Шукан А.

Ақпараттық технологиялар саласындағы қылмыстармен күрес мәселесі

Қазіргі уақытта ақпараттық технологиялар мен коммуникация, байланыс саласындағы технологиялардың адам айтқысыз жылдам дамуы, террористік, экстремистік ұйымдардың, қылмыскерлердің әрекетін арттыру белсенді түрде пайдаланылуда.

Мақалада аталған мәселемен күрес жолдары мен тәсілдері қарастырылған. Сонымен қатар аталған қылмыстардың алдын алу мәселелері де қарастырылған.

Түйін сөздер: ақпараттық технологиялар, зиянкес бағдарламалар, электронды ақпарат.

Shukan A.

Problems of fighting crime in the sphere of information technologies

A serious problem is the use of telecommunications by terrorists and other antisocial extremist organizations.Agitation, so for the collection, transfer funds, and coordinate their actions in an Internet page.

This article discusses the above-mentioned problems of crime control in the field of information technology.As well as methods of dealing with IT crime.

Key words: information technology,virus programs, electronic information.

Шукан А.

Проблемы борьбы с преступностью в сфере информационных технологий

Серьезной проблемой остается использование телекоммуникаций террористами и иными антисоциальными экстремистскими организациями. Агитации, так для сбора, перевода денежных средств, и координации своих акций в страницах интернета.

В этой статье рассматривается вышеуказанные проблемы борьбы с преступностью в сфере информационных технологии. Атакжемето дыборьбысИТпреступности.

Ключевые слова: информационные технологий, вирусные прораммы, электронная информация.

ӘОЖ 343

Шукан А.

Қазақстан Гуманитарлық Заң университеті,
Қазақстан Республикасы, Астана қ.
E-mail: alia_shukan@mail.ru

АҚПАРАТТЫҚ ТЕХНОЛОГИЯЛАР САЛАСЫНДАҒЫ ҚЫЛМЫСТАРМЕН КҮРЕС МӘСЕЛЕСІ

Қазіргі әлем қоғамдастығының ақпараттық серпіліс дәуіріне аяқ басқандығына бәріміз куә болудамыз, себебі заманауи өркениет адам қызметінің барлық салаларында дерлік қолданылатын жаңа телекоммуникациялық технологияларға тікелей бағынышты. Олар азаматтардың өмір салтын, олардың қарым-қатынас жасау тәсілін де өте қатты өзгеріске ұшыратты. Алайда мұндай прогрестің қоғам үшін жағымсыз жақтары да жоқ емес – азаматтардың конституциялық құқықтары мен бостандықтарын қорғау, соның ішінде жеке өмірін қорғау сияқты тұлғалардың ажырамас құқығы сияқты ұғымдар ақпараттандыру саласы үшін мәнсіз терминге айналды.

Қазіргі уақытта әлемдегі барлық мемлекеттердің, басқару органдарының, ұйымдардың, жеке тұлғалардың жаһандық ақпараттық электрондық желілерде, айналымдағы ақпаратқа, оның нақтылығына, қорғалғандығына, қауіпсіздігіне тікелей тәуелді екендігі жасырын емес. Сонымен қатар ақпараттық және желілік технологиялардың қоғамның барлық саласына кірігу даму процесінің бұдан әрі жалғасатыны да сөзсіз. дамыту ақпараттандыру саласында қылмыс түрлерінің артуына алып келді.

Сондықтан аталған саладағы қылмыс түрлерінің алдын алу, онымен күрес түрлері мен жолдарын қарастыру ақпараттық технологиялар саласындағы қоғам қауіпсіздігін сақтау үшін аса маңызды екені анық.

Киберқылмыскерлер қоғамның барлық желілеріне кіруге, оның басқаруды өз қолдарына алуға немесе желілердегі ақпараттық алмасуды жоюға мүмкіндік беретін шабуылдардың көптеген түрлерін қолдануда. Вирустық бағдарламалар, соның ішінде ақпаратты өзгертетін және жойып жеберетін немесе есептеу жүйелерінің жұмысын шектейтін желілік құрттар, белгілі жағдайларда іске қосылатын логикалық бомбалар, өз «қожайынына» интернет арқылы бұзылған компьютерден, электронды ақпараттық құралдардан әртүрлі ақпаратты жіберетін «троян аттары» - мұның бәрі ақпараттық шабуылдың негізгі сипаттарына жатады.

Ақпараттық технологиялар саласындағы қылмыстардың алдын алуда төмендегі аспектілердің маңызының аса жоғары екендігін атап айтқымыз келеді.

