

ӨӨЖ 343.9
DOI 10.56525/RLOX3761

ДАРКНЕТТИ ҚҰҚЫҚТЫҚ РЕТТЕУДІҢ МӘСЕЛЕЛЕРІ

***З.Т. МЕДЕУБЕК
А.М. АБДУХАИМОВА
Л.Р. АСИЛБЕКОВА**

Орталық-Азия
инновациялық университеті
Шымкент қ., Қазақстан

***Корреспондент авторы: medeubek.z@mail.ru**

Аңдатпа. Бұл мақаланың негізгі мақсаты - интернеттің көлеңкелі жағы-DarkNet сияқты заманауи интернеттің сегментіне қатысты негізгі аспектілерді зерттеу. Жұмыста көлеңкелі интернеттің түрлері, формалары, ерекшеліктері, жағымды және жағымсыз жақтары талданып, ашық интернетпен салыстыру жүргізілді. Анонимділіктің сипаттамалары зерттелді. Сонымен қатар мақалада Darknet-ті дұрыс пайдаланбау және теріс пайдалану туралы негізгі ойлар және ақпараттық қауіпсіздік әдістері ұсынылған.

Кілт сөздер: DarkNet, Интернет, TOR, көлеңкелі желі, BitCoin, криптовалюта, анонимділік, домен

Кіріспе. Соңғы жылдары әлемнің құқықтық жүйелері «жаңа» ортаға тап болды, оның қалыптасуына ақпараттық-коммуникациялық технологиялар үлкен әсер етті. Осыған байланысты дәстүрлі түрде «материалдық» түрде болған көптеген құқықтық қатынастар топтары киберкеңістікке ауысады. Кез-келген жоғары технология үш түрде қолданылуы бар: азаматтық, әскери және қылмыстық. Соңғысы бұл мәселені өте өзекті етеді.

Darknet-ке кіру TOR сияқты арнайы браузерлер арқылы жүзеге асырылады, ол бастапқыда АҚШ-тың әскери жобасы болды және кейінірек бүкіл әлемге таралды. Қазақстандықтар арасында даркнеттің сұранысы туралы ресми статистиканың деректері куәландырады, оған сәйкес 600 мыңнан астам отандастарымыз Тог браузерін пайдаланды [1, 56].

Darknet-тен басқа, deep web («терең желі») сияқты ұғым бар, ол сарапшылардың пікірінше жалпы Интернеттің 96% -99% құрайды. Сонымен қатар, Дүниежүзілік Желінің осы бөлігінде орналасқан іздеу жүйелерімен индекстелмегенімен, заңды және қауіпсіз болып табылады. Бұған медициналық карталар, ақылы контент, жабық форумдар және басқа да құпия деректер кіреді. Қараңғы желіге келетін болсақ, ол өз кезегінде тек «терең желінің» бір бөлігі ғана болып табылады және оның көлемінің шамамен 5% алады, алайда оның нақты пайыздық мөлшері белгісіз. Dark web - те ұсынылған құралдар мен қызметтердің ең танымал санаттарының бірі-DDoS шабуылдарын ұйымдастыру, бұзу, тыңшылық, клиенттік базаны ұрлау, корпоративті және жеке қаржылық ақпарат. Д. Бартлетт сонымен қатар Darknet-те порнографиялық мазмұнды орналастыру, қару сату, кісі өлтірушілерді жалдау, зияткерлік меншік құқығын бұзу, виртуалды валюта сияқты әлеуметтік қауіпті әрекеттерді көрініс табады. Сонымен қатар, Darknet, мысалы, қарым-қатынастың шығармашылық формаларын дамыту үшін сәтті қолданылады. Сондықтан, технологиялар емес, оларға қол жеткізу үшін пайдалануға болатын мақсаттар қылмыстық деп саналуы керек екендігіне ерекше назар аудару керек.

