ҚАЗАҚСТАН РЕСПУБЛИКАСЫНЫҢ ІШКІ ІСТЕР МИНИСТРЛІГІ
010000, Астана қ., Тәуелсіздік даңғылы, 1
электрондық мекенжай: kense@mvd.kz

МИНИСТЕРСТВО ВНУТРЕННИХ ДЕЛ РЕСПУБЛИКИ КАЗАХСТАН
010000, г. Астана, проспект Тәуелсіздік, 1
электронный адрес: kense@mvd.kz

20___ж._____ №_____

_____ Мына
на №_____

№ исх: 1-3-6-43/2914-Д от: 13.11.2017

Қазақстан Республикасы
Парламенті Мәжілісінің
депутаттары
М. Махамбетовке, С. Ахметовке,
С. Қаныбековке, Б. Мәкенге,
В. Олейникке

2017 жылғы 25 қазандағы
№ДЗ-256 депутаттық сауалға

Құрметті депутаттар!

Сіздің сұрау салуыңызға сәйкес киберқылмысқа қарсы іс-қимыл жасасу бойынша жүргізілген жұмыстарға қатысты ақпарат жолдаймыз.

Қосымша: ____ парақта.

Құрметпен,

Министр **Қ. Қасымов**

15.11.2017 Копия электронного документа.

орын.: Р.Дүйсетаев
тел.: 72-22-37

Депутатам
Мажилиса Парламента
Республики Казахстан
М. Махамбетову, С. Ахметову,
С. Каныбекову, Б. Макену,
В. Олейнику

На депутатский запрос
от 25 октября 2017 года
№ДЗ-256

Уважаемые депутаты!

Согласно Вашего запроса направляем информацию касательно проводимой работы по противодействию киберпреступности.

Приложение: ____ листов.

С уважением,

Министр **К. Касымов**

Исп.: Р.Дюсетаев
тел.: 72-22-37

№ исх: 1-3-6-43/2914-Д от: 13.11.2017

Қосымша

Ішкі істер министрлігі өз құзыреті шегінде киберқылмысқа қарсы іс-қимыл жасасу бойынша тапсырмаларды жүзеге асырады. Көрсетілген саладағы қылмыстық құқық бұзушылық Қазақстан Республикасы ҚК-нің 7-тарауында *(Ақпараттандыру және байланыс саласындағы құқық бұзушылықтар)* көзделген.

Статистикалық мәліметтерге сәйкес 2015 жылы ҚК-нің 7-тарауы бойынша 128 құқық бұзушылық тіркелген *(ашылғаны – 12, тергеу мерзімдерінің үзілгені 37 іс бойынша)*, 2016 жылы тіркелгені – 113 *(ашылғаны – 13, тергеу мерзімдерінің үзілгені 27 істер бойынша)*.

Ағымдағы жылғы 10 айда 83 қылмыстық құқық бұзушылық тіркелген, ашылғаны – 6, ашылмай қалғаны – 19.

Одан басқа, Қылмыстық кодексте құқық бұзушылықтар құрамының бірқатарында ақпараттық технологияларды пайдалануды қарастыратын саралау белгілері бар *(интернет-алаяқтық, ақпараттық технологияларды пайдалану арқылы жасалатын ұрлық және т.б.)*.

Осы құқық бұзушылықтардың көп бөлігін интернет пайдаланушыларға қатысты жасалған алаяқтық құрайды.

Мәселен, 2015 жылы тіркелген интернет-алаяқтықтың 45-тен, ашылғаны – 7, мерзімдері үзілгені 25 іс бойынша, 2016 жылы жасалғаны – 1046, ашылғаны – 24, ашылмағаны – 916.

Ағымдағы жылғы 10 айда осы алаяқтықтың 1694 тіркелген, аяқталғаны – 129, тергеу мерзімдері үзілгені 1259 істер бойынша.

Сонымен қатар, ағымдағы жылы ҚК-нің 190-бабы 4-тармағы, 2-бөлігі бойынша тіркелген құқық бұзушылықтарға жасалған талдаудың көрсеткені, Интернет желісін пайдаланушыларына қатысты алаяқтық 1694 жағдайдың тек 875-де жасалған.

