YASHIRIN TARMOQ DARKNET ORQALI SODIR ETILGAN IQTISODIY JINOYATLARGA QARSHI KURASHISH SAMARADORLIGINI OSHIRISHDA XORIJIY TAJRIBANING O‘RNI VA AHAMIYATI

Muxsimov Ulug‘bek Timurbek o‘g‘li

Sergeli tuman prokuraturasi katta tergovchisi

ANNOTATSIYA

Darknetda jinoiy faoliyatning kuchayishi global kiberxavfsizlikka jiddiy tahdid solmoqda va butun dunyo bo‘ylab huquq-tartibot idoralari unga qarshi kurashish uchun choralar ko‘rmoqda. Ushbu chora-tadbirlar huquqiy himoyani kuchaytirish, aholining xabardorligini oshirish, axborot almashishni yaxshilash va yangi dasturiy vositalarni ishlab chiqishni o‘z ichiga oladi. Yevropa Ittifoqi a’zo davlatlarga kiberjinoyat va iqtisodiy jinoyatlarni tergov qilish va ta’qib qilishda operativ yordam va ekspertiza bilan ta’minlash uchun Yevropa kiberjinoyatchilik markazini (EC3) tashkil etdi. Bundan tashqari, Evropa Ittifoqining huquqni muhofaza qilish organlarining favqulodda vaziyatlarda harakat qilish protokoli favqulodda vaziyatlarda huquqni muhofaza qilish idoralari o‘rtasidagi hamkorlikni osonlashtirishga qaratilgan. Maqolada, shuningdek, huquqni muhofaza qilish organlari xodimlarini darknet faoliyatini aniqlash va kuzatish, agentliklar o‘rtasida ma’lumot almashishni yaxshilash va darknetdagi noqonuniy harakatlarga qarshi kurashish uchun yangi tashkiliy tuzilmalar va huquqiy standartlarni yaratishga o‘rgatish muhimligi ta’kidlangan.

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

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

ABSTRACT

The rise of criminal activities on the darknet poses a significant threat to global cybersecurity, and law enforcement agencies worldwide are taking steps to combat it. Measures include strengthening legal protection, increasing public awareness, improving information sharing, and developing new software tools. The European Union has established the European Cybercrime Centre (EC3) to provide operational support and expertise to member states in investigating and prosecuting cybercrime and economic crime. Additionally, the EU Law Enforcement Emergency Response Protocol aims to facilitate cooperation between law enforcement agencies in emergency situations. The article also highlights the importance of training officers to identify and track darknet activities, improving information sharing between agencies, and creating new organizational structures and legal standards to combat illegal activities on the darknet.

Keywords: *Darknet, cybercrime, money muling, EC3, Tor, RAND project, Safe internet league.*

Qorong‘u tarmoqdagi jinoyatlarni o‘rganish internet xavfsizligini ta’minlash va kiberjinoyatlarga qarshi kurashda muhim qadamdir. “Darknet” global hodisaga aylandi va u orqali sodir etilayotgan iqtisodiy jinoyatlar butun dunyo mamlakatlariga ta’sir ko‘rsatmoqda. Darknetdagi jinoyatlarga qarshi kurashish uchun maxsus usullar kerak, chunki ular maxsus shaklda sodir etiladi va deyarli hech qanday iz qoldirmaydi. Jahon mamlakatlari “Darknet” orqali sodir etilgan iqtisodiy jinoyatlarga qarshi kurashni takomillashtirishga oid bir necha vazifalarni o‘z oldiga qo‘yishgan:

Huquqni muhofaza qilishni kuchaytirish: AQSh Federal Qidiruv Byurosi (FQB) darknet bilan bog‘liq jinoiy faoliyatlarni tergov qilish bilan shug‘ullanuvchi

maxsus guruhiga (*Joint Criminal Opioid Darknet Enforcement*) ega, Buyuk Britaniyaning Milliy Jinoyat Agentligida (NCA) kiberjinoyat va iqtisodiy jinoyatlarga e'tibor qaratadigan maxsus guruh (*Jinoiy daromadlarni legallashtirish bo'yicha qo'shma razvedka guruhi, JMLIT*) mavjud.