Материалдар мен зерттеу әдістері. Зерттеу жүргізу барысында диалектикалық, логикалық, жүйелік әдістер пайдаланылған.

Зерттеу нәтижелері. Осылайша, біз Darknet-ке тыйым салудың мүмкін еместігі мен қажетсіздігі туралы айтатын зерттеушілердің көзқарасымен келісеміз. Себебі, ол өздігінен емес тек пайдаланушылардың қылмыстық мақсаттарына байланысты қоғамдық қауіп-қатерге ие болатын құрал ретінде әрекет етеді. Бұдан басқа, мемлекеттер әлі де Darknet-ті пайдалануды толығымен бұғаттай алмайтыны анық, бұл осы желінің ерекшелігіне байланысты көптеген қиындықтардан туындайды. Сонымен қатар, қылмыстардың едәуір бөлігі дәстүрлі Интернетте де бар, бұл қараңғы желінің қылмыстық маңыздылығын асыра сілтегендерін көрсетеді. Біз осы саладағы одан әрі қызметтің ең дұрыс бағыты Darknet-тің қауіпті көріністерімен күресудің жаңа құқықтық және техникалық құралдарын әзірлеу болады деп санаймыз.

Darknet аудиториясының көбеюіне жаһандық локдаун мен жаңа коронавирустық инфекция да әсер етті. 2020 жылы бірнеше күн ішінде коронавирусқа байланысты 130 домен сатып алынды, олар заңсыз мақсаттарда пайдаланылуы мүмкін еді. Атап айтқанда, коронавирусқа қарсы «вакциналарды» сататын алаяқтар күшейе түсті. Қазақстан аумағында жүзеге асырылатындар Darknet-те қанша сатылым алатыны туралы ақпарат жоқ. Алғаш рет Darknet, атап айтқанда Tor, есірткінің 340-қа жуық түрі ұсынылған 2011 жылдан 2013 жылға дейін жұмыс істеген «Жібек жолы» деп аталатын заңсыз психотропты заттар саудасы бойынша анонимді алаңның қызметіне байланысты құқық қорғау органдарының назарын аударды. Жабылғаннан кейін сайтта көшірмелер пайда болды, олардың саны қазір жасырын желіде өсіп келеді.

Сонымен қатар, Darknet-те бәрі қарапайым Интернеттегідей ұйымдастырылған: жаңалықтар сайттары, базарлар, кез-келген тауарларды сататын сайттар бар. Негізгі айырмашылық - көптеген сайттар заңсыз әрекеттермен айналысады. Егер бұл жаңалықтар болса, онда олар тыйым салынған, тауарлар заңсыз немесе ұрланған, ал форумдарда адамның психикалық денсаулығына зиян келтіретін барлық нәрсе талқыланады.

Көлеңкелі желі пайдаланушыларға кез-келген талғамға арналған өнімдерді ұсынады: онда сіз кез-келген жоғары оқу орнының дипломын немесе кез-келген мемлекеттің түпнұсқа төлқұжатын сатып ала аласыз. Сондай - ақ, қазіргі уақытта адамдар, қару-жарақ, есірткі және психотроптық заттар сатылады. Сондай - ақ, кейбір сайттарда әртүрлі елдердің жалған вексельдерін, ал басқаларында сатып алу құнынан 2 есе арзан тұратын ұрланған техниканы сатып алуға болатындығын атап өткен жөн.

Даркнеттің белгілі бір артықшылықтары бар екені сөзсіз. Олар көп емес, себебі кемшіліктері барлық артықшылықтардан бірнеше есе көп. Darknet-тің жағымды жақтарына оның компьютерлік, желілік және ақпараттық қауіпсіздік туралы білімнің тұтас энциклопедиясы екенін жатқызуға болады.