Құқықтық
Моральді-этикалық
Ұйымдастырушылық қызметтер

Ақпараттық технологиялар саласындағы қылмыстардың алдын алудың құқықтық шараларына халықаралық заң нормалары (әсіресе ақпараттық технологиялар саласындағы қылмыстардың алдын алуда аса маңызды), мемлекет ішіндегі қолданыстағы заңнамалар (ақпараттық технологияларға қатысты қылмыстарды жазалауды және алдын алуды көздейтін), нормативті актілер (азаматтардың ақпаратты қолдану құқығы мен міндеттерін және ақпараттық технология саласындағы негізгі міндеттерді бұзған жағдайдағы жауапкершілік түрлерін анықтауға бағытталған).

Диссертациялық жұмысымыздың бірінші тарауында біз Түркия және басқа да елдердің ақпараттық технология саласындағы қылмыстарға байланысты заңнамаларын қарастырған болатынбыз. Сондықтан бұл бөлімде ақпараттық технологиялар саласындағы қылмыстарға байланысты қабылданған басқа елдердің заңнамаларына да көз жүгіртіп өтуді жөн деп таптық.

Ақпараттық технологиялар саласындағы қылмыстарды жауапкершілікке тартатын алғашқы заңнама 1978 жылы Аризона мен Флорида штаттарында қабылданған болатын. Заңнама «Computer crıme act of 1978» (1978 жылғы компьютерлік қылмыс актісі) деп аталды. Аталған заңнамадағы ақпараттық технологиялар саласындағы қылмыстардың жазасы аса қатал болды. Мысалы, біреудің жекеменшігіне қол сұғу мақсатында ақпаратқа заңсыз ену және өзгерту әрекеті 15 жылға бас бостандығынан айырумен және он мың доллар көлеміндегі штраф төленумен жазаланды. Бұл қабылданған заңнама негізінде АҚШ-тың барлық штаттарында ақпараттық технология саласындағы қылмыстарды жазалауға бағытталған заңнамалар қабылданды. Бұл заңнаманың қабылдануы Америка Құрама Штаттарында ғана емес барлық әлемде АТ саласындағы қылмыстармен күресудің басты шарттарын қалыптастырды.

Аталған салаға қатысты заң шығару шаралары ТМД елдері арасында Ресей Федерациясы тарапынан белсенді іске асырылғандығын атап айтуымыз керек. Ресей Федерациясы өз Қылмыстық кодексінде «компьютерлік ақпарат саласындағы қылмыстар» атты жаңа тарау енгізумен қатар, ақпараттық технология саласындағы электронды ақпаратты өңдеу мен аталған саладағы азаматтардың, мекемелердің, мемлекеттің міндеттері мен құқықтарын анықтайтын базалық актілер қабылдады. Сонымен қатар «Ақпарат, ақпараттандыру және ақпаратты қорғау» мен «Қауіпсіздік жайында» атты заңнамалар да қабылданды.

Ақпараттық технология саласындағы қылмыстардың алдын алуға бағытталып, қабылданған отандық заңнамадағы қылмыстық-құқықтық нормалар АТ саласындағы қылмыстармен күресте аса маңызды рөл атқаратындығын айта кеткеніміз жөн.

Электронды ақпаратты қорғауды реттеу мақсатында қабылданған алғашқы базалық актілердің біріне Қазақстан Республикасы Үкіметінің «Ақпаратты қорғаудың ұлттық стандарттарының қорғалу тәртібі атты» қаулысы болды (3 шілде 1998 жыл) және «Ақпараттық жүйелердің, техникалық, бағдарламалық-техникалық және бағдарламалық құралдардың (бұйымдардың), ақпаратты қорғаудың техникалық құралдарының ақпараттық қауіпсіздік талаптарына сәйкестігін растау жөніндегі Нұсқаулығын бекіту туралы«(Қазақстан Республикасы Премьер-Министрінің Кеңсесі басшысының 2013 жылғы 14 маусымдағы № 25-1-21 бұйрығы). «Қазақстан Республикасы ақпараттық қауіпсіздігінің 2016 жылға дейінгі тұжырымдамасы туралы«(Қазақстан Республикасы Президентінің 2011 жылғы 14 қарашадағы № 174 Жарлығы) [1]. Аталған заңдық актілер мен жарлықтар еліміз-дегі ақпараттық технологиялар саласындағы ақпаратты қорғауға байланысты механизімдерді реттеуші негізгі құжаттар болып есептеледі. Ақпараттық технологиялар саласындағы қауіп-сіздікке байланысты назар аударатын келесі бір құжат ол Елбасы Нұрсұлтан Әбішұлы Назарбаевтың «Қазақстан – 2050» бағдарламасы. Елбасы аталған халыққа Жолдауында, XIX ғасырдың негізгі он қауіп қатерінің жетіншісі деп – Үшінші индустриялық революцияны атаған болатын, әрі ақпараттық технологиялар саласындағы қауіпсіздікті қамтамасыз ету жол-дары да айқын көрсетілген [2].