Jinoiy daromadlarni legallashtirish bo'yicha qo'shma razvedka guruhi – bu pul yuvish va kengroq iqtisodiy tahdidlarga oid ma'lumotlarni almashish va tahlil qilish uchun huquqni muhofaza qilish organlari va moliya sektori o'rtasidagi hamkorlikdir. JMLIT davlat-xususiy axborot almashishning innovatsion modeli bo'lib, 2015-yilda tashkil etilgan va xalqaro miqyosda ilg'or tajriba namunasi hisoblanadi.

Aholining xabardorligini oshirish: 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 internatda noqonuniy faoliyatni aniqlasalar, ular **"**http://www.ligainternet.ru/hotline/" havolasi orqali xabar berishlari mumkin. Birgina AQShning o'zida 60 milliondan ortiq odam elektron identifikator o'g'irlanishidan zarar ko'rgan.[1]

Xavfsiz Internet ligasi – bu "World Wide Web"da xavfli kontent tarqalishiga qarshi kurashish uchun yaratilgan tashkilot. Liga a'zolari tijorat, jamoat tashkilotlari, ommaviy axborot vositalari vakillari va internetdagi xavfli kontentga qarshi kurashga real hissa qo'shish imkoniyati va istagiga ega bo'lgan shaxslar bo'lishi mumkin.[2]

Ma'lumotlar almashishni yaxshilash: Yevropa Ittifoqi butun qit'adagi huquqni muhofaza qilish idoralari o'rtasida ma'lumotlar almashish va hamkorlikni osonlashtirish uchun Yevropa Kiberjinoyat markazini (EC3) tashkil etdi. EC3 "Darknet" orqali sodir etilgan kiberjinoyat va iqtisodiy jinoyatlarni tergov qilish va ta'qib qilishda a'zo davlatlarga operativ yordam va ekspertiza o'tkazishda yordam beradi.

[1] United States; Congress; House; Committee on Ways and Means (2018). Protecting Children from Identity Theft Act: report (to accompany H.R. 5192) (including cost estimate of the Congressional Budget Office).

[2] Лига Безопасного интернета. URL: https://www.tadviser.ru/index.phpКомпания:Лига_безопасного_интернета

Yevropa Ittifoqi Kengashi tomonidan “Yevropa Ittifoqi Huquqni muhofaza qilish organlarining favqulodda vaziyatlarda harakat qilish protokoli” (*EU Law Enforcement Emergency Response Protocol*) qabul qilindi. Protokol Yevropolning Yevropa kiberjinoyatchilik markaziga (EC3) markaziy rol o‘ynaydi va Yevropa Ittifoqining keng ko‘lamli transchegaraviy kiberxavfsizligini muvofiqlashtirish rejasining bir qismidir.[1]

Mazkur protokol 7 bosqichni o‘z ichiga oladi:

– Muhim ahamiyatga ega bo‘lgan kibertahdidni erta fosh etish va aniqlash;

– Xavfni tasniflash;

– Favqulodda vaziyatlarda harakatni muvofiqlashtirish;

– Vaqtli ogohlantirish xabari;

– Huquqni muhhofaza qilish organlarining tezkor tadbir rejasi;

– Tergov va bir necha bosqichli tahlil;

– Favqulodda vaziyatlarga javob berish protokoli yakuni.

Yevropolning tezkor tadbirlar bo‘yicha ijrochi direktori o‘rinbosari Uil van Gemert: “Yevropa Ittifoqi va uning fuqarolarini keng ko‘lamli kiberhujumlardan himoya qilish uchun kibertayyorligimizni oshirish juda muhimdir”, deb aytib o‘tgan.[2] Bundan ko‘rinib turibdiki, kiberxavfsizlik masalasi global ahamiyat kasb etmoqda. Bundan tashqari, dasturiy ta’minotlarni zamonaviylashtirmasdan turib xavfsiz kibermakon yaratib bo‘lmaydi.

