ISSN: 2181-9416
4-SON, 2026

YURIST AXBOROTNOMASI

ВЕСТНИК ЮРИСТА * LAWYER HERALD

HUQUQIY, IJTIMOIY, ILMIY-AMALIY JURNAL

iD g doi crossref CYBERLENINKA НАУЧНАЯ ЭЛЕКТРОННАЯ БИБЛИОТЕКА eLIBRARY.RU

ISSN 2181-9416
DOI JURNAL: 10.34920/2181-9416/2026/4

YURIST AXBOROTNOMASI

4-SON

ВЕСТНИК ЮРИСТА

НОМЕР 4

LAWYER HERALD

ISSUE 4

Toshkent — 2026

JUMANAZAROVA Marjona Botir qizi
Toshkent davlat yuridik universiteti
Jinoiy odil sudlov fakulteti
Tadqiqot markazi katta ilmiy xodimi,
yuridik fanlar bo‘yicha falsafa doktori (PhD)
E-mail: botirqizi@gmail.com

KIBERJINOYATCHILIKKA QARSHI KURASHISH BO‘YICHA XALQARO-HUQUQIY HUJJATLAR VA XORIJIY DAVLATLAR TAJRIBASI

Iqtibos keltirish uchun (для цитирования, for citation): JUMANAZAROVA M.B. Kiberjinoyatchilikka qarshi kurashish bo‘yicha xalqaro-huquqiy hujjatlar va xorijiy davlatlar tajribasi // Yurist axborotnomasi – Вестник юриста – Lawyer herald. № 4 (2026) B. 109-116.

4 (2026) DOI https://doi.org/10.34920/2181-9416/2026/4-012

ANNOTATSIYA

Ushbu maqolada kiberjinoyatchilikka qarshi kurashishning xalqaro-huquqiy asoslari va xorijiy davlatlarning ilg‘or tajribasi kompleks tahlil qilinadi. Muallif dastlab yuridik adabiyotlarda “kiberjinoyat” tushunchasiga nisbatan mavjud turlicha ilmiy yondashuvlarni tanqidiy ko‘rib chiqadi (D.N.Karpova, I.G.Chekunov, N.Shevko) va ularni umumlashtirgan holda o‘z ta’rifini taklif etadi. Maqolada Yevropa Kengashining 1989-yildagi Tavsiyalaridan tortib, 2001-yilgi Budapesht konvensiyasi, uning qo‘shimcha protokollari, hamda Birlashgan Millatlar Tashkilotining 2024-yilda qabul qilingan Kiberjinoyatchilikka qarshi Konvensiyasigacha bo‘lgan asosiy xalqaro-huquqiy hujjatlar xronologik tartibda tahlil qilinadi. Shuningdek, O‘zbekiston Respublikasining Belarus, Kipr, Tojikiston, Quvayt, Turkmaniston va Turkiya bilan tuzgan ikki tomonlama shartnomalari ham tadqiqot doirasiga kiritilgan. Maqolaning markaziy qismida Shvetsiya, Yaponiya, Germaniya, Xitoy, AQSh, Buyuk Britaniya va Estoniyaning kiberjinoyatchilikka qarshi kurashish borasidagi institutsional va normativ-huquqiy tajribasi so‘nggi statistik ma’lumotlar asosida qiyosiy tahlil qilinadi. Shuningdek, xorijiy davlatlarning rasmiy statistik manbalariga murojaat etish orqali kiberjinoyatchilikning rivojlanish tendensiyasi va ularga qarshi kurashish natijalari ilmiy tahlil etilgan. Maqola natijasida muallif kiberjinoyatlar bo‘yicha yagona milliy xabar berish tizimini joriy etish, davlat organlari, banklar va aloqa operatorlari o‘rtasida majburiy va tezkor axborot almashinuvini ta’minlash, kiberjinoyat sodir etilgan har bir hodisaga tezkor javob taqdim etish salohiyatini kuchaytirish, aholiga yo‘naltirilgan profilaktik xabardor etish choralarini tizimli yo‘lga qo‘yish kabi amaliy tavsiyalarni ishlab chiqadi va ularni asoslaydi.

Kalit so‘zlar: kiberjinoyatchilik, kompyuter jinoyatlari, xalqaro-huquqiy hamkorlik, elektron dalillar, kiberxavfsizlik, onlayn firibgarlik, fishing, kiberhodisa, axborot, iqtisodiy zarar.