Анықтама ретінде: *875 интернет-алаяқтықтың 596-сы ашылмай қалды, оның ішінде:*

- *тауарларды сату туралы жарнамаларды сайттарға орналастыру жолымен – 63/436;*
- *қызмет ұсыну туралы жарнамаларды сайттарға орналастыру жолымен – 48/22;*
- *әлеуметтік инженериялар әдістерін қолдана отырып, азаматтардың дербес мәліметтерін алып және ары қарай банктік (пластикалық) есеп-шоттардан не микро кредиттерді рәсімдеу арқылы ақшаларды ұрлау – 141/108;*
- *жалған парақшаларды пайдалану жолымен әлеуметтік желілердің пайдаланушыларына қатысты (материалдық көмек көрсету туралы өтініш) – 56/30 қылмыстар.*

Қалған 819 тіркелген алаяқтықтың интернетті қолданумен жасалмаған және оның басқа түрлері болып келеді. Негізінен көпшілігі жалған ұтысты, туысқанды полиция ұстау не бас тәсілдерді желеулетіп жасалған телефондық алаяқтық. Оларды жасауда қылмыскерлер өздерін білдірмеуді қамтамасыз ету

мақсатында, электрондық төлеу құралдарын пайдаланады *(төлем карталары, Qiwi-кошелектер және т.б.)*.

Қарастырылып отырған қылмыстарды анықтау және ашу бойынша жұмыстың оң тәжірибесі бар.

- *2011 жылы Петропавл қаласында жалған пластикалық төлем карточкаларды пайдалану жолымен «Цеснабанк» АҚ-ға **14 млн. теңгеден** астам залал келтірген Германияның азаматы ұсталды.*
- *2013 жылы Алматы қаласында «Халық банк» және «Жинақбанк» АҚ банкоматтарына «скиммингтік құралдарды» (пластикалық карталардан ақпаратты көшіру үшін банкоматтарға орналастырылатын қолдан жасалған құрылғылар) орналастырып ұрлық жасаған екі топ (Болгария және Румыния азаматтары) ұсталды. Келтірілген залал **– 8 млн. теңгеден** астам.*
- *2013-14 жылдарда вирусты және қашықтан банктік қызмет көрсету жүйесін пайдалану жолымен ұйымдардың банктік шоттарынан ірі ақша сомаларының ұрлықтары тергелді. Көрсетілген қылмыстарды жасағаны үшін Қазақстан Республикасының азаматтары ұсталды, олар 2011 жылдан бастап 2013 жылға дейінгі мерзімде бухгалтерлердің компьютерлеріне құқыққа сыйымсыз енуді жүзеге асырған және 40-тан астам компаниялардың шоттарынан **500 млн. теңге** ұрлаған.*
- *2016 жылы шілде айында аурудан азап шегуші балаға материалдық көмек беруді желеулетіп, Петропавл қаласы тұрғынының банктік шотына рұқсат алған және 7 млн. теңге ақшасын ұрлаған, интернет-алаяқ ұсталды. Тергеу нәтижелері бойынша ол 3,6 жылға бас бостандығынан айыру арқылы сотталды.*

Ағымдағы жылғы қазан айында жедел-іздестіру іс-шараларын жүргізу арқылы «Колеса.кз» сайтында жалған жарнамаларды орналастыру жолымен *(автобөлшектерді әкелуді желеулетіп, автобөлу)* интернет-алаяқтықты жасаған Қостанай қаласының екі тұрғыны ұсталды.

Жалдамалы пәтерге тінтуді жүргізу барысында қылмысты жасау үшін қолданылған айғақ заттар *(15 ұялы телефон, 13 СИМ-карта, 2 ноутбук, 9 пластикалық карта және т.б.)* алынды.

Қазіргі уақытта оларға Қазақстанның жеті өңіріндегі тұрғындарына қатысты 34 алаяқтық жасағаны үшін айып тағылды. Осыған ұқсас ашылмаған қылмыстарға қатыстылығын анықтау бойынша жұмыстар ары қарай жүргізілуде.

Интернет-пайдаланушылардың құқыққа қайшы ақпараттарды орналастыру фактілерін анықтау мақсатында Интернет желісіне тұрақты түрде мониторинг жүргізіледі. Шетел пайдаланушылары не ресурстары анықталған жағдайда, оларды бұғаттауға шаралар қабылданады.

Өткен жылы ішкі істер органдары құқыққа қайшы 1419 шетел ресурстары анықталды, оның ішінде экстремистік сипатта – 703, есірткі бизнесіне қарсы әрекет жасасу желісі бойынша – 402, порнографияларды

тарату бойынша ресурстар – 259, лицензиясыз бағдарламалар бойынша – 53, улы заттарды дайындау бойынша – 2.