Сондай-ақ, онда сандық қауіпсіздік тақырыбында хакерлер өзара байланысатын көптеген пайдалы форум ағындары бар. Бұл форумдар компьютерлік және ақпараттық қауіпсіздікті сақтауға мүдделі адамдар үшін мазмұнды және танымдық болуы мүмкін. Бағдарламалау саласындағы сарапшылар үшін кейде жаңа, креативті, жетілдірілген идеяларды білу қызықты. Алайда жасөспірімдердің мұндай ақпаратты заңсыз мақсатта пайдалану тенденциясын атап өткен жөн. Олардың құмарлығын, қызығушылығын және тыйым салынған барлық нәрсені білуге деген ұмтылысын, сондай-ақ олардың әрекеттері үшін жауап бере алмайтындығын ескере отырып, жасөспірімдер цифрлық және ақпараттық қауіпсіздікті сақтау жолдарын біле отырып, вирустық шабуылдармен азаматтардың жеке деректерін пайдалана отырып, олардың құқықтарына айтарлықтай зиян келтіруі мүмкін деп болжауға болады.

Қараңғы веб-сайттар көбінесе жалған Домен «onion» аймағында орналасқан және олардың атаулары шифрлау кілтінен өтіп, әріптер мен сандардың 16 таңбалы тіркесіміне ұқсайды. Мұндай сайттар виртуалды арнайы серверлерде жұмыс істейді, яғни олар өздері хостинг провайдерлері болып табылады. «Onion» аймағында сайт әкімшілерін анықтау қиын, сондықтан көбінесе «Darknet-те» өздерін қорғау үшін коммерциялық қызметпен айналысатын адамдар өздерін ықтимал проблемалардан немесе басқа мәселелерден қорғау

үшін ескі сайттардағы проблемаларды күтпестен жаңа сайттар ашады. Көптеген адамдар бұл ресурстарда толық анонимділікке ие болатынын түсініп, бұл мүмкіндікті жақсы ниетпен пайдалана бастайды. «DarkNet» дүкендері бір бағыттағы бизнес емес. Мұнда әртүрлі адамдар ресми нарықта табылмайтын «заңсыз» тауарлар мен қызметтерді сатады. Сарапшылардың пікірінше, Darknet дүкендері 100% алдын-ала төлеммен жұмыс істейді. Сауда-саттықты әділ ету үшін сайттар дилерлердің квоталары мен депозиттерін тоқтатады, үлкен көлемдегі мәмілелер кезінде әкімшілер кепілгер бола алады. Маркетплейс сайттарында сатушылар сатып алушыларға немесе «онлайн сайттарға» әр мәміледен комиссия төлейді [2, 36].

Сонымен қатар, «Darknet-те» ұсынылған іс-әрекеттермен қатар, мәмілелер жасауға, ақша төлеуге және жылыстатуға байланысты жаңа ақпараттық технологиялар пайда болды. Бұл жағдайда ең тиімді және қолайлы нәтижелердің бірі криптовалюталардың пайда болуы болды. Нәтижесінде жаңа заңсыз сауда алаңдары белсенді түрде құрыла бастады: сату және сатып алу қауіпсіз болды. Бұл фактор криптовалюталарды өңдеумен айналысатын алаңдар құпия деректерді жинауды білдірмейтіндігімен байланысты. Осылайша, криптовалюта Darknet алаңдарында өз қызметтерін ұсынатын барлық саудагерлердің құралына айналды. Алайда, соңғы уақытта BitCoin криптовалютасы маңызды рөл атқара бастады. Биткоин-бұл криптовалютаның бір түрі, операцияларды есепке алу үшін аттас бірлікті пайдаланатын пирингтік төлем жүйесі. Биткоиннің жұмыс істеуі және қорғалуы үшін криптографиялық әдістер қолданылады.