ЖУМАНАЗАРОВА Маржона
Старший научный сотрудник
Исследовательского центра факультета
Уголовного правосудия Ташкентского
Государственного юридического университета,
доктор философии по юридическим наукам (PhD)
E-mail: botirqizi@gmail.com

МЕЖДУНАРОДНО-ПРАВОВЫЕ ДОКУМЕНТЫ И ОПЫТ ЗАРУБЕЖНЫХ ГОСУДАРСТВ ПО ПРОТИВОДЕЙСТВИЮ КИБЕРПРЕСТУПНОСТИ

АННОТАЦИЯ

В статье осуществлён комплексный анализ международно-правовых основ противодействия киберпреступности и передового опыта зарубежных государств в этой сфере. Автор рассматривает существующие в юридической литературе разнообразные научные подходы к понятию «киберпреступность» (Д.Н.Карпова, И.Г.Чекунов, Н.Шевко) и на их основе формулирует обобщённое авторское определение. В работе в хронологическом порядке анализируются ключевые международно-правовые документы — от Рекомендаций Совета Европы 1989 года до Будапештской конвенции о киберпреступности 2001 года, дополнительных протоколов к ней, а также принятой Генеральной Ассамблеей ООН в 2024 году Конвенции против киберпреступности. Отдельное внимание уделено двусторонним международным договорам Республики Узбекистан с Беларусью, Кипром, Таджикистаном, Кувейтом, Туркменистаном и Турцией. Центральное место в статье занимает сравнительно-правовой анализ институционального и нормативно-правового опыта Швеции, Японии, Германии, Китая, США, Великобритании и Эстонии в области противодействия киберпреступности, подкреплённый актуальными статистическими данными. Кроме того, на основе официальных статистических данных зарубежных государств осуществлён научный анализ тенденций развития киберпреступности и результатов противодействия ей. В статьи автором разработаны и обоснованы практические рекомендации, направленные на внедрение единой национальной системы сообщений о киберпреступлениях, обеспечение обязательного и оперативного обмена информацией между государственными органами, банковскими учреждениями и операторами связи, повышение эффективности оперативного реагирования на каждый случай совершения киберпреступления, а также системное осуществление профилактического информирования населения.

Ключевые слова: киберпреступность, компьютерные преступления, международно-правовое сотрудничество, электронные доказательства, кибербезопасность, онлайн-мошенничество, фишинг, кибер-инцидент, информация, экономический ущерб.

MARJONA Jumanazarova
Senior Research Fellow
Research Center of the Faculty of Criminal Justice
Tashkent State University of Law,
Doctor of Philosophy in Law (PhD)
E-mail: botirqizi@gmail.com

INTERNATIONAL LEGAL INSTRUMENTS AND FOREIGN COUNTRIES' EXPERIENCE IN COMBATING CYBERCRIME

ANNOTATION

This article provides a comprehensive analysis of the international legal framework for combating cybercrime and the advanced experience of foreign states in this field. The author first critically examines the diverse scholarly approaches to the concept of "cybercrime" found in legal literature (D.N.Karpova, I.G.Chekunov, N.Shevko) and, on this basis, proposes a generalized definition. The article chronologically analyzes key international legal instruments, ranging from the 1989 Council of Europe Recommendation to the 2001 Budapest Convention on Cybercrime and its additional protocols, as well as the United Nations Convention against Cybercrime adopted by the UN General Assembly in 2024. Particular attention is given to bilateral treaties concluded by the Republic of Uzbekistan with Belarus, Cyprus, Tajikistan, Kuwait, Turkmenistan, and Turkey. The central part of the article presents a comparative legal analysis of the institutional and regulatory experience of Sweden, Japan, Germany, China, the United States, the United Kingdom and Estonia in countering cybercrime, supported by current statistical data. Furthermore, the development trends of cybercrime and the effectiveness of measures to combat it were scientifically analyzed using official statistical data from foreign countries. Based on the findings of the study, the author formulates and substantiates practical recommendations aimed at introducing a unified national cybercrime reporting system, ensuring mandatory and timely information exchange among government agencies, banks, and telecommunications operators, enhancing the capacity for rapid response to every cybercrime incident, and systematically implementing public awareness and prevention measures.

Key words: cybercrime, computer crimes, international legal cooperation, electronic evidence, cybersecurity, online fraud, phishing, cyber incident, information, economic damage.

Zamonaviy axborot-kommunikatsiya texnologiyalarining jadal rivojlanishi bilan bir qatorda kiberjinoyatchilik ham global miqyosda tobora kengayib bormoqda. Kiberjinoyatlarning transchegaraviy xususiyati ularga qarshi kurashishni aynan bir yagona davlat doirasida emas, balki xalqaro-huquqiy hamkorlik va unifikatsiyalashgan yondashuv orqaligina samarali amalga oshirish mumkinligini koʻrsatadi. Ushbu yoʻnalishda Yevropa Kengashining Budapesht Konvensiyasidan tortib, Birlashgan Millatlar Tashkilotining 2024-yilda qabul qilingan Kiberjinoyatchilikka qarshi Konvensiyasigacha boʻlgan xalqaro-huquqiy baza shakllanib, rivojlanib bormoqda. Shu bilan birga, Shvetsiya, Yaponiya, Germaniya kabi rivojlangan davlatlarning institutsional va normativ-huquqiy tajribasini oʻrganish milliy qonunchilikni takomillashtirish uchun muhim amaliy ahamiyat kasb etadi. Aynan shu jihatdan, mazkur maqolada kiberjinoyatchilikka qarshi kurashishning xalqaro-huquqiy asoslari va xorijiy davlatlar tajribasini kompleks qiyosiy-huquqiy, statistik tahlil qilish, ularning natijalari asosida Oʻzbekiston Respublikasi uchun amaliy tavsiyalar ishlab chiqish bugungi kunda dolzarb ahamiyat kasb etmoqda.

Yuqorida qayd etilgan dolzarblikdan kelib chiqib, dastlab "kiberjinoyatchilik" tushunchasining mohiyatini qisqacha tahlil etish maqsadga muvofiqdir, zero, ushbu tushunchaning aniq va yagona ta'rifini aniqlamaslik xalqaro hamkorlik doirasida atamalarni unifikatsiya qilishda hamda milliy qonunchilikni takomillashtirishda bir qator metodologik qiyinchiliklarni keltirib chiqarishi mumkin.

Yuridik adabiyotlarda kiberjinoyatchilik tushunchasiga bir qator oʻziga xos yondashuvlar mavjud. Masalan, D.N.Karpova internetga kirish imkoniga ega boʻlgan istalgan texnik vosita orqali jinoyat

obyektiga zarar yetkazish maqsadida amalga oshiriladigan ijtimoiy xavfli qilmish ekanini ta'kidlaydi [1]. I.G.Chekunov fikricha, kiberjinoyatchilikka kengroq yondashish lozim, chunki kiberjinoyatlarni sodir etishda nafaqat kompyuterlar, balki mobil (uyali) kommunikatsion texnik qurilmalar va aloqa tizimlaridan ham foydalanish imkoniyati mavjud [2]. Bu ta'rifga yanada kengroq ma'no berishga urinib N.Shevko kiberjinoyat umumiy tushuncha ekanligi, axborot texnologiyalaridan jinoyat qonunida mavjud an'anaviy jinoyatlarni sodir etish uchun foydalanilgan hollarning barchasi uchun qo'llanilishi mumkinligi, shuning uchun ham bu kabi jinoyatlar uchun Jinoyat kodeksining turli boblarida javobgarlik belgilanganligi haqida fikr yuritgan [3]. Demak, xulosa qiladigan bo'lsak, kiberjinoyatlar deganda, shunday ijtimoiy xavfli qilmishlar tushunilishi lozimki, ular internetda qayta ishlanadigan va foydalaniladigan axborotga nisbatan kompyuter texnikasi va har qanday zamonaviy axborot texnologiyalari vositalarini qo'llangan holda sodir etilishi bilan ajralib turadi.

Xalqaro tajribada "kiberjinoyat" deganda ko'pincha eng avvalo iqtisodiy zarar yetkazuvchi xatti-harakatlar nazarda tutiladi. Boshqa bir qator jinoyatlarda bo'lgani kabi kiberjinoyatlarga e'tibor faqat ular rivojlana borgan va oldini olmaslik davlatga ulkan iqtisodiy zarar yetkazishi aniq bo'lgan davrda osha boshladi. Xalqaro darajada ushbu toifadagi jinoyatlarni tartibga solish zarurat aslida 1970-1980-yillar davomida yuzaga kelgan edi. Aynan mazkur davrda bir qator xorijiy davlatlar jinoyat kodekslarida kompyuter jinoyatlari uchun javobgarlik kiritilgan edi.

Ushbu normalarni xalqaro doirada unifikatsiya qilish zarurati dastlab Yevropa Kengashi tomonidan 1989-yil 13-sentabrda kompyuter jinoyatlarning minimal tarkibini o'zida aks ettirgan Tavsiyalar (№(89)9) ishlab chiqilgan. Ushbu tavsiyalar bilan kiberjinoyatlarning majburiy hamda fakultativ ro'yxati shakllantirilgan edi. Majburiy jinoyatlar tarkibi ro'yxati o'z ichiga quyidagilarni qamrab olgan edi:

a) kompyuter firibgarligi;
b) kompyuter soxtakorligi;
c) kompyuter axboroti va kompyuter dasturlariga zarar yetkazish;
d) kompyuter sabotaji;
e) kompyuter tarmoqlariga qonunga xilof kirish;
f) ma'lumotlarni qonunga xilof ushlab qolish;
g) himoyalangan kompyuter dasturini ruxsatsiz ko'paytirish;
m) mikrosxema topologiyasini ruxsatsiz ko'paytirish [4].

Kiberjinoyatlarga qarshi kurashning xalqaro-huquqiy poydevori avvalo xalqaro normativ-huquqiy hujjatlar bilan mustahkamlanadi.

2003-yil 10-12-dekabrda Jenevada o'tkazilgan "Axborot jamiyati bo'yicha Butunjahon sammiti" doirasida qabul qilingan deklaratsiya (WSIS Declaration of Principles and Plan of Action) axborot jamiyatini qurish jarayonida xalqaro hamkorlik, umumiy mas'uliyat va rivojlanish maqsadlari uyg'unligini ilgari suradi [5].

Yevropa Kengashi tomonidan 2001-yil 23-noyabrda qabul qilingan "Kiberjinoyatlar to'g'risida"gi Konvensiya (Budapesht konvensiyasi) kiberjinoyatlarni tergov qilish va ta'qib etishning moddiy-huquqiy hamda protsessual asoslarini qamrab oladi, kiberjinoyatlarga qarshi kurashda xalqaro hamkorlikning umumiy tamoyillarini belgilaydi, milliy darajada unifikatsiyalashgan jinoiy javobgarlik normalarini qabul qilish zaruratidan kelib chiqadi, kriminallashtirilishi lozim bo'lgan qilmishlar doirasini belgilaydi, shuningdek, ekstraditsiya dalillarni o'zaro taqdim etish va tergovda o'zaro yordam masalalarini tartibga soladi [6]. Konvensiya 2004-yilda kuchga kirgan bo'lib, uni Yevropa Kengashiga a'zo davlatlar bilan bir qatorda, a'zo bo'lmagan AQSh, Kanada, Yaponiya, Janubiy Afrika Respublikasi kabi davlatlar ham imzolagan.

Ushbu Konvensiya a'zo davlatlar uchun quyidagi 4 toifadagi kiberjinoyatlarni milliy jinoyat qonunchiligida mustahkamlash majburiyatini yuklaydi (Konvensiyaning 2-10-moddalari):

1. Kompyuter ma'lumotlari va tizimlarining maxfiyligi, yaxlitligi hamda mavjudligiga qarshi qaratilgan jinoyatlar (kompyuter ma'lumotlariga g'ayriqonuniy aralashuv (data interference), qurilmalardan g'ayriqonuniy foydalanish (misuse of devices).

2. Kompyuter vositasida sodir etiladigan jinoyatlar (kompyuter soxtakorligi (computer-related forgery), kompyuter firibgarligi (computer-related fraud).

3. Axborot kontenti (mazmuni)ga oid jinoyatlar (bolalar pornografiyasi bilan bog‘liq jinoyatlar).

4. Mualliflik huquqi va turdosh huquqlarni buzish bilan bog‘liq jinoyatlar.

Mazkur Konvensiyaga 2003-yil kompyuter tizimlari orqali sodir etiladigan irqchilik va ksenofobiya mazmunidagi qilmishlar uchun javobgarlik belgilashni nazarda tutuvchi qo‘shimcha protokol imzolandi (2006-yil kuchga kirdi). 2022-yilda Budapesht konvensiyasiga Ikkinchi qo‘shimcha protokol qabul qilingan bo‘lib, unda hamkorlikni kuchaytirish va elektron dalillarni oshkor qilishga oid normalar kiritilgan.

Global doirada kiberjinoyatchilikka qarshi kurash yo‘nalishida yangi qadam Birlashgan Millatlar Tashkilotining Kiberjinoyatchilikka qarshi Konvensiyasi BMT Bosh Assambleyasi tomonidan 2024-yil 24-dekabrda Nyu-Yorkda 79/243-rezolyutsiya bilan qabul qilinishi bilan bog‘liq [7]. Ushbu Konvensiya “AKT tizimi”, “elektron ma’lumotlar”, “trafik ma’lumotlari”, “kontent ma’lumotlari”, “xizmat ko‘rsatuvchi”, “abonent ma’lumotlari”, “shaxsga doir ma’lumotlar” kabi asosiy tushunchalarga aniq ta’rif beradi (2-modda), bir qator kiberjinoyat turlari (7-16-moddalar) uchun javobgarlikni kuchaytirish yuzasidan rahbariy ko‘rsatmalarni belgilaydi. Ushbu Konvensiya kiberjinoyatlar uchun javobgarlik belgilash bilan cheklanmay, protsessual qismda elektron dalillarni yig‘ish, olish, saqlashni ham qamrab oladigan qo‘llanish doirasini belgilaydi. Konvensiya nafaqat jinoyatlarni fosh etish, balki jabrlanuvchi va guvohlarni himoya qilish qoidalarini ham alohida normalar bilan mustahkamlaydi.

Aynan kiberjinoyatchilikka qarshi kurashda ikki tomonlama xalqaro shartnomalarning ham ahamiyatli. Masalan, O‘zbekiston Respublikasi hukumati bilan Belarus Respublikasi hukumati o‘rtasidagi “Jinoyatchilikka qarshi kurash sohasida hamkorlik to‘g‘risida”gi bitimda aynan axborot texnologiyalari, shu jumladan, kompyuter-axboroti sohasidagi jinoyatlar yuzasidan o‘zaro hamkorlik belgilangan [8]. Ushbu toifa jinoyatlarga qarshi kurashda hamkorlik masalalari O‘zbekiston Respublikasi hukumati bilan Kipr Respublikasi hukumati o‘rtasidagi “Jinoyatchilikka qarshi kurashda hamkorlik qilish to‘g‘risida”gi Bitimda ham belgilangan (2-modda) [9]. O‘zbekiston Respublikasi bilan Tojikiston Respublikasi o‘rtasida “Xavfsizlik va jinoyatchilikka qarshi kurashish sohasida hamkorlik to‘g‘risida”gi bitimda ham axborot texnologiyalaridan foydalanishga oid jinoyatlar va kiberjinoyatchilikning oldini olish va ularga qarshi kurashish, shuningdek, tomonlarning milliy manfaatlariga qarshi axborot tarqatadigan internet-saytlar faoliyatini aniqlash va taqiqlash yo‘nalishida hamkorlik aloqalari o‘rnatilgan [10]. Shuningdek, bu kabi bitimlar yana bir qator davlatlar (Quvayt [11], Turkmaniston [12], Turkiya [13] v.b.) bilan ham tuzilganligi aynan mazkur jinoyatlarga qarshi kurashish yuzasidan mamlakatimiz tomonidan jiddiy choralar ko‘rilayotganidan dalolat beradi.

Milliy jinoyat qonunchiligimizda kiberjinoyatchilikka qarshi kurashish muammolarini hal etishning eng maqbul yo‘li xalqaro tajribadan unumli foydalanish sanaladi. Quyida aynan mazkur xalqaro tajribalar tahlilini amalga oshiramiz.

Shvetsiyada kiberjinoyatchilik jiddiy ijtimoiy xavf sifatida qaraladi. Swedish Crime Survey (2024) natijalarida aholining internetda firibgarlikka uchrashdan xavotiri 2022-yildagi *32%* dan 2024-yilda *38%* ga ko‘tarilgani ko‘rsatiladi [14]. Shvetsiya tajribasi kiberjinoyatchilikka qarshi kurashishda (ayniqsa onlayn firibgarlik va elektron dalillar bilan ishlashda) quyidagi asosiy chora-tadbirlarni yo‘lga qo‘yganligi bilan e’tiborga loyiq:

Shvetsiyada Kiberjinoyatchilikka ixtisoslashgan huquqni muhofaza qiluvchi organ tashkil etilgan. Kiberjinoyatlar bo‘yicha ishlar *Swedish Police Authority* tarkibidagi Milliy operatsiyalar departamenti (NOA) kabi markazlashgan tizim orqali muvofiqlashtiriladi [15]. Shvetsiya amaliyoti shuni ko‘rsatadiki, banklar, politsiya hamda telekommunikatsiya operatorlari o‘rtasida kuchaytirilgan axborot almashinuvi hamda spoofing (soxta raqam ko‘rsatish)ni cheklovchi texnik yechimlar joriy etilgan. Shuningdek, ushbu davlatda kiberjinoyatchilikka oid zamonaviy usullar haqida aholini xabardor qilish kompaniyalari (onlayn firibgarlik, phishing, “romance scam” kabi sxemalarga qarshi ogohlantirish) joriy etilgan. Ushu mamlakat telefon orqali firibgarlikka qarshi yaxshi natijaga erishgan. Shvetsiya bank sektori “telefon firibgarligi” bo‘yicha amaliy dastur natijasida 2024-yilda jinoyat daromadlari 2023-yilga nisbatan

40% kamaygani haqidagi hisoboti fikrimizni tasdiqlaydi [16]. Yana bir e'tiborli holat shundaki, barcha darajadagi davlat organlari raqamli bank xizmatlari, raqamli ijtimoiy xizmatlar va raqamli tijorat kabi raqamli xizmatlardan foydalanishda yordamga muhtoj shaxslarni qo'llab-quvvatlab boradilar. Bu esa, aholining yordamga muhtoj qismi kiberjinoyat qurboniga aylanib qolishining oldini olishga qaratilgan. Shvetsiya Budapesht konvensiyasi doirasida kiberjinoyatlar bo'yicha hamkorlik ham amalga oshiruvchi davlatlar qatoriga kiradi.

Yaponiyaning kiberfiribgarlik, axborot tizimiga noqonuniy kirish, phishing kabi jinoyatlarga qarshi kurashga oid "Noqonuniy kompyuter tizimiga kirishni taqiqlash to'g'risida"gi Qonun [17] (14 moddani o'z ichiga oladi) bunday qilmish uchun javobgarlik belgilab, tegishli jazo hamda profilaktika choralarini o'rnatgani bilan ahamiyatlidir.

Japan National Police Agency (NPA) 2023-yil davomida "computer fraud" jinoyatiga oid 950 ta ish (*31,6%*) kuzatilganligi hamda yuqorida nomi keltirilgan Qonun buzilishi bilan bog'liq 521 ta (*17,3%*) holat qayd etilganligi bo'yicha statistik ma'lumotlar e'lon qiladi [18]. Ushbu holatlarga qarshi kurash bo'yicha HMQO organlarini va aholini o'qitish choralari doimiy ravishda olib boriladi. Ushbu davlat tajribasida eng muhim jihat shundaki, sog'liqni saqlash sohasida yuzaga keluvchi kiberjinoyatchilikni oldini olishga oid choralar doirasi normativ hujjatlar bilan mustahkamlanganligidir. Masalan, Japan National Police Agency (NPA) 2023-yil aprelida Japan Medical Association bilan memorandum imzolab, tibbiyot muassasalarida ransomware kabi kiberhodisalarni oldini olish va hodisa yuz bersa tezkor xabar berish va maslahatlashuv mexanizmini kuchaytirish choralarini ishlab chiqqan va amaliyotga tatbiq etilgan. NPA xalqaro qo'shma tergovlarni kuchaytirib, Yevropol va boshqalar bilan hamkorlik doirasida 2024-yil fevralida LockBit bilan bog'liq jinoyatlarni aniqlash va serverlarga reydlar o'tkazish bo'yicha doimiy faoliyat yuritib keladi.

Yaponiya JKda kompyuterga zarar yetkazish orqali biznesga to'sqinlik qilish (Art. 234-2), Kompyuter firibgarligi (Art. 246-2), Elektromagnit yozuvlarni ruxsatsiz yaratish (Art. 161-2), To'lov kartalari bo'yicha elektron yozuvlarni qalbakilashtirish (Art. 163-2–163-5) va boshqa ijtimoiy xavfli qilmishlar uchun jinoiy javobgarlik belgilangan. Shu bilan birga e'tibor berish kerakki, Yaponiyada axborot tizimiga ruxsatsiz kirish kabi ayrim kiberjinoyatlar alohida maxsus qonunlar bilan ham tartibga solinadi.

Germaniyada ham so'nggi yillarda kiberjinoyatchilik darajasiga oid rasmiy statistik ma'lumotlarga qaraganda 2024-yilda Germaniyada Politsiya jinoyat statistikasida 131391 ta kiberjinoyat qayd etilgan; bundan tashqari, 201877 ta kiberjinoyatlarni sodir etgan shaxslar chet el hududida bo'lgani holda jinoyatni Germaniyada sodir etgani ta'kidlanadi [19]. Shuningdek, 2023-yilda kiberjinoyatlarni fosh etish darajasi 32,2% ekani ham qayd etilgan [20]. 2024-yil bo'yicha Bundeslagebild (Federal jinoiy politsiya idorasi)ning taqdimotida ransomware tahdidi ham dolzarbligi saqlanib, masalan 950 ta ransomware hujumi ro'yxatga olingani tilga olinadi.

Germaniya kiberjinoyatchilikka qarshi kurashni, avvalo, jinoyat-huquqiy normalar orqali "kiber-muhitdagi tajovuzlar"ni kriminallashtirish orqali kompleks yo'lga qo'yadi. Germaniya JKda (StGB) kiberjinoyatlar sifatida: ma'lumotlarni ruxsatsiz qo'lga kiritish (Data espionage §202a), Phishing (§202b), (§202a va §202b jinoyatlarga tayyorgarlik harakatlari (§202c), kompyuter ma'lumotlarini yo'q qilish, o'zgartirish, buzish (Data manipulation §303a), kompyuter sabotaji (§303b), kompyuter firibgarligi (§263a), shuningdek isbotlashga oid ma'lumotlarni qalbakilashtirishga doir normalar (§269-§270) belgilangan.

Axborot texnologiyalari xavfsizligi bo'yicha Federal idora (Bundesamt für Sicherheit in der Informationstechnik)ga kiberhodisalar ro'y bergan har bir holat haqida kritik infratuzilmalarni, ya'ni jamiyat uchun juda muhim bo'lgan tashkilotlar va obyektlarni xabardor etish majburiyati yuklatilgan [21]. Aynan mazkur idora tashkilotlar uchun axborot, tavsiyalar, tajriba almashish va amaliy yo'riqnomalar platformasini yuritadi.

Xitoy Xalq Respublikasi Jamoat xavfsizligi vazirligi ma'lumotiga ko'ra, 2023-yil yanvar-noyabr oralig'ida kiberfiribgarlik bo'yicha 391 000 ta jinoyat ishi fosh etilgan. 2024-yilda kiberfiribgarlik jinoyatlari bo'yicha 78 000 kishi prokuratura tomonidan ta'qib qilingan (kiberfiribgarlik 2023-yilga qaraganda 53.9% ortgan) [22].

XXRda kiberjinoyatchilik JKning bir qator moddalari (285, 286, 287, 287[1]-moddalar) bilan birgalikda 2017-yil 1-iyundagi "Kiberxavfsizlik to'g'risidagi qonun" (Cybersecurity Law), 2021-yilda qabul qilingan "Ma'lumotlar xavfsizligi to'g'risidagi qonun" (Data Security Law), "Shaxsiy ma'lumotlarni himoya qilish to'g'risidagi qonun" (Personal Information Protection Law), 2022-yildagi ("Telekommunikatsiya va onlayn firibgarlikka qarshi kurash to'g'risidagi qonun" (Anti-Telecom and Online Fraud Law) kabi normativ-huquqiy hujjatlar bilan ham tartibga solinadi. Masalan, "Kiberxavfsizlik to'g'risida"gi Qonun mamlakatda umumiy kiberxavfsizlik rejimini belgilab bersa, "Ma'lumotlar xavfsizligi to'g'risidagi qonun" ma'lumotlarni qayta ishlash umumiy tartibi va davlat xavfsizligi bilan bog'liq yo'nalishda mazkur turdagi jinoyatlarga qarshi hujjat sanaladi. "Telekommunikatsiya va onlayn firibgarlikka qarshi kurash to'g'risida"gi qonun internet platformalari, moliya institutlari va boshqa subyektlar zimmasiga firibgarlik xavflarini kamaytirish, nazorat mexanizmlarini joriy etish, shubhali operatsiyalarni cheklash va hamkorlik qilish kabi majburiyatlarni yuklaydi.

