huquqlari va milliy xavfsizlik o'rtasidagi muvozanatni saqlashga qaratilgan huquqiy tizimni yanada rivojlantirish zarurligini ko'rsatadi.

Foydalanilgan adabiyotlar ro'yxati :

1. H.R.4952 - Electronic Communications Privacy Act of 1986 <https://www.congress.gov/bill/99th-congress/house-bill/4952>;
2. H.R.4718 - Computer Fraud and Abuse Act of 1986 <https://www.congress.gov/bill/99th-congress/house-bill/4718>;
3. H.R.3103 - Health Insurance Portability and Accountability Act of 1996 <https://www.congress.gov/bill/104th-congress/house-bill/3103/text>;
4. <https://www.ftc.gov/business-guidance/privacy-security/data-security>'
5. <https://www.congress.gov/bill/107th-congress/house-bill/3162>;
6. <https://oag.ca.gov/privacy/ccpa>;
7. General Data Protection Regulation (GDPR), 2018 (EU) <https://gdpr.info.eu/>;
8. Bundesdatenschutzgesetz (BDSG), 2018 (Germany) <https://dsgvo-gesetz.de/bdsg/>;
9. Act on the Protection of Personal Information (APPI), 2003, revised 2017 (Japan). ¹ <https://www.japaneselawtranslation.go.jp/en/laws/view/3648/en>;
10. Telecommunications Business Act, 1984 (Japan). <https://www.japaneselawtranslation.go.jp/en/laws/view/4241/en>;
11. O'zbekiston Respublikasining "Shaxsga doir ma'lumotlar to'g'risida"gi Qonuni, 2019-yil 2-iyul;
12. O'zbekiston Respublikasi Jinoyat-protsessual kodeksi.