Ақпараттық технологиялар саласындағы қылмыстармен тиімді күресудің және алдын алудың келесі бір құқықтық шарасы ол құқық қорғау органдарындағы арнайы мамандардың кәсібилік мәселесі болып табылады. Қазіргі уақытта Қазақстанда ақпараттық технологиялар саласындағы қылмыстардың алдын алу және күресуге бағытталған «CERTkz» және Ішкі істер министірлігіне қарайтын «К» бөлімі.

«К» бөлімі Ішкі істер министірінің бұйрығымен 2004 жылы ішкіістер министірлігінің құрамында құрылған ұйым. Аталған ұйым ақпараттық технологиялар саласындағы келесі қылмыс түрлерімен күресуге бағытталған;

Ақпараттық технология жадысындағы, электронды төлем желісіндегі, ақпараттарға заңсыз ену және көшіру.

Заңсыз радиоэлектронды құралдарды сату және айналымға енгізу

Телкоммуникация, ұялы байланыс және желі арқылы жасалатын қылмыстар.

4. Заңсыз ақпарат көздерімен, порнография, балалар порнографиясы және т.б. ақпараттарды электронды желілер арқылы заңсыз таратумен күресу [3].

Байланыс және ақпарат агенттігі негізінде құрылған «CERTkz» ұйымы Қазақстанда 2011 жылы компьютерлік инциденттерге әрекет ету жөніндегі арнайы қызмет көрсету ұйымы ретінде ұйымдастырылды.

KZ-CERTайналысады:

1. Мемлекеттік органдардың компьютерлік қауіпсіздік бөлімшелерінің, байланыс операторларының, сондай-ақ компьютерлік және ақпараттық технологияларды пайдалану саласындағы құқық бұзушылықтардың алдын алу мәселелері бойынша ұлттық ақпараттық инфрақұрылымның басқа да субъектілерінің әрекеттерін үйлестірумен;

2. Компьютерлік қауіпсіздіктің қазіргі қатерлері туралы және қолданылатын байланыс құралдарының тиімділігі туралы ақпараттарды жинаумен, талдаумен және жинақтаумен [4].

Соңғы он жылда Қазақстан аумағында жоғарыда аталған екі ұйымның құрылғанына қарамастан, қазіргі уақытта Қазақстан зиянкес бағдарламалар шабуылына ұшыраудан әлемде екінші орын алуда, сонымен бірге соңғы уақыттарда елімізде смс хабарламалар арқылы жалған ақпараттар тарату мен порнография, балалар порнографиясы, интернет арқылы таратылатын террористік хабарламалар, басқа да қоғамның рухани азғындауына әсер ететін интернет сайттар ешқандай тосқауылсыз елімізде белсенді жұмыс істеуде екендігі барлығымызға мәлім. Демек Қазақстандық құқық қорғау органдарында ақпараттық қауіпсіздікке байланысты жұмыс атқаратын орган қызметкерлерінің кәсібилігі мен тәжірибесін арттыратын арнайы оқу орны мен басқа Еуропа т.б. елдер қызметкерлерімен тәжірибе алмасу шаралары қолға алыну қажет. Себебі қазіргі ақпараттық қоғамда, ақпараттық қауіпсіздікті сақтау, қоғам қауіпсіздігін сақтаудың ең басты алғышарты болып табылады. Егер арнайы құқық қорғау ұйымдары ақпараттық қауіпсіздікті қорғаумен кәсіби түрде айналыспаған жағдайда еліміздің барлық ақпараттық электронды желілері (электронды үкімет, білім беру, денсаулық сақтау, әскери және банк желілері мен т.б. қоғамдық электронды желілер) ақпараттық технологиялар саласы шабуылдардың астында қалатыны анық. Қазірдің өзінде еліміздің вирустық шабуылдар қарқыны жағынан әлемде екінші орын алуы сөзімізге айқын дәлел бола алады.