Биткоинді қолданған кезде транзакцияға қатысушылардың бір біріне қатысты ақпараты болмайды. Биткоиннің анонимділігі мен орталықсыздығын көбінесе мемлекеттер қауіп ретінде түсіндіреді, бұл оны қолданумен күресуге әкеледі. Дегенмен, ол тіпті тыйым салынған елдерде, соның ішінде «көлеңкелі желілерде» есептеу үшін қолданылады. Биткоинді кеңінен қолданудың негізгі себептерінің бірі-алаяқтық және үзілген операциялардан автоматты түрде қорғалған есептеулердің бұрын-соңды болмаған сенімділігі. Bitcoin артықшылығы-ол бұрын-соңды болмаған анонимділік пен төлемнің өтуін қадағаламауды қамтамасыз ететін кез-келген мемлекетке немесе белгілі бір банкке байланысты болмауында. Жүйеде кез-келген әкімшілік орталық немесе әкімшіліктендірілген түйін жоқ, сондықтан транзакциялар туралы қысқаша мәлімет жинау қиын, сонымен қатар жүйенің жоғары трансшекаралық сипатына байланысты кез-келген мемлекеттің юрисдикциясы мұндай төлемдерді бақылауға таралуы екіталай.

Алайда, бұл ретте «Darknet» қылмыстық мақсатта пайдаланылатын Интернет желісінің жалғыз ресурсы емес екенін атап өткен жөн. Дүниежүзілік Желінің заманауи ресурстары, ашық Интернет, көптеген артықшылықтар мен ерекшеліктерге ие, олар арқылы қылмыс өркендейді.

Мәселен, сарапшылардың пікірінше, қарапайым Интернет желісінде қарапайым адамдар мен қылмыскерлер келесі артықшылықтарды пайдаланады:

Біріншіден, Интернет ғаламдық трансшекаралық сипатқа ие, бұл желінің архитектурасынан туындайды. Бұл оның түрлері мен санаттарына қарамастан бүкіл интернет-қылмыстың дамуы мен өсуіне ықпал етеді. Интернет әлемдегі кез-келген елдің аумағында басқа мемлекеттегі үй компьютерінен көптеген әлеуметтік қауіпті әрекеттерді жасауға мүмкіндік береді. Сонымен қатар, жаһандық желі халықаралық ұйымдасқан қылмыстық топтар мен қауымдастықтардың жасалған қылмыс түріне қарамастан кооперациясы мен шоғырлануына ықпал етеді.

Екіншіден, интернеттехнологияның принциптерінің бірі-анонимділік, бұл бірінші кезекте алаяқтық пен алдаудың барлық түрлеріне артықшылықтар береді. Анонимділік кез келген сипаттағы ақпаратты қылмыстық немесе басқа жауапкершілікке тартылу қаупі аз етіп жариялауға мүмкіндік береді. Анонимділік қылмыстық ақпаратты орналастыруда артықшылықтар беріп қана қоймайды, сонымен қатар оған сұраныстың артуына әсер етеді. Интернеттің анонимділігі азғындық, қоғамға қарсы және қылмыстық сипаттағы ақпаратқа тұрақты сұранысты қалыптастыруға ықпал етеді.

Үшіншіден, ғаламтор Ғаламдық аудиторияға жету үшін үлкен әлеуетке ие, бұл зардап шеккендердің саны бойынша бұрын-соңды болмаған қылмыстар жасауға мүмкіндік береді. Интернетті қылмыс жасау үшін пайдалану көбінесе келтірілген зиянды бірнеше есе арттыруға және ұзақ уақыт бойы пайда болатын жағымсыз салдарға әкеледі, бұл әдеттегі әлеуметтік қауіпті әрекеттермен салыстыруға келмейді.

Төртіншіден, қылмысқа қарсы күрестегі және интернет кеңістігін құқықтық реттеудегі қиындықтар жаһандық желіні пайдаланатын қылмыскерлерге белгілі бір артықшылықтар береді, желінің негізгі түйіндерінің таралуын және олардың өзара алмастырылуын тудырады [1, 36].

Қорытынды. Жоғарыда айтылғандарға сүйене отырып, біз Darknet қылмыстық жауапкершілікке тартылған және қылмыстық заңдарды бұзатын көптеген ресурстарды қамтиды деген қорытындыға келеміз. Оның кейбір авторлар Қазақстанның ұлттық қауіпсіздігіне қатер ретінде бағалайды. Тәжірибелі заңгерлермен және ғалымдармен байланысты заң шығарушының маңызды міндеттерінің бірі қазіргі заманға сәйкес нормативтік құқықтық актілер мен Darknet-ке қылмысқа қарсы тұру әдістерін әзірлеу болып табылады. Сонымен, ҚР құқық қорғау органдары мен атқарушы билік органдарының жұмысы, оның ішінде біз осы бапта ұсынған тәсілдермен жетілдірілуге тиіс.

Осылайша, бұл құбылыстың әлеуметтік қауіптілігі айқын және алдын-алу жұмыстарының тиімділігін арттыруды талап етеді. Қараңғыда қылмысқа қарсы іс-қимылды талдау киберқылмыспен күресудің негізгі әдістерін әзірлеуге және оларды өмірге сәтті енгізуге және қарапайым адамдарды заңсыз әрекеттерден қорғауға мүмкіндік береді. Бірақ ең бастысы - әр адамның жеке ақпараттық қауіпсіздігі, егер адам тек мемлекет пен оның құқық қорғау, бақылау органдарына ғана емес, сонымен бірге өздері де құқықбұзушылыққа әрекет жасамауы керек.

ӘДЕБИЕТТЕР

[1]. Узденов Р. М. «Новые границы киберпреступности» // Всероссийский криминологический журнал. 2016.

[2]. Свищёв А. В., Лаухина А.С. «Darknet: полезный инструмент или источник угрозы» // Colloquium-journal. 2020

REFERENCES

[1]. Uzdenov R. M. «Novyye granitsy kiberprestupnosti» // Vserossiyskiy kriminologicheskiy zhurnal. 2016.

[2]. Svishchov A. V., Laukhina A.S. «Darknet: poleznyy instrument ili istochnik угрозы» // Colloquium-journal. 2020

Медеубек З.Т.

магистр права, старший преподаватель

Абдухаимова А.М.

магистр права, преподаватель

Асилбекова Л.Р. преподаватель

Инновационный университет Центральной Азии, Казахстан Шымкент.

ВОПРОСЫ ПРАВОВОГО РЕГУЛИРОВАНИЯ ДАРКНЕТА

Аннотация. Основной целью данной статьи является изучение основных аспектов, касающихся такого сегмента современного Интернета, как черная сторона Интернета - DarkNet. В работе проанализированы виды, формы, особенности, положительные и отрицательные стороны Даркнета, а также проведено сравнение с открытым Интернетом. Исследованы характеристики анонимности. Кроме этого в статье выяснены основные моменты, касающиеся неправомерности использования и отрицательных особенностей DarkNet и предложены способы информационной безопасности.

Ключевые слова: DarkNet, Интернет, TOR, темная сеть, BitCoin, криптовалюта, анонимность, домен

Medeubek Z.T.

Master of Laws, Senior Lecturer

Abdukhaïmova A.M.

Master of Law, Senior Lecturer

Asilbekova L.R., teacher

Innovative University of Central Asia, Kazakhstan Shymkent.

ISSUES OF LEGAL REGULATION OF THE DARKNET

Abstract. The main purpose of this article is to study the main aspects related to such a segment of the modern Internet as the black side of the Internet - DarkNet. The paper analyzes the types, forms, features, positive and negative sides of the Darknet, as well as a comparison with the open Internet. The characteristics of anonymity are investigated. In addition, the article clarifies the main points regarding the misuse and negative features of the DarkNet and suggests ways of information security.

Key words: DarkNet, Internet, TOR, BitCoin, cryptocurrency