INTERNET TARMOG‘I ORQALI SODIR ETILGAN IQTISODIY JINOYATLARGA QARSHI KURASHISH SAMARADORLIGINI OSHIRISHDA XORIJIY TAJRIBANING O‘RNI VA AHAMIYATI

Ruzmatov Bekzod Sherzod o‘g‘li
O‘zbekiston Respublikasi Jamoat xavfsizligi
Universiteti magistratura tinglovchisi

Annotatsiya *darknet hozirgi kunda internet tarmog‘ida global kiberxavfsizlikka hamda iqtisodiy jinoiy faoliyatning kuchayishi jiddiy tahdid solmoqda va butun dunyo bo‘ylab huquq-tartibot idoralari unga qarshi kurashish uchun choralar ko‘rilmoqda. Ushbu chora-tadbirlar huquqiy himoyani kuchaytirish, aholining xabardorligini oshirish, axborot almashishni yaxshilash va yangi dasturiy vositalarni ishlab chiqishni o‘z ichiga oladi. Maqolada huquqni muhofaza qilish organlari xodimlarini darknet faoliyatini aniqlash va kuzatish, darknetdagi noqonuniy iqtisodiy harakatlarga qarshi kurashish uchun yangi tashkiliy tuzilmalar va huquqiy standartlarni yaratish muhimligi ta’kidlangan.*

Kalit so‘zlar: *Darknet, kiberjinoyat, pul tashish (money muling), EC3, Tor, Xavfsiz internet ligasi.*

РОЛЬ И ЗНАЧЕНИЕ ЗАРУБЕЖНОГО ОПЫТА В ПОВЫШЕНИИ ЭФФЕКТИВНОСТИ БОРЬБЫ С ЭКОНОМИЧЕСКИМ ПРЕСТУПЛЕНИЯМИ, СОВЕРШАЕМЫМИ ЧЕРЕЗ СЕТЬ ИНТЕРНЕТ

Аннотация *даркнет в настоящее время представляет собой серьезную угрозу глобальной кибербезопасности и росту экономической преступности в Интернете, и правоохранительные органы по всему миру принимают меры по борьбе с ней. Эти меры включают усиление правовой защиты, повышение осведомленности общественности, улучшение обмена информацией и разработку новых программных инструментов. В статье подчеркивается важность создания новых организационных структур и правовых норм для сотрудников правоохранительных органов по выявлению и мониторингу даркнет-деятельности, а также по борьбе с незаконной экономической деятельностью в даркнете.*

Ключевые слова: *Даркнет, киберпреступность, отмывание денег, EC3, Tor, Лига безопасного Интернета.*

THE ROLE AND SIGNIFICANCE OF FOREIGN EXPERIENCE IN INCREASING THE EFFICIENCY OF THE FIGHT AGAINST ECONOMIC CRIMES COMMITTED THROUGH THE INTERNET NETWORK

Abstract *the Darknet is now a serious threat to global cyber security and the rise of economic crime on the Internet, and law enforcement agencies around the world are taking steps to combat it. These measures include strengthening legal protection, increasing public awareness, improving information sharing, and developing new software tools. The article emphasizes the importance of creating new organizational structures and legal standards for law enforcement officials to detect and monitor darknet activities, and to combat illegal economic activities on the darknet.*

Keywords: *Darknet, cybercrime, money laundering, EC3, Tor, Safer Internet League.*