Dasturiy ta’minot: 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.[3] Ushbu dasturiy ta’minot orqali qorong‘u tarmoqda noqonuniy faoliyat bilan shug‘ullangan shaxslarni deanonimlashtirish amalga oshiriladi.

[1] Commission Recommendation (EU) 2017/1584 of 13 September 2017 on coordinated response to large-scale cybersecurity incidents and crises C/2017/6100

[2] New EU Protocol Preps for X border Cyber-attacks. URL: https://www.cybercureme.com/new-eu-protocol-preps-for-x-border-cyber-attacks/

[3] Kevin Poulsen, “FBI Admits It Controlled Tor Servers Behind Mass Malware Attack,” Wired.com, September 13, 2013.

Darknetdagi jinoiy faoliyatga qarshi kurashish maqsadida Adliya tizimi nomidan RAND va Politsiya Ijroiya Tadqiqot Forumi tomonidan tashkil etilgan ekspertlar seminarida quyidagilarga qaratilgan yuqori darajadagi tavsiyalar taqdim 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.[1]

RAND loyihasi *– Ikkinchi Jahon urushidan keyin 1948-yil 14-mayda tashkil etilgan tashkilot – Kaliforniyaning Santa Monika shahridagi Duglas aviatsiya kompaniyasidan ajralib chiqdi va mustaqil, jamoat farovonligi va xavfsizligi maqsadidagi notijorat tashkilotga aylangan. RAND butun dunyo bo‘ylab jamiyatlarni xavfsizroq, sog‘lomroq va farovonroq qilishga yordam berish uchun davlat siyosati muammolariga yechimlar ishlab chiqadigan tadqiqot tashkilotidir*.[2]

Aleksandr va Safranovlar o‘zlarining tadqiqit ishlarida darknet bilan bog‘liq jinoyatlarni oldini olish va u bilan bog‘liq muammoni hal qilish uchun quyidagi vazifalarni amalga oshirishni ta’minlash kerakligini ta’kidlab o‘tishgan:

1. Darknet tarmog‘ida jinoyatchilar tomonidan qo‘llaniladigan vositalar va resurslarni chuqurroq o‘rganish. Shuni ta’kidlash kerakki, “TOR” brauzeri hozirda yangilik emas, ammo boshqa yopiq veb-brauzerlarda qo‘shimcha bilimlarni kengaytirish;

[1] 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
[2] About the RAND Corporation. URL: https://www.rand.org/about.html

2. Ushbu sohadagi jinoyatlarni tergov qilish metodologiyasi va taktikasini takomillashtirish. Shuningdek, soyali internetdan olingan ma’lumotlarning huquqiy holatini aniqlashtirish;

3. jinoyatlarni ochish uchun tezkor xodimlarni ommaviy tarmoqlarga yo‘naltirish kerak, chunki ko‘p hollarda jinoyatchilar yopiq tarmoqdan faqat jinoyat sodir etish platformasi sifatida foydalanadilar va mijozlar bazasi asosan ochiq tarmoqda to‘planadi.[1]

Sudakova T. va Nomokonov V. lar ham o‘z tadqiqot ishlarida mazkur turdagi jinoyatlarga qarshi kurashishda zaruriy tavsiyalarni berib o‘tishgan. Ular quyidagilar:

– Darknet tarmog‘ining jinoiy tarkibiy qismlarining tizimli tavsiflash;

– Darknetdagi jinoiy faoliyatlar to‘g‘risida aholining turli yosh guruhlari xabardorligini o‘rganish, undan foydalanishning afzal shakllari va maqsadlarini aniqlash, so‘rovnoma qatnashchilarining ushbu hodisaga shaxsiy munosabatini aniqlash;

– Darknetda kiberjinoyatchilikka qarshi kurashish sohasidagi qonunchilik va huquqni qo‘llash amaliyotining qiyosiy huquqiy tahlili (AQSh, Yevropa Ittifoqining alohida davlatlari, Xitoy tajribasi);

– Darknetda va undan foydalanish orqali sodir etilgan jinoiy harakatlarni tergov qilish usullarini ishlab chiqish;

– Raqamli kriminologiyaning ajralmas qismi sifatida Darknetda mavjud bo‘lgan anonim jinoyatlarning oldini olish bo‘yicha kompleks dastur asoslarini ishlab chiqish.[2]

Yuqorida aytib o‘tilganidek, darknetdagi kiberjinoyatlarning oldini olish uchun xavfsizlik organlari internet tarmog‘ida o‘tkaziladigan harakatlarni kuzatishga harakat qilmoqda, ammo darknetdagi anonimlik tufayli faoliyatni kuzatish xavfsizlik organlari

[1] Александров А. Г., Сафронов А. А.,. Криминалистика; судебно-экспертная деятельность; оперативно-розыскная деятельность. Использование сети Даркнет при подготовке и совершении преступлений. – 2021.

[2] Sudakova T. M., Nomokonov V. A. Understanding the future of criminolo-gy: an overview of current trends. Vserossiiskii kriminologicheskii zhurnal / Russian Journal of Criminology, 2018, vol. 12, no. 4, pp. 531–540. DOI: 10.17150/2500-4255.2018.12(4).531-540.

uchun muammo keltirib chiqarmoqda. Muammolarni hal qilish uchun quyidagi yo‘nalishlarga e’tibor qaratish mumkin:

– Mijoz ma’lumotlarini monitoring qilish;

– Ijtimoiy sayt monitoringi;

– Yashirin xizmat monitoringi;

– Semantik tahlil.

Mijoz ma’lumotlarini monitoring qilish: huquqni muhofaza qilish organlari nostandart domen bilan o‘zaro aloqani aniqlash uchun mijozlar veb-ma’lumotlarini kuzatishi va tahlil qilishi mumkin. Shunday qilib, ushbu monitoring darknetdagi havolalarni aniqlamasligi mumkin, ammo bu ularning faoliyati haqida ma’lumot beradi. Monitoring davomida foydalanuvchi maxfiyligi buzilmaydi, chunki huquqni muhofaza qilish organlar veb-saytga kiradigan shaxsni emas, balki veb-so‘rovning manzilini tekshiradi.

Yashirin monitoring: ko‘pgina darknet veb-xizmatlar tez-tez yopiladi va ma’lum vaqtdan keyin yangi domen ostida qayta ishga tushiriladi. Yashirin tekshiruv faoliyati yangi saytlar ishga tushirilishi bilanoq aniqlash va tahlil qilish orqali sayt maqsadini aniqlashdan iborat.

Semantik tahlil: darknetdagi maxfiy xizmatlar ma’lumotlarni olgandan so‘ng, maxfiy xizmat haqida muhim ma’lumotlarni o‘z ichiga olgan semantik ma’lumotlar bazasi yaratilishi mumkin. Ushbu ma’lumotlar bazasi bilan kelajakda saytdagi noqonuniy harakatlarni oldini olish mumkin.

Darknet tarmog‘idagi iqtisodiy jinoyatlarni qarshi kurashish samaradorligini oshirishda jinoyatni isbotlash protsedurasi, ya’ni internet provayderlaridan dalillar olish va sudga dalillarni taqdim etish ham muhim ahamiyat kasb etadi. Darknet tarmog‘ida jinoyat sodir etgan shaxslarni javobgarlikka tortishda muhim jihatlardan biri ularning aybini isbotlab beruvchi dalillar hisoblanadi. Ushbu dalillarni internet provayderlaridan olish va sudga taqdim etish muhim protsessual harakat hisoblanadi. Ushbu jarayonni tezlashtirish va osonlashtirish uchun Yevropa Ittifoqiga a’zo davlatlar elektron dalillar bo‘yicha kelishuvni tasdiqladi. Unga ko‘ra, a’zo davlatdagi xizmat

ko‘rsatuvchi provayderlarga elektron dalillarni olish uchun sud qarorlarini yuborish imkonini beradi.