Ақпараттық технологиялар саласындағы қылмыстармен күрестің моральдық – этикалық қыры құқықтық нормалар сияқты міндетті принциптерден тұрмайтынын ескергеніміз жөн. Алайда ақпараттық технологиялар саласындағы қылмыстармен күресте маңызды роль атқаратындағын да атап айтқымыз келеді.

Моральдық-этикалық түсініктер арқылы қоғамдағы ақпараттық технологияларды дұрыс мақсатта пайдалану тәртібін қалыптастыруға болады деп есептейміз. Мысалы, медицина, құқық, экономика т.б. салаларда мұндай этикалық нормалардың қалыптасып үлгергендігі барлығымызға мәлім.

Электронды ақпараттық ортада мұндай этикалық нормалар түсінігін қалыптастыру ақпараттық технологиялар саласындағы қылмыстармен күресіп қана қоймайды сонымен қатар қоғамда белгілі түрде ақпараттық технологиялар мен ондағы ақпаратты пайдалану мәдениетін де қалыптастырады деп есептейміз.

Электронды ақпаратты пайдаланудың моральдық этикасын қалыптастырудың жолы біз білім беруде деп есептейміз. Мысалы, әлемнің көптеген елдерінде ақпараттық технологиялар мен ондағы ақпаратты пайдалану этикасы немесе тәртібі атты пәндер бастауыш сыныптардан бастап мектеп қабырғасын аяқтағанға дейін өтетінін ескерсек. Біздің қоғамымызға да аталған үрдісті енгізу әр бір тұлғаның, мекеменің қызметкерлерінің арасында белгілі бір деңгейде ақпаратты пайдаланудың этикалық мәдениетін, дәстүрін қалыптастыруға себепкер болатын анық.

Ақпараттық технологиялар саласындағы қылмыстардың алдын алудың келесі бір қыры ол ұйымдастырушылық шаралар. Қазіргі ақпараттық технологиялар саласындағы белсенді қылмыстық әрекеттерден қорғанудың келесі тәсілі ретінде ұйымдастырушылық шараларды атап айтқымыз келеді. Әр бір ұйымда әсіресе банк, білім беру, медицина, электронды үкіметке қатысты мекемелерде ақпараттық технологиялар саласындағы қылмыстық шабуылдардан қорғауға бағытталған арнайы персоналдық кадрлердің міндетті түрде болуын біз осы аспектіге жатқызамыз.

Аталған персоналдық қызметкерлер төмендегі міндеттерді атқаруы қажет:

ақпараттық жүйені қорғаудың жалпы талаптарын қалыптастыру;

ақпаратты қорғаудың маңызды, негізгі бағыттарын анықтау;

электронды жүйені бақылауда ұстап, оның әлсіз тұстарын анық білу және оны жетілдіру;

ақпараттық жүйені қолданушылардың қауіпсіздік талаптарын орындауын бақылауда ұстау.

Мекемелердегі ақпараттық технологиялар саласындағы қауіпсіздікті сақтауға байланысты қызметкерлерді төмендегі талаптарға сәйкес қабылдау тиімді деп есептейміз.

Ақпараттық технологиялар жүйесінің қауіпсіздігіне жауап беруші маман ай сайын ақпараттық технологиялар саласындағы қылмыстардан қорғанысқа байланысты шыққан жаңа бағдарламалар мен стандарттарға мониторинг жасап, мекемеге тиімдісін іріктеу және оны енгізу жұмыстарын жүргізуі тиіс.

Ақпараттық технологиялар жадысындағы, желісіндегі мәліметтердің рұқсатсыз өзгермеуін, сақталуын қадағалаушы маман.

Басқарушы маман мекеменің ақпараттық техникалық желісінің, жүйесінің толыққанды қауіпсіз режимде жұмыс істеуі мен қорғаныста болуын қамтамасыз етуші, бақылаушы және ұйымдастырушы.

Әрине жоғарыда аталған шаралардың барлығы ақпараттық технологиялар саласындағы түрлі қылмыстарға қарсы толыққанды нәтиже береді деп айта алмаймыз, ол мүмкін емес. Алайда жоғарыда аталған қорғаныс шаралары қоғамда кешенді түрде атқарылған жағдайда еліміздің электронды ақпараттық желісіндегі мәліметтерді вирустардан, спамдар мен рұқсатсыз жалған ақпараттардың таратылуынан қорғау деңгейі белгілі бір түрде артатыны сөзсіз деп есептейміз.

Ақпараттық технология саласындағы қауіпсіздікті қамтамасыз ету мәселелерінің трансшекаралық сипатын ескере отырып, осы салада тең құқықтық халықаралық ақпарат алмасу қағидаттарына сай келетін халықаралық ынтымақтастықты жетілдіру қажет деп есептейміз.

Жаһандық ақпараттық инфрақұрылымды пайдалану, ақпараттық және телекоммуникациялық технологияларды террористік және басқа да қылмыстар мақсатында пайдаланудың алдын алу, анықтау, жолын кесу және салдарын жою саласындағы Қазақстан Республикасының және шет елдердің құқық қорғау органдарының арасындағы өзара іс-қимылды жетілдіру саласында мемлекетаралық қатынастарды реттейтін халықаралық құқықтық нормаларды әзірлеу осы саладағы стандарттар мен сертификаттаудың ұлттық жүйесін халықаралық жүйемен үндестіру талап етіледі.

Ұйымдастырушылық – өкімдік және ұйымдастырушылық – техникалық қамтамасыз ету бағыты бойынша ақпараттандырудың аса маңызды объектілерінің ақпараттық қауіпсіздігін қамтамасыз ету, ақпараттық қауіпсіздік саласында, оның ішінде ақпаратты қорғаудың жүйесі саласында біртұтас мемлекеттік техникалық саясатты қамтамасыз ету жөніндегі іс-шаралар кешенін іске асыру талап етіледі. Осы мәселені шешу үшін ақпараттық кеңістік мониторингінің біртұтас мемлекеттік жүйесін құру, ақпараттық қауіпсіздікті қамтамасыз етудің жедел орталығының ақпараттық жүйесін және инфрақұрылымын құру талап етіледі. Сонымен қатар мемлекеттік органдардың бірыңғай ақпараттық-коммуникациялық желі-сін жетілдіру, ақпараттық технологиялар саласындағы аса маңызды инфрақұрылымды қорғау үшін ақпараттық қауіпсіздікті қамтамасыз етудің жедел орталығын құру, мемлекеттік органдар үшін бірыңғай электрондық пошта жүйесін дамыту, мемлекеттік органдардың резервтік деректер қорын сақтаудың кемінде екі аумақтық ажыратылған орталығын құру, Қазақстан Республикасының киберкеңістігінде ұлттық сәйкестендіру жүйесін дамыту, киберқауіпсіздік торапта-рын құру, «электрондық үкіметтің» ақпараттық қауіпсіздігін қамтамасыз ету жүйелерінің рұқсат етілмеген қол жеткізуді, ақпаратты жоғалтуды, бұрмалауды болдырмауға бағытталған сапасы мен сенімділігін арттыру талап етіледі.

Интернеттің жаһандық ақпараттық желісінің қазақстандық сегментін дамыту мен реттеудің оңтайлы моделі енгізіледі, жағымды мазмұндағы контент өндірісін, отандық интернет – БАҚ-ты дамытуды, телекоммуникациялық инфрақұрылымды жаңғыртуды ынталандыру тетіктері әзірленетін болады.

Осы іс-шаралардың іске асырылуы үшін елдің имиджін ілгерілету мақсатында, Қазақстандық БАҚ-тың Орталық Азия мен халықаралық ақпараттық кеңістікте қатысуын күшейтуге бағытталған. Бұдан басқа ғылымды, технологияларды және техниканы дамытудың басым бағыттары бойынша зерттеу жобаларын жүргізу саласындағы халықаралық ынтымақтастық дамитын болады.

Кадрмен қамтамасыз ету бағыты бойынша ақпараттық қауіпсіздікті қамтамасыз ету және мемлекеттік құпияларды қорғау саласындағы кадрлар даярлау жүйесін жетілдіру, құқық

қорғау органдарының, оның ішінде ақпараттық терроризмге және ақпараттық қылмысқа қарсы іс-қимыл мәселелерімен айналысатын бөлімшелерін кадрмен қамтамасыз ету мәселелерін шешу талап етіледі. Ақпараттық қауіпсіздік және мемлекеттік құпияларды қорғау мәселелері бойынша оқу және білім беру бағдарламаларының тиімділігін арттыру мәселесі өте маңызды.