AQShda FBI Internet Crime Complaint Center (IC3) 2024-yilda kiberjinoyatlar yuz berganligiga oid 859 532 ta shikoyat va $16,6 mlrd zarar qayd etilganini e'lon qiladi [23]. **Buyuk Britaniya** rasmiy statistikasida ham aynan ushbu turdagi jinoyatlar yuqori ko'rsatkichni qayd etganligi qayd etiladi. Bu holatga qarshi kurashishda "kiber gigiyena" (zararli dasturlardan himoya (antimalware)**,** bir necha bosqichli parol siyosati**,** bulutli zaxira (cloud back-ups), administrator huquqlarini cheklash) va xatarni muntazam o'lchash va ularni aholini ogohlantirish orqali kamaytirish yondashuvi ilgari surilmoqda [24]. **Estoniya** kiberxavflarni boshqarishning institutsional modelini joriy eta olgan, deyish mumkin. NATO Cooperative Cyber Defence Centre of Excellence (Tallinn) ilmiy-amaliy markazi [25] tomonidan trening, seminar va huquqiy-tahliliy yo'nalishlarda aholi va davlat organlari xodimlarining kiberxavfsizlikka oid bilimlarini oshirish choralari doimiy ravishda ko'rilib kelishi bilan ahamiyatli.

Yuqorida tahlil etilgan kiberxavfsizlik yo'nalishida yutuqlarga erishgan mamlakatlar tajribasini o'rganish orqali bir qator taklif va tavsiyalar shakllantirildi. Quyida xulosa sifatida ularni keltirib o'tamiz:

Birinchidan, **kiberjinoyat bo'yicha yagona milliy xabar berish portali va muntazam yillik statistika e'lon qilish amaliyotini joriy etish.** Statistika bu holatda hisobot vositasi emas, balki tahliliy resurs sifatida namoyon bo'lishi lozim. U, avvalo, jinoyatlarni erta aniqlash, resurslarni maqsadli taqsimlash va bu yo'nalishdagi davlat siyosati samaradorligini obyektiv o'lchash imkonini beradi. Mamlakatimizda bunday yagona yondashuv shakllantirilmasa, latent kiberjinoyatchilik darajasi oshishining oldini olish imkoni cheklanadi.

Ikkinchidan, **davlat organlari, bank, mobil operatorlar o'rtasida majburiy va tezkor axborot almashinuvini ta'minlash.** Shvetsiya tajribasi bu taklifning samaradorligini tasdiqlaydi, ya'ni banklar, politsiya va telekommunikatsiya operatorlari o'rtasidagi kuchaytirilgan axborot almashinuvi natijasida kiberfiribgarlikdan olingan jinoiy daromadlarning kamayganligi bunga misol bo'la oladi. Xitoyda esa, bunday hamkorlikni ixtiyoriy emas, balki internet platformalari va moliya institutlari zimmasiga yuklatilgan majburiyat sifatida belgilanganligi ham e'tiborga loyiq. Kiberfiribgarlikda mablag' daqiqalar ichida o'tkazilishini hisobga olib, shubhali operatsiyalarni vaqtincha to'xtatib turish va xabar berish choralari barcha banklarda joriy etilishi maqsadga muvofiq. Ayni paytda bunday ma'lumot almashinuvi shaxsiy ma'lumotlarni himoya qilish talablari bilan aniq chegaralanishi shart.

Uchinchidan, **kiberjinoyat sodir etilgan har bir hodisaga tezkor javob taqdim etish salohiyatini kuchaytirish.** Bu esa, ikki holatga e'tibor berishni talab qiladi: birinchisi, kiberxavfsizlikka ixtisoslashgan markazlashgan tuzilma yaratish bo'lsa, ikkinchi holat kiberjinoyatlarga qarshi transchegaraviy hamkorlik kanallarini kengaytirishdir.

To'rtinchidan, **aholiga yo'naltirilgan profilaktik xabardor etish (phishing, firibgarlik, identifikatsiya imkoniyatining cheklanganligi) choralarini tizimli yo'lga qo'yish**. Kiberjinoyatlarning aksariyati texnik bilimlarning zaifligidan emas, balki inson omilidan foydalanish orqali sodir etiladi. Shu bois, ma'rifiy ish mustaqil profilaktika yo'nalishi maqomiga ega bo'lishi kerak. Buyuk Britaniyaning "kiber gigiyena" (antimalware, ko'p bosqichli parol siyosati, administrator huquqlarini cheklash) yondashuvi va Estoniyaning NATO CCDCOE bazasidagi muntazam trening modeli bunga misol bo'la oladi.

IQTIBOSLAR/СНОСКИ/REFERENCES:

1. Карпова Д. Н. Киберпреступность: глобальная проблема и ее решение // Власть. 2014. № 8. С. 46–50.

2. Чекунов И. Г. Понятие и отличительные особенности киберпреступности // Российский следователь. 2014. № 18. С. 53.

3. Шевко Н. Р. Особенности раскрытия и расследования киберпреступлений: проблемы и пути их решения // Ученые записки Казанского юрид. ин-та МВД России. 2016. Т. 1, № 1 (1). С. 13–16.

4. Computer-related crime, Recommendation № R (89) 9 on computer-related crime and finel report of the European Committee on crime problems, Strasbourg, 1990 // https://www.oas.org. (Murojaat etilgan sana: 14.07.2026).

5. World Summit on the Information Society, First Phase: 10-12 December 2003 // https://www.itu.int/net/wsis/geneva/index.html.

6. Convention on Cybercrime, Budapest, 23.XI.2001 //rm.coe.int/1680081561

7. United Nations Convention against Cybercrime// https://www.unodc.org/unodc/en/cybercrime/convention.

8. O‘zbekiston Respublikasi hukumati bilan Belarus Respublikasi hukumati o‘rtasidagi 2008-yil 24-dekabrdagi “Jinoyatchilikka qarshi kurash sohasida hamkorlik to‘g‘risida”gi bitim // O‘zbekiston Respublikasi xalqaro shartnomalari to‘plami, 2008-y., 3-4-son (https://lex.uz/docs/-1469438).

9. O‘zbekiston Respublikasi hukumati bilan Kipr Respublikasi hukumati o‘rtasidagi “Jinoyatchilikka qarshi kurashda hamkorlik qilish to‘g‘risida”gi Bitim // O‘zbekiston Respublikasi xalqaro shartnomalari to‘plami, 2015-y., 1-son. (https://lex.uz/docs/-2685713?otherlang=1).

10. O‘zbekiston Respublikasi bilan Tojikiston Respublikasi o‘rtasida “Xavfsizlik va jinoyatchilikka qarshi kurashish sohasida hamkorlik to‘g‘risida”gi bitim // https://lex.uz/docs/-3801311.

11. O‘zbekiston Respublikasi hukumati bilan Quvayt davlati hukumati o‘rtasidagi “Jinoyatchilikka qarshi kurash sohasida hamkorlik to‘g‘risida”gi Bitim // O‘zbekiston Respublikasi xalqaro shartnomalari to‘plami, 2007-y., 2-3-son. https://lex.uz/docs/-1333995.

12. O‘zbekiston Respublikasi hukumati bilan Turkmaniston Hukumati o‘rtasidagi “Jinoyatchilikka qarshi kurashda hamkorlik qilish to‘g‘risida”gi Bitim // lex.uz/docs/-2067308.

13. O‘zbekiston Respublikasi hukumati bilan Turkiya Respublikasi Hukumati o‘rtasida “Jinoyatchilikka qarshi kurashda hamkorlik qilish to‘g‘risida”gi Bitim // https://lex.uz/uz/docs/-5847512.

14. Statistics from the judicial system of Sweden //https://bra.se/download/18.1e21615019329787e39813b2024 (Murojaat etilgan sana: 09.07.2026).

15. The Swedish Police Authority // https://polisen.se/en/the-swedish-police/the-swedish-police-authority (Murojaat etilgan sana: 09.07.2026).

16. Threat assessment for Sweden’s banks. Published May 2025 // https://www.financesweden.se/media.

17. Act on Prohibition of Unauthorized Computer Access（Act No. 128 of 1999) // https://www.japaneselawtranslation.go.jp.

18. Threats in Cyberspace in 2023 // https://www.npa.go.jp/english/bureau/cyber/document.

19. 2024 National Situation Report on Cyber Crime: Numerous succesful investigations, but the threat level remains high // https://www.bmi.bund.de/SharedDocs/pressemitteilungen/EN/2025/06/pm-lb-cybercrime.

20. Geographische Grenzen für Cyberkriminelle unerheblich // https://www.bmi.bund.de.

21. Statistics from The Federal Office for Information Security (BSI) of the Germany (Bundesamt für Sicherheit in der Informationstechnik) // https://www.bsi.bund.de/DE/Themen/Regulierte-Wirtschaft/Kritische (Murojaat etilgan sana: 09.07.2026).

22. Statistics from The Supreme People’s Procuratorate (SPP) of the People’s Republic of China // https://en.spp.gov.cn/2025-03/08/c_1076764 (Murojaat etilgan sana: 10.07.2026).

23. Federal Bureau of Investigation Internet crime report // https://www.ic3.gov/AnnualReport/Reports/2024. (Murojaat etilgan sana: 10.02.2026).

24. Cyber security breaches survey 2025/2026: technical report // https://www.gov.uk/government/statistics (Murojaat etilgan sana: 10.07.2026).

25. Cyber security in Estonia 2025 // https://ria.ee/sites/default/files/documents. (Murojaat etilgan sana: 10.07.2026).

YURIST AXBOROTNOMASI

4-SON

ВЕСТНИК ЮРИСТА

НОМЕР 4

LAWYER HERALD

ISSUE 4

ISSN 2181-9416

DOI JURNAL: 10.34920/2181-9416/2026/4

2026-YIL