Global internet tarmog‘i rivojlanib borgani sari odamlar uchun nafaqat qulaylik, balki xavf o‘choqlaridan biriga aylanib bormoqda. Bu borada mutaxassislar internetdagi jinoyatlarning turi va ko‘lami kengayib borayotganligini aytishmoqda. Hozirgi kunda Darknet ya’ni “Qora tarmoq” global hodisaga aylanib, u orqali sodir etilayotgan iqtisodiy jinoyatlar butun dunyo mamlakatlariga ta’sir ko‘rsatmoqda. Ushbu yashirin tarmoq orqali turli xil iqtisodiy jinoyatlarni amalga oshirilib kelinadi hamda ular anonimlikni saqlab qolish maqsadida to‘lovlarni kriptovalyutalar orqali amalga oshiradilar. Darknetdagi jinoyatlarga qarshi kurashish o‘ta murakkab hisoblanadi, chunki u hech qanday iz qoldirmaydi. Darknetda kiberjinoyatchilar to'planib, noqonuniy tovarlarni sotib olish va sotish platformalari mavjud. Deyarli barcha Darknet saytlari TOR («The Onion Router», Internetdagi maxfiylik va anonimlik uchun yaratilgan notijorat tashkilot) brauzeri orqali yashirinadi. Jahonda “Darknet” orqali sodir etilgan iqtisodiy jinoyatlarga qarshi kurashni takomillashtirishda bir qator ishlar amalga oshirilgan. Misol uchun, AQSh Federal Qidiruv Byurosi (FQB) darknet bilan bog‘liq jinoiy faoliyatlarni tergov qilish bilan shug‘ullanuvchi maxsus guruhga (Joint Criminal Opioid Darknet Enforcement) ega, Buyuk Britaniya Milliy Jinoyat Agentligida (NCA) kiberjinoyat va iqtisodiy jinoyatlarga e’tibor qaratadigan maxsus guruh ya’ni (Jinoiy daromadlarni legallashtirish bo‘yicha qo‘shma razvedka guruhi, JMLIT) mavjud. Jinoiy daromadlarni legallashtirish bo‘yicha qo‘shma razvedka guruhi – bu pul yuvish va iqtisodiy tahdidlarga oid ma’lumotlarni almashish va tahlil qilish uchun huquqni muhofaza qilish organlari va moliya sektori o‘rtasidagi hamkorlikdir.

Rossiya Federatsiyasi hukumati fuqarolarni “Darknet”, shuningdek internetdagi xavf-xatarlari haqida xabardor qilish va har qanday shubhali faoliyat haqida xabar berishga undash uchun “Xavfsiz Internet Ligasi” veb-sayti ishlab chiqilgan. Agar fuqarolar internetda noqonuniy faoliyatni aniqlasalar, ular “http://www.ligainternet.ru/hotline/” havolasi orqali xabar berishlari mumkin hamda ushbu sayt bolalar va ota-onalarga internet tarmogidan xavfsiz foydalanish haqida kunlik ma’lumotlar berilib boriladi. Ushbu veb-sayt orqali fuqarolarni turli ko‘rinishdagi jinoyatlardan saqlash maqsadida bir qator tavsiyalar berib o‘tilgan.

Yevropa Ittifoqi 2013-yil 11-yanvar kuni internet tarmoqlardagi jinoyatlarga qarshi kurashish maqsadida Yevropa Kiberjinoyat markazini (EC3) tashkil etdi. EC3

“Darknet” orqali sodir etilgan kiberjinoyat va iqtisodiy jinoyatlarni ta’qib qilishda a’zo davlatlarga operativ yordam va ekspertiza o‘tkazishda yordam beradi.

Kiberjinoyatchilik markazi (EC3) har yili Yevropa Ittifoqidagi hukumatlar, biznes va fuqarolarga ta’sir ko‘rsatadigan kiberjinoyatchilikdagi tahdidlar va o‘zgarishlar to‘g‘risidagi asosiy strategik hisobotni nashr etib boradi.

FQB “Tor”ning ma’lum foydalanuvchilarini aniqlashga urinib, 2002-yildan beri FQB “Tor” kabi proksi-serverlar yoki anonimlik xizmatlaridan foydalangan holda o‘z manzilini yashirayotgan gumonlanuvchilarni aniqlash uchun “kompyuter va internet protokoli manzilini tekshirish” (CIPAV) dasturidan foydalangan[38].

Ushbu dastur orqali darknetda noqonuniy faoliyat bilan shug‘ullangan shaxslarni deanonimlashtirishni amalga oshiradi.

Darknetdagi jinoiy faoliyatga qarshi kurashish maqsadida Politsiya Ijroiya Tadqiqot Forumi tomonidan tashkil etilgan ekspertlar seminarida quyidagilar tavsiya etilgan:

– Trening – ofitserlar va tergovchilarni darknet tarmog‘ining tegishli dalillarini aniqlashga o‘rgatish;

– Axborot almashish – agentliklar o‘rtasida ham ichki, ham xalqaro miqyosda axborot almashishni yaxshilash;

– Hamkorlik uchun yangi tuzilmalar – hamkorlik uchun tashkilotlararo tuzilmalarni qurishning afzalliklarini o‘rganish;

– Yangi sud standartlari – kompyuterlarda darknet veb-dalillarni to‘plash va sudga taqdim etish uchun yangi standartlarni ishlab chiqish;

– Jinoyatlarmi aloqadorlik bo‘yicha o‘rganish – huquqni muhofaza qilish organlariga darknetda an’anaviy jinoyatlar va kamroq sodir etiladigan jinoyatlarni o‘rganish va jinoyani ochishda yordam berish uchun o‘zaro bog‘liqligini o‘rganish[39].

Internetda uyushgan jinoyatchilik tahdidini baholash (IOCTA) – huquq-tartibot idoralari, siyosatchilar va huquqni muhofaza qiluvchi organlarga kiberjinoyatlarga samarali va kelishilgan tarzda javob berish uchun asosiy tavsiyalar ishlab chiqadi[40].

So‘nggi Internet tarmog‘ida uyushgan jinoyatchilik tahdidini baholash *(Internet Organized Crime Threat Assessment, IOCTA*) shuningdek, qo‘shimcha jinoyatlar sohasini, onlayn jinoiy bozorlarni ham ko‘rib chiqadi. Shuningdek, IOCTAning yana bir tipik yo‘nalishi – bu bir nechta jinoyat sohasini qamrab oluvchi, ya’ni o‘z-o‘zidan jinoiyatni yashiradigan yoki uning sodir etilishiga omil boladigan qo‘zg‘atuvchilarni ham qamrab oladi. Ushbu faollashtiruvchilarga quyidagilar kiradi:

– Biznes elektron pochta kelishuvi;

[38] Kevin Poulsen, “FBI Admits It Controlled Tor Servers Behind Mass Malware Attack,” Wired.com, September 13, 2013.
[39] National Instiute of Justice. Taking on the Dark Web: Law Enforcement Experts ID Investigative Needs. URL: https://nij.ojp.gov/topics/articles/taking-dark-web-law-enforcement-experts-id-investigative-needs
[40] Internet Organized Crime Threat Assessment (IOCTA). URL: https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment

– Qattiq himoyalangan xosting;

– Anonimlashtirish vositalari;

– Kriptovalyutalarni jinoiy egallab olish;

– Pul tashish (*money muling*).

Pul tashish – jinoiy daromadlarni legallashtirishning bir turi. Pulni tashuvchi – bu uchinchi shaxsdan o‘z bank hisobvarag‘iga pul olib, boshqasiga o‘tkazadigan yoki naqd pulda olib, boshqa birovga beradigan, buning uchun komissiya oladigan shaxs[41].

Ular jinoiy daromadlarni legallashtirish bilan bog‘liq jinoyatlarda (kiber jinoyatlar, onlayn firibgarlik va boshqalar) vositachi hisoblanishadi, chunki ular bunday jinoyatlardan olingan daromadlarni legallashtirishga va anonim qolishga yordam beradi.

Jinoyatchilar vaqt o‘tishi bilan yangi innovatsion usullarda jinoyat sodir etadilar, shuning uchun huquqni muhofaza qilish organlarining asosiy vazifasi tez rivojlanayotgan jinoyatchilikdan ortda qolmasliklari lozim. Bunda jinoyatchilikka qarshi ilg‘or, zamonaviy vosita va usullar bilan kurashish zarur.

Bu borada mamlakatimizda Ichki ishlar vazirligi hamda Xalqaro Interpol jinoyat politsiyasi tashkiloti bilan hamkorlikda Markaziy Osiyo mamlakatlari huquq-tartibot va axborot texnologiyalari sohasi mutaxassislari bilan seminarlar tashkil etilgan. Bu seminarda kiber-jinoyatchilikka qarshi kurashishni kuchaytirish va raqamli ekspertizalar o‘tkazish bo‘yicha tajriba almashish, Interpol doirasidagi amaliy hamkorlik, shuningdek ushbu yo‘nalishda mintaqaviy sheriklar bilan o‘zaro aloqalar o‘rnatish hamda mutaxassislar axborot xavfsizligini ta’minlashga oid eng so‘nggi yutuqlar, kiber-jinoyatchilikning oldini olish usullari, ularga qarshi kurashish borasida qo‘llanilishi zarur bo‘lgan texnologiyalar va ma’lumotlar bilan bilan tanishib chiqilgan.

Markaziy bankda ham kiberxavfsizlik va moliyaviy firibgarlikka qarshi kurashuvchi hamda bank axborot tizimlarining uzluksiz ishlashini monitoring qiluvchi markaz ochilishi xabar qilingan edi.

Ushbu markazning asosiy vazifasi bank va moliya sohasida axborot hamda kiberxavfsizlik tahdidlarining oldini olish hamda moliyaviy firibgarliklarga qarshi ta'sir choralarini ko‘rishdan iborat ekanligi ma'lum qilingan.

Umuman olganda, yashirin tarmoqdagi “Darknet” orqali sodir etilayotgan iqtisodiy jinoyatlarga qarshi kurashda huquq-tartibot tizimini kuchaytirish, aholining xabardorligini oshirish, ma’lumotlar almashishni yaxshilash, xalqaro hamkorlikni mustahkamlash, ilg‘or texnologiyalarni rivojlantirish, hamda xususiy sektor bilan ishlashni o‘z ichiga olgan global sa’y-harakatlarni talab qiladi.

Davlatlar o‘rtasida tajribalar almashish va hamkorlik qilish orqali “Darknet” tarmog‘ida sodir etilayotgan iqtisodiy jinoyatlarning oldini olish va ularga barham berishda muvaffaqiyatga erishish mumkin.

[41] Money Muling. URL: https://www.europol.europa.eu/operations-services-and-innovation/public-awareness-and-prevention-guides/money-muling

Yuqoridagilardan kelib chiqib quyidagilar xulosalar qilindi:

Huquqni muhofaza qilish organlari hodimlarining zarur malakasi va tayyorgarligiga e'tibor berib, ularning qorong'u tarmoq haqida xabardorligini oshirish.

Fuqarolarni "Darknet", shuningdek internetdagi xavf-xatarlari haqida xabardor qilish va har qanday shubhali faoliyat haqida xabar berishga undash uchun veb-sayt ishlab chiqish. Ushbu sayt orqali aholiga turli xil kiberhujumlarga uchramasliklari uchun tavsiyalar berib borish. Jumladan:

Ijtimoiy tarmoqlarda o'zingiz haqingizdagi ma'lumotlarni, fotosuratlaringiz, manzillaringiz, sevimli mashg'ulotlaringiz joylashtirmaslikni, internetda har qanday xaridni amalga oshirayotganda hushyor bo'lish kerakligini, saytni batafsil va diqqat bilan o'rganishlikni, uning nomi va manzili, tovar va xizmatlarni sotib olmoqchi bo'lgan tashkilotning rasmiy nomi bilan solishtirishlikni, hech qanday tasodifiy havolalarni bosmaslikni, shubhali saytlarda bank kartangiz tafsilotlarini qoldirmaslikni, sotuvchi haqida sharhlarni o'rganishlikni hamda ushbu saytda bozorda u haqidagi sharhlar sanasini tekshirishlikni va sotuvchining barcha yozishmalarini va kontaktlarini saqlab, sayt nomini yozish kerakligini, ushbu ma'lumot huquqni muhofaza qilish organlariga firibgarlarni qo'lga olishga yordam beradi. Hatto notanish saytlarga ham kirmaslik kerakligini, ba'zi saytlar o'z-o'zidan zararli dasturlar va viruslarni o'rnatishga qodir. Ishonchsiz va shubhali elektron pochta xabarlarini ochmaslik va elektron pochtada noma'lum jo'natuvchidan kelgan fayllarni yuklab olmasliklardan habardor qilish.

Agar fuqarolar internatda noqonuniy faoliyatni aniqlasalar, ular veb-sayt orqali xabar berishlari mumkin.

FOYDALANILGAN ADABIYOTLAR:

1. Kevin Poulsen, "FBI Admits It Controlled Tor Servers Behind Mass Malware Attack," Wired.com, September 13, 2013.
2. National Instiute of Justice. Taking on the Dark Web: Law Enforcement Experts ID Investigative Needs. URL: https://nij.ojp.gov/topics/articles/taking-dark-web-law-enforcement-experts-id-investigative-needs
3. Internet Organized Crime Threat Assessment (IOCTA). URL: https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment
4. Money Muling. URL: https://www.europol.europa.eu/operations-services-and-innovation/public-awareness-and-prevention-guides/money-muling