Жоғарыда айтылған ойларды қорытындылай келе төмендегідей қорытынды жасауға болады:

Біз жүргізген зерттеудің талдауы ақпараттық технологиялық құралдардың өзіне, жүйесіне немесе желісіне қашықтықтан қол жеткізу тәсілі белгілі, қашықтықта орналасқан ақпа-раттық құралға (желілік сервермен) және он-дағы ақпаратпен жанама байланыс орнатуды білдіретінін көрсетті. Мұндай байланыс жер-гілікті немесе жаһандық ақпараттық құралдар желісінің, басқа байланыс құралдары арқылы жүзеге асырылуы мүмкін. Бір ғана ақпараттық технология жүйесі шегінде жүзеге асырылатын әдеттегі (тікелей қол жеткізу) желілік жүйелермен қатар кеңістіктегі ресурстар мен ақпараттың таралуымен шарттастырылған шабуылдардың ерекше түрі қолданылады – олар желілік (немесе алыстағы) шабуылдар деп аталады (remote немесе network attacks). Шабуылдардың бұл түрі кибертеррористерге үлкен мүмкіндік беретін қару ретінде айтарлықтай қауіпті құрал болып есептеледі [5]. Мұндай шабуыл ретінде әдетте байланыс каналдары бойынша бағдарламалық жүзеге асырылатын бөлінген есептеу жүйесіне ақпараттық бүлдіруші әсер ету түсініледі. Мысалы, сындарлы инфрақұрылымның басқару жүйесіне осылайша немесе ядролық реактормен әсер ету нәтижелері зардабы жағынан жаһандық мәндегі апаттың сипатына ие болуы мүмкін.

Ақпараттандыру саласындағы қылмыстылықпен күрес мәселесін бүгінде терроризммен және ұйымдасқан қылмыспен бір деңгейде тіпті одан да қауіпті деп қарастыруға болады. Бұл ретте бұл мәселені халықаралық деңгейде шешуде кешенді тәсілді жүзеге асыру қажет. Әрі Қазақстан да аталған қылмыс түрімен күресуде мол тәжірибиесі бар мемлекеттермен бірлесе қызмет атқаруы қажет.

Киберқылмыс түрлерімен жалпы электронды ақпаратты ортада жасалатын жаңа қылмыс түрімен тиімді күресу үшін, жаһандық киберполиция ұйымын құру қажет, себебі аталған қылмыспен әр мемлекеттің жеке-жеке күресуінің аса тиімсіз екендігін ғалымдар атап айтуда [6].

Кедендік Одақ, ТМД, Қазақстан Республикасындағы ақпараттық технологиялар саласындағы қылмыстармен күрес шаралары халықаралық әріптестікке тығыз негізделуі қажет. Әсіресе Еуропа Киберқылмыстармен күрес Конвенциясын ратификациялау тиімді нәтижелерге қол жеткізуге септігін тигізеді.

Сонымен қатар ТМД арасында және басқа да Еуропа мемлекеттері заңнамаларында қарастырылған, ақпараттық технологиялар саласындағы қылмыстарға байланысты, қылмыстық-құқықтық нормалар мен қылмыстық заңнамалар үйлесімділігі және мемлекет ішіндегі аталған мәселеге байланысты заңнамалар арасында ұғымдық үйлесімділікті іске асыру қажет.

Ақпараттық технологиялар саласындағы қылмыстармен күресте оның алдын алуда жоғарыда көрсетілген құқықтық, моральдық-этикалық,ұйымдастырушылық аспектілерін комплексті қолдану шаралары да белгілі бір тиімді нәтижеге әкеледі деп есептейміз.

Әдебиеттер

1 http://adilet.zan.kz/kaz/search/docs/fulltext.
2 http://www.centrasia.ru/newsA.php?st=1084834920.
3 http://kz-cert.kz/kz/.
4 Shlapp M.G. behavior and Gland Disease// Journal of HeridATe. –1924. № 15.–P. 11-14.
5 Спасович В.Д. Избранные труды и речи / сост. И.В. Потапчук. – Тула: Автограф, 2000. –302 с.
6 Астафьев К.В. Виктимологический аспект мошенничества: уголовно– правовое и криминологическое исследование: автореферат канд. юрид. наук. – Казань, 2007. – с. 35.

References

1 http://adilet.zan.kz/kaz/search/docs/fulltext.
2 http://www.centrasia.ru/newsA.php?st=1084834920.
3 http://kz-cert.kz/kz/.
4 Shlapp M.G. behavior and Gland Disease// Journal of HeridATe. – 1924. № 15.–P. 11-14.
5 Spasovich VD Selected Works and speech / comp. IV Potapchuk. – Tula: Autograph, 2000. – 302 p.
6 Astafev K. Viktimology aspect of fraud: criminal legal and criminological research: the author's PhD. jurid. Sciences. – Kazan, 2007. – 35 p.