Shvetsiya Adliya vaziri Gunnar Strommer: “ushbu kelishuv bilan biz adliya organlarimizning asosiy so‘roviga javob beramiz. Borgan sari ko‘proq jinoyatlar onlayn tarzda rejalashtirilgan yoki sodir etilmoqda va bizning rasmiylar oflayn rejimda sodir etilgan jinoyatlar uchun bo‘lgani kabi ularni jinoiy javobgarlikka tortish vositalariga muhtoj. Dalillarni taqdim etish bo‘yicha yangi qoidalar orqali sudyalar va prokurorlarga, ular qayerda saqlanishidan qat’i nazar, ular yo‘qolishidan oldin kerakli dalillarni tezda olish imkonini beradi”, deb ta’kidlagan.[1]

Bugunki kunda jinoyatchilar darknet tarmog‘idagi jinoyatni rejalashtirish va sodir etish uchun texnologiyadan foydalanmoqda. Natijada, huquqni muhofa qilish organlari ularni kuzatib borish va hukm qilish uchun elektron dalillarga tobora ko‘proq tayanishi kerak. Biroq, elektron dalillarga kirish, ayniqsa, ma’lumotlar chet elda saqlangan bo‘lsa, uzoq va murakkab jarayon bo‘lishi mumkin. Shu sababli, Yevropa Kengashining chaqiriqlaridan so‘ng, Komissiya 2018-yil aprel oyida elektron dalillardan foydalanishni yaxshilash uchun yangi qoidalarni taklif qildi.

Elektron dalillar *– jinoiy huquqbuzarliklarni tergov qilish va ta’qib qilish uchun foydalaniladigan raqamli ma‘lumotlarni anglatadi. U o‘z ichiga elektron pochta xabarlari, matnli xabarlar yoki xabar almashish ilovalaridagi kontent, audiovizual kontent foydalanuvchining onlayn hisobi haqida ma’lumotlarni o‘z ichiga oladi.*[2]

Yevropolning Yevropa kiberjinoyatchilik markazi (EC3) har yili Yevropa Ittifoqidagi hukumatlar, biznes va fuqarolarga ta’sir ko‘rsatadigan kiberjinoyatchilikdagi asosiy topilmalar va paydo bo‘layotgan tahdidlar va o‘zgarishlar to‘g‘risidagi asosiy strategik hisobotni (Internet Organized Crime Threat Assessment - IOCTA) nashr etadi.

[1] Electronic evidence: Council confirms agreement with the European Parlament on new rules to improve cross-border to e-evidence. URL: https://www.consilium.europa.eu/en/press/press-releases/2023/01/25/electronic-evidence-council-confirms-agreement-with-the-european-parliament-on-new-rules-to-improve-cross-border-access-to-e-evidence/

[2] Better access e-evidence to fight crime. URL: https://www.consilium.europa.eu/en/policies/e-evidence/

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.*[1]

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

– Biznes elektron pochta kelishuvi;

– 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.*[2]

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

Shunday qilib, biz ishonch bilan aytishimiz mumkinki, taraqqiyot bir joyda to‘xtab qolmaydi, jinoyatchilikning yangi elementlari paydo bo‘ladi, jinoyatchilar vaqt o‘tishi bilan yangi innovatsion usullarda jinoyat sodir etadilar, shuning uchun huquqni

[1] Internet Organized Crime Threat Assessment (IOCTA). URL: https://www.europol.europa.eu/publications-events/main-reports/internet-organised-crime-threat-assessment

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

muhofaza qilish organlarining asosiy vazifasi tez rivojlanayotgan jinoyatchilikdan ortda qolmaslikdan iborat. unga qarshi kurashning eski usullari haqida. Bunda ichki ishlar organlari xodimlarining amaliy faoliyati tajribasini hisobga olish, jinoyatchilikka qarshi ilg‘or, zamonaviy vosita va usullar bilan kurashish zarur.

Umuman olganda, “Darknet” orqali sodir etilayotgan iqtisodiy jinoyatlarga qarshi kurash huquq-tartibot tizimini kuchaytirish, aholining xabardorligini oshirish, ma’lumotlar almashishni yaxshilash, xalqaro hamkorlikni mustahkamlash, ilg‘or texnologiyalarni rivojlantirish, yanada mustahkam me’yoriy-huquqiy hujjatlarni o‘rnatish va xususiy sektor bilan ishlashni o‘z ichiga olgan global sa’y-harakatlarni talab qiladi. Dunyo mamlakatlari ushbu jinoyatlarga qarshi kurashish bo‘yicha turli strategiyalarni amalga oshirmoqda va 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.

Yuqoridagilardan kelib chiqib quyidagi xulosalarga kelindi:

Darknet asosida sodir etiladigan jinoyatlar – bu transchegaraviy hisoblanadi. Shu sababli, davlatlar o‘rtasida o‘zaro ma’lumot almashish, jinoyat sodir etgan shaxslarni qidirib topish va ularni ekstraditsiya qilish kabi masalalarda o‘z ichiga olgan xalqaro hamkorlik shartnomasi tuzishlari maqsadga muvofiqdir;

Huquqni muhofaza qilish organlari hodimlarining zarur malakasi va tayyorgarligiga yetarlicha e’tibor berib, ularning qorong‘u tarmoq haqida xabardorligini oshirish, ya’ni huquqni muhofaza qilish organlarining tergov qilish vakolatiga ega bo‘lgan xodimlarning darknet tarmog‘ida tegishli dalillarni aniqlashga o‘rgatish va tergov usullarini takomillashtirish zarur;

Milliy jinoyat-protsessual qonunchiligimizga kiberjinoyatlarni tergov qilish va sudda javobgarlik masalasini aniq belgilab berishga xizmat qiladigan ishlar yuzasidan elektron dalillarni to‘plash, olib qo‘yish, tintuv qilish, ularning butunligi va yaxlitligini ta’minlash, sudda ko‘rib chiqish uchun taqdim etish tartibini aniq ko‘rsatuvchi qo‘shimchalar kirtish lozim deb hisoblaymiz.

FOYDALANILGAN ADABIYOTLAR:

1. Александров А. Г., Сафронов А. А.,. Криминалистика; судебно-экспертная деятельность; оперативно-розыскная деятельность. Использование сети Даркнет при подготовке и совершении преступлений. – 2021;

2. Sudakova T. M., Nomokonov V. A. Understanding the future of criminolo-gy: an overview of current trends. Vserossiiskii kriminologicheskii zhurnal / Russian Journal of Criminology, 2018, vol. 12, no. 4, pp. 531–540. DOI: 10.17150/2500-4255.2018.12(4).531-540;

3. Commission Recommendation (EU) 2017/1584 of 13 September 2017 on coordinated response to large-scale cybersecurity incidents and crises C/2017/6100;

4. Kevin Poulsen, “FBI Admits It Controlled Tor Servers Behind Mass Malware Attack,” Wired.com, September 13, 2013.

REFERENCES

1. Александров А. Г., Сафронов А. А.,. Криминалистика; судебно-экспертная деятельность; оперативно-розыскная деятельность. Использование сети Даркнет при подготовке и совершении преступлений. – 2021;

2. Sudakova T. M., Nomokonov V. A. Understanding the future of criminolo-gy: an overview of current trends. Vserossiiskii kriminologicheskii zhurnal / Russian Journal of Criminology, 2018, vol. 12, no. 4, pp. 531–540. DOI: 10.17150/2500-4255.2018.12(4).531-540;

3. Commission Recommendation (EU) 2017/1584 of 13 September 2017 on coordinated response to large-scale cybersecurity incidents and crises C/2017/6100;

4. Kevin Poulsen, “FBI Admits It Controlled Tor Servers Behind Mass Malware Attack,” Wired.com, September 13, 2013.