Ағымдағы жыл басынан бастап құқыққа қайшы 1007 интернет-ресурстар анықталды *(порнографиялық материалдарды тарату бойынша 413, экстремистік материалдар 349, әлеуметтік желілерде суицидті насихаттайтын 171 материал және 74 контрафактілік өнімдерді тарататын сайттар).*

Интернет желісіне Қазақстандық пайдаланушылардың енуін бұғаттау бойынша шаралар қабылдау үшін олар туралы ақпарат Ақпарат және коммуникациялар министрлігіне жолданды.

«Блокчейн» технологиясын ендіруге қатысты бөлігінде, қазіргі уақытта Қазақстан Республикасында «криптовалюталарды» дамыту мен пайдалануға қатысты мәселе заңнама түрінде реттелмеген.

Ішкі істер министрлігі криптовалютталарды ендіруге, пайдалануға, айналдыруға, оның ішінде «Эфириум» технологиясына қатысты әлемдік тәжірибені зерделеуде.

<u>Анықтама ретінде:</u>

«Эфириум» (Ethereum) – GPU қуаттылығында «Эфириум» майнингінің көмегімен көптеген операцияларды бағдарламалы орындауы мүмкін алгоритмді құруға мүмкіндік беретін технология. Ақшалай қаражаттар мен операцияларда ең тиімді және ыңғайлы болып келетін және орталықтандырылмаған майнингтік желіде негізделген блокчейнді құруға жасаушылардың әрекеті, «Эфириумның» негізі болып қосымшаларды әзірлеуге жол беретін Blockchain жатады.

Ақылды контрактілер немесе смарт-контрактілерді пайдаланудан тұратын «Эфириумнің» бірегей айырмашылығы бар. Жүйенің әрбір транзакциясы компьютерлік бағдарламаны пайдаланумен жүзеге асырылады. Ол келісім шарттарын және жіберуші мен алушы арасында міндеттемені орындауды тексереді. Барлық пункттердің орындалуын адамдар емес, машиналар қадағалайды, ол адалдықты және біреуге тартпаушылықты қамтамасыз етеді. Осылайша «ақылды контракттіні» айналып өту немесе жою мүмкін емес.

Ашық дереккөздерді мониторингілеу барысында «Ethereum» қоғамдастығында орын алған «токендерді» (монеталарды) ұрлау, фишингтік шабуылдардың көмегімен жасалған, онда «кошелектардың» иелері логиндер мен парольдерді өздері берген.

Сонымен қатар, елімізде «токендерді» не криптовалюталардың басқа түрлері бойынша ұрлық тіркелмеген.

Жалпы, киберқылмысқа қарсы іс-қимыл жасау бойынша тапсырмалар ішкі істер органдары жүйесінде Криминалдық полиция департаменті «К» басқармасы мен оның Астана, Алматы қалаларының және облыс орталықтарының құрылымдық бөліністеріне жүктелген.

Еліміз бойынша көрсетілген бөліністердің қызметкерлерінің штаттық саны 59 адам *(орталық аппарат – 13, «К» аумақтық бөліністерінде – 46 адам, оның ішінде Астана қаласын ІІД – КПБ «К» бөлінісі (5 адам), Алматы қаласы ІІД – КПБ «К» бөлімі (11 адам), Алматы облысы ІІД – КПБ «К» бөлімі (4 адам). Қалған ІІД «К» тобы 1-2 қызметкерлерден)*.

«К» бөліністері қызметкерлерінің жалпы санынан ІІО-да қызмет өтелімі: *3 жылға дейін* – 2, *3 жылдан 5 жылға дейін* – 3, *5 жылдан 10 жылға*

дейін – 12, *10 жылдан 15 жылға дейін* – 20, *15 жылдан жоғары* – 17 қызметкер.

Жоғары техникалық білім 9 қызметкерде бар *(ақпараттық жүйелер – 2, есептеу техникасы және бағдарламалық қамтамасыз ету – 3, радиотехника – 1, инженер-жүйетехнигі – 3).*

Тұрақты негізде біліктілікті арттыру курстары жүргізіледі. Көрсетілген бөліністердің қызметкерлері оқу курстарына шетелдік және отандық сарапшыларды шақырумен шетелдерде де, сондай-ақ Қазақстан Республикасы аумағында да қатысады.

ІІО «К» бөліністерінің қызметкерлері *(2-3 қызметкер бойынша)* 2012 жылдан бастап ҰҚШҰ-ға мүше мемлекеттерінің құқық қорғау, өртке қарсы, авариялық-құтқару және арнайы қызмет органдары үшін кадрларды дайындау туралы келісімді іске асыру шеңберінде Ресей ІІМ Воронеж институтында біліктілікті көтеру курстары өтеді.

Ресей тарапымен келісім бойынша сабақтар бағдарламасына киберқылмысты ашу *(жедел-іздестіру іс-шараларын жүргізу тактикасы, тәсілі),* киберқылмысты жасаудың жаңа тәсілдері туралы ақпараттандыру, мамандандырылған бағдарламалық қамтамасыз етулермен және жабдықтаулармен практикалық жұмыстар бойынша өзекті мәселелер қосылған.

Шетел мемлекеттердің құқық қорғау органдарымен уағдаластық бойынша Түркияда *(Түрік ұлттық полициясы – 2011 жылы)*, Қытайда *(Қоғамдық қауіпсіздік министрлігі, 2014 жылы – 15 қызметкер, 2015 жылы – 8, 2016 жылы – 15)* оқу курстары өткізілді.

ІІО қызметкерлері Астана қаласында 2012-2014 жылдары Қазақстан Республикасындағы АҚШ Елшілігі ұйымдастырған киберқылмысты анықтау, жолын кесу және ашу мәселелері жөніндегі Қазақстанның құқық қорғау және арнайы органдарына арналған оқу курстарына қатысты.

2015-2016 жылдары АҚШ Елшілігімен уағдаластық бойынша ІІО, Бас прокуратура, Әдмин *(сарапшы-мамандар)* және ҚМ *(МКК)* қызметкерлері үшін АҚШ Құпия қызметінің мамандарын тарта отырып, ІІМ Алматы академиясы базасында үш кезеңнен тұратын курстар жүргізілді.

2014 жылдан бастап жыл сайын ІІМ Алматы академиясында киберқылмысқа қарсы күрес желісі бойынша аумақтық бөліністер қызметкерлеріне арналған біліктілікті арттыру мамандандырылған курстары жүргізіледі.

Жалпы, әр бір аумақтық ІІД-нің *(Астана, Алматы қалалары және облыстар мен көліктегі)* қызметкерлері жыл сайын қарастырылып отырған желі бойынша біліктілікті арттыру курстарынан өтеді.

<u>Мемлекеттік органдармен және жеке секторлармен өзара іс-қимыл жасасу</u>

- 2016 жылы Қорғаныс және аэроғарыш өнеркәсібі министрлігі жанында ведомствоаралық жұмыс тобы құрылды, оның құрамы «Қазақстанның киберқалқаны» киберқауіпсіздіктің 2017-2020 жылдарға

арналған тұжырымдамасын *(бұдан әрі - Тұжырымдама)* әзірлеуге белсенді қатысты.

Анықтам ретінде: *Тұжырымдама «Қазақстанның Үшінші жаңғыруы: жаһандық бәсекеге қабілеттілік» Қазақстан Республикасы Президентінің Жолдауына сәйкес әзірленді.*

Тұжырымдаманы іске асыру жөніндегі іс-шаралар жоспарына шетелдік әлеуметтік желілер мен мессенджерлердің қазақстандық пайдаланушыларының қосылулары туралы мәліметтерге рұқсат алу туралы мәселелерді әзірлеу туралы ІІМ-нің ұсынысы қосылды.

Осы шара олардың серверлерін Қазақстан Республикасы аумағында орналастыруды немесе қазақстандық байланыс операторларымен келісімшарт жасауды ұйғарады.

Бұдан басқа, киберқауіпсіздік және цифрлық дәлелдемелерді зерттеу бойынша мамандарды оқыту, біліктілігін арттыру жөніндегі іс-шаралар қарастырылды.

•Ұлттық экономика министрлігінің *(бұдан әрі – ҰЭМ)* электрондық сауданы дамыту жөніндегі жұмыс тобының құрамына Криминалдық полиция департаменті «К» басқармасының қызметкерлері қосылған. Интернет-дүкендердің қызметіне, алаяқтық жасауды болдырмау бойынша шараларға қатысты тиісті ұсыныстар ҰЭМ-ге жолданды.

• Киберқылмыстарға қарсы іс-қимыл мәселелері бойынша Ұлттық қауіпсіздік комитетімен тұрақты түрде өзара іс-қимыл жасалады. Қазақстандық пайдаланушылардың қосылулары туралы мәліметтерді жедел алуды қамтамасыз ету мақсатында, ҰҚК-нің келісімімен отандық интернет-провайдерлердің *(оның ішінде ұялы байланыс операторлары)* IP-мекенжайларының тиесілігін тексеру бойынша арна алынды.

•Электрондық жымқыруға уақтылы ден қою мақсатында ақпаратпен жедел алмасу бойынша екінші деңгейдегі банктермен *(қауіпсіздік қызметтері)* өзара тығыз іс-қимыл жасалады.

Мәселен, 2015 жылы Астана қаласында Халық банкінің қауіпсіздік қызметімен өзара іс-қимыл жасасу кезінде Халық банкінің 90 клиентінің карточкаларынан «скиммингті құрылғыларды» пайдаланумен ақпарат ұрлаған Молдованың азаматтары ұсталды. Шығын 9 млн. тенгеден асады.

2016 жылғы наурызда «Казкоммерцбанктің» банкоматына скимингті құрылғы орнатқан және 51 клиенттің пластикті карточкасынан ақпарат ұрлаған Ақтөбе қаласының тұрғыны ұсталды.

Халықаралық ынтымақтастық

Әдеттегідей, киберқылмыстарды жасау кезінде шетелдік серверлер пайдаланылады, пайдаланушылар шетелдік сайттарда, әлеуметтік желілерде тіркеледі. Осыған байланысты халықаралық ынтымақтастықты дамытуға және нығайтуға көп көңіл бөлінеді.

• Шетелдердің құқық қорғау органдарымен жедел ақпарат алмасу үшін ІІМ-де 2007 жылдан бастап, ол 70-тен астам шет мемлекеттің киберқылмысқа қарсы күрес жөніндегі бөліністерімен өзара іс-қимылды *(бастамашылық*

хабарламалар, сұрау салулар) қамтамасыз ететін Ұлттық байланыс пункті *(бұдан әрі – ҰБП)* жұмыс істейді.

Осыған ұқсас басқа мемлекеттердің құқық қорғау органдарымен ақпарат алмасу КПД «К» басқармасына бөлінген Интерполдың ҰОБ-ның арналары арқылы жүзеге асырылады. Мәселен, 2016 жылы осы арна арқылы жасөспірімді азғындаған және Интернет желісінде балалар порнографиясын таратқан Ақтау қаласының тұрғынын әшкерелеген ақпарат алынды.

• ТМД-ға қатысушы мемлекеттердің ынтымақтастығы туралы нормативті актілердің бірқатарын жүзеге асыру шеңберінде ҰҚККБ арқылы киберқылмыстылыққа қарсы іс-қимыл мәселелері бойынша өзара іс-қимыл жасалады.

<u>Анықтама ретінде:</u>

2013 жылғы 25 қазанда ТМД-ға қатысушы мемлекеттердің басшылары кеңесінің шешімімен өңірде ынтымақтастықтың негізгі бағыттарын көздейтін ТМД-ға қатысушы мемлекеттердің ақпараттық технологияларды пайдалана отырып жасалатын қылмыстарға қарсы күрестегі ынтымақтастығының тұжырымдамасы қабылданды.

ТМД-ға қатысушы мемлекеттер басшыларының шешімімен 2016 жылғы 16 қыркүйекте Бішкек қаласында ақпараттық технологияларды пайдалана отырып жасалатын қылмыстарға қарсы күрестегі ынтымақтастықтың 2016-2020 жылдарға арналған бағдарламасы бектілді. Бағдарлама осы бағытта ынтымақтастықты нығайтуға бағытталған.

Қазіргі уақытта, ТМД-ға қатысушы мемлекеттермен ТМД-ға қатысушы мемлекеттердің ақпараттық технологиялар саласындағы қылмыстарға қарсы күрестегі ынтымақтастығы туралы келісімнің жобасын әзірленді (Мемлекет басшыларының қол қоюы 2018 жылы жоспарланды).

• Бірқатар ұйымдастырушылық-практикалық іс-шаралар 2013 жылғы 25 қазандағы ТМД мемлекеттерінің басшылары кеңесінің шешімімен бекітілген, Қылмысқа қарсы күрестің бірлескен шараларының 2014-2018 жылдарға арналған мемлекетаралық бағдарламасы шеңберінде жүргізілуде.

Мәселен, Бағдарламаның 2.1.13-тармағын орындау мақсатында ел аумағында жылына екі мәрте кең ауқымды киберқылмысқа, авторлық және сабақтас құқықтарды бұзушылыққа қарсы іс-қимылға бағытталған ауқымды жедел профилактикалық іс-шаралар жүргізіледі.

• Жыл сайын ақпараттық саладағы қылмыстық әрекеттерге қарсы іс-қимыл бойынша ҰҚШҰ-ға мүше мемлекеттермен өзара іс-қимыл жасасу туралы *(2014 жылғы 23 желтоқсанда қол қойылды, 2016 жылғы 28 наурызда ратификацияланды)* хаттаманы іске асыру шеңберінде тұрақты «Прокси» операциясын өткізуге қатысамыз *(операцияның Ұлттық штабы ҰҚК-де)*. Осы операция ақпараттық технологиялар *(соның ішінде конституциялық құрылыс және қауіпсіздік, бейбітшілік)* саласындағы қылмыстарға қарсы іс-қимылда арнайы және құқық қорғау органдарының өзара іс-қимыл жасасуды жақсартуға бағытталған.

• БҰҰ ЕҚБ бағдарламасы шеңберінде киберқылмыстылыққа қарсы іс-қимыл мәселелері бойынша халықаралық өңірлік семинарларға қатысады *(2013 жыл – Иран, Тегеран қаласы, 2015 жыл – Түркіменстан, Тәжікстан)*. Практикалық қызметкерлерге арналған ұқсас семинарларды ІІМ БҰҰ ЕҚБ

және ЕҚЫҰ-мен бірлесіп, 2015 және 2016 жылдары Алматы қаласында өткізді.

Проблемалық мәселелер

Киберқылмыстылыққа қарсы іс-қимыл жөніндегі іс-шаралар жүргізу барысында бірқатар проблемалық мәселелер туындайды.

- Ақпараттық технологияларды, онлайн-қызметтерді енгізу, компьютерлік құрылғылар мен гаджеттердің қолжетімділігі, сондай-ақ интернет желілерін пайдаланушылардың артуы киберқылмыстардың өсуіне, оларды жасаудың жаңа тәсілдерінің пайда болуына әкеледі.

Осындай құқық бұзушылықтарды тергеп-тексеру басқа «дәстүрлі» қылмыстарды тергеп-тексеруден айтарлықтай ерекшеленеді және қызметкерлерден бастапқы жұмыстарды сауатты жүргізуді, жедел талдауды, қылмыстың мүмкін құралдары – заттар мен құжаттарды *(бағдарламалар, деректер базалары, жеке файлдар мен басқа электронды құжаттар және т.б.)* қарауды және зерделеуді талап етеді.

Технологиялардың тұрақты дамуын және киберқылмыстарды жасаудың жаңа тәсілдерінің пайда болуын ескеріп, қызметкерлердің білім деңгейін және кәсіби шеберлігін тұрақты арттыру қажет.

- Компьютерлік техниканы және басқа ақпарат тасымалдаушыларды зерттеудің *(сараптамаға)* сапасына осы салада сот сарапшыларының жетіспеушілігі, әртүрлі тасмалдаушылардан ақпаратты оқуға арналған құрылғыларды *(оның ішінде қолдан жасалған)* зерттеу әдістемелерінің шалағайлығы әсер етеді. Сот сарапшыларының тасымалдағышта зиянкес бағдарламаның болуы немесе оның арналуы туралы сұрақтарға жауап бере алмайтын жағдайлар орын алады *(дербес деректерді ұрлау, қашықтықтан рұқсат және т.б.)*.

Мысалы, 2013 жылы Астана қаласында ұсталған Молдова азаматтарынан алынған шиммингтік құрылғылар *(пластикалық карточкадан ақпаратты жасырын оқуға арналған қолдан жасалған құрылғы)* алынды. Сараптама тағайындау кезінде Астана қаласы ӘдМ-нің Сот сараптамасының орталық институтынан (ССЗО) оларды зерттеу әдістемесінің болмауы туралы жауап алынды. Зерттеулердің жеке түрлері бойынша ұқсас проблемалар іс жүзінде барлық облыстық ӘдМ Сот сараптамасының орталық институттарында бар.

Осыған байланысты, компьютерлік қылмыстарды ашу бойынша жұмыстың тиімділігін арттыру үшін өңірлерде электрондық ақпаратты тасымалдағыштарды зерттеуге мамандандырылған сарапшылардың санын жүргізілетін зерттеулердің шеңберін кеңейте отырып арттыру қажет.

- Ең қиын проблема әлеуметтік желілерді, мессенджерлерді *(Facebook, Twitter, В контакте, одноклассники, WhatsApp, Viber, Line және т.б.)* және басқа шетелдік интернет-ресурстарды, оның ішінде құқыққа қайшы ақпарат *(порнография, экстремистік сипаттағы материалдар, ұлтаралық және басқа да алауыздықты тудыратын белгілері бар пікірлер және т.б.)* тарату үшін пайдалану болып табылады.

Шетелдің әлеуметтік желілері *(негізінен ресейлік және американдық)* үлкен танымалдылыққа ие, бұл интернет-ресурстардың әртүріне бақылаусыз енуге

әкеп соғады. Оларды пайдаланушылар жалған парақшалар, аккаунттар тіркеп, өздерін жиі жасырады.

Оларда тіркелген қазақстандық пайдаланушылар туралы қажет мәліметтерді *(тіркеу деректері, телефон нөмірлері, IP-мекенжайлар және т.б.)* алу үшін сұрау салу жолдау қажет. Бұл ретте, сұрау салу немесе халықаралық тергеу тапсырмалары ұзақ уақыт орындалады, бұл ІІО қызметкерлерінің жедел іс-қимылын қамтамасыз етпейді не өзінің өзектілігін жоғалтады *(телефон, компьютер иесінің ауысуы, ақпараттың жойылуы және т.б.)*.

Анықтама ретінде: *«Дербес деректер және оларды қорғау туралы» Қазақстан Республикасының Заңына 2016 жылдан бастап, онда дербес деректерді сақтауды меншік иесі және (немесе) оператор, сондай-ақ үшінші тұлға Қазақстан Республикасының аумағында орналасқан базаларда сақтауды көздейтін (көрсетілген Заңның 12-бабы, 2-тармағы), яғни Қазақстанда әлеуметтік желілердің, мессенджерлердің серверлеріне ие болуға міндеттейтін өзгерістер енгізілді. Алайда, осы шара қазіргі уақытта жұмыс істемейді және қосымша пысықтауды талап етеді.*

Шетелдік ресурстарды (сайттар, сілтемелер және т.б.) анықтау кезінде оларды бұғаттауға шаралар қолданылады.

Анықтама ретінде: *2016 жылы Интернет желісіне мониторинг барысында 1419 шетелдік заңға қайшы ресурс, ағымдағы жылдың басынан 1007 құқыққа қайшы интернет-ресурс (413 порнографияны тарату бойынша, 349 экстремистік материал, әлеуметтік желілерде өз-өзіне қол жұмсауды насихаттайтын 171 материал, контрафактілік өнімдерді тарататын 74 сайт) анықталды.*

- Жымқыру жасау кезінде қылмыскерлер электрондық төлем құралдарын жиі қолданады *(Qiwi-әмиян және т.б.)*. Әдеттегідей, оларды тіркеу үшін көбінесе «әмиянды» құру үшін тек бір рет қана пайдаланылатын SIM-картаның *(бір реттік нөмір)* болуы жеткілікті. Бұл ретте, сауалнамалық деректерді немесе басқа бекітілген мәліметтерді ұсынудың қажеті жоқ *(Шетелдік байланыс операторларының абоненттік нөмірлері арқылы құрылған «әмияндерді» пайдалану жағдайлары бар)*.

Бұдан басқа, Байланыс қызметтерін көрсету қағидаларының *(Қазақстан Республикасы Инвестициялар және даму министрінің 2015 жылғы 24 ақпандағы № 171 бұйрығымен бекітілген)* 19-тармағында абоненттік нөмірлер иелерін міндетті тіркеу көзделген. Алайда, абоненттік нөмірлерді делдалдарға не бөгде адамдарға тіркеу фактілері орын алады.

Осыған байланысты, «электрондық әмиян» иесін абоненттік нөмірмен байланыстырудан басқа міндетті сәйкестендіруді *(авторизация)* көздейтін норманы *(қағиданы)* бекіту туралы мәселені пысықтау мақсатқа сай деп ұйғарылады.

Баяндалғанды ескере отырып, қазіргі уақытта ІІМ киберқылмыстылыққа қарсы іс-қимыл бойынша жұмыстың тиімділігін арттыруға қажетті шараларды қабылдауда. Осы бағыт басым болып табылады және бақылауда.

Ішкі істер министрлігі

№ исх: 1-3-6-43/2914-Д от: 13.11.2017

Приложение

Министерство внутренних дел в пределах своей компетенции осуществляет задачи по противодействию киберпреступности. Уголовные правонарушения в указанной сфере предусмотрены Главой 7 УК Республики Казахстан *(Уголовные правонарушения в сфере информатизации и связи)*.

Согласно статистическим данным в 2015 году по Главе 7 УК зарегистрировано 128 правонарушений *(раскрыто – 12, прерваны сроки расследования по 37 делам)*, в 2016 году зарегистрировано – 113, *(раскрыто – 13, прерваны сроки расследования по 27 делам).*

За 10 месяцев т.г. зарегистрировано 83 уголовных правонарушения, раскрыто – 6, остаются нераскрытыми – 19.

Кроме того, в Уголовном кодексе ряд составов правонарушений содержит квалифицирующий признак, предусматривающий использование информационных технологий *(интернет-мошенничества, кражи с использованием информационных технологий и т.д.).*

Большую часть таких правонарушений составляют мошенничества, совершенные в отношении интернет-пользователей.

Так, в 2015 году из 45 зарегистрированных интернет-мошенничеств раскрыто – 7, прерваны сроки по 25 делам, в 2016 году совершено – 1046, раскрыты- 24, нераскрыты- 916.

За 10 месяцев т.г. зарегистрировано 1694 мошенничеств, окончено – 129, прерваны сроки расследования по 1259 делам.

Вместе с тем, проведенный анализ зарегистрированных в т.г. правонарушений по п.4, ч.2 ст.190 УК показывает, что лишь в 875 из 1694 случаев имеет место совершение мошенничества в отношении пользователя сети Интернет.

Справочно: *из 875 остались нераскрытыми 596 интернет-мошенничеств, в т.ч.:*

- *путем размещения на сайтах объявлений о продаже товаров- 63/436;*
- *путем размещения на сайтах объявлений о предоставлении услуг- 48/22;*
- *с применением методов социальной инженерии, с завладением персональных данных граждан и последующим хищением денег с банковских (пластиковых) счетов либо оформлением микрокредитов- 141/108;*
- *в отношении пользователей социальных сетей путем использования подложных страниц (просьба об оказании материальной помощи) – 56/30 преступлений,*

Остальные 819 зарегистрированных мошенничеств не совершались с использованием интернета и представляют собой другие ее виды. В основной массе это телефонные мошенничества, совершенные под предлогом мнимого выигрыша, задержания полицией родственника либо совершенные другим способом. При их совершении, в целях обеспечения своей анонимности, преступники использовали электронные средства оплаты *(платежные карты, Qiwi-кошельки и т.д.)*.

Имеется положительный опыт работы по выявлению и раскрытию рассматриваемых преступлений.

- *В 2011 году в г.Петропавловске задержан гражданин Германии, который путем использования поддельных пластиковых платежных карт нанес ущерб АО «Цеснабанк» свыше* ***14 млн. тенге.***
- *В 2013 году в г. Алматы задержаны две группы (граждане Болгарии и Румынии), которые, установив «скимминговые устройства» устройства кустарного производства, устанавливаемые на банкоматы для копирования информации с пластиковых карт) совершили кражи из банкоматов АО «Народный банк» и «Сбербанк». Ущерб – свыше* ***8 млн. тенге.***
- *В 2013-14 гг. расследовался ряд хищений крупных сумм денег с банковских счетов организаций путем использования вируса и системы дистанционного банковского обслуживания. За совершение указанных преступлений задержаны граждане Республики Казахстан, которые в период с 2011 до 2013 годы осуществили неправомерный доступ к компьютерам бухгалтеров и похитили* ***500 млн. тенге*** *со счетов более 40 компаний.*
- *В июле 2016г. задержан интернет-мошенник, который под предлогом перечисления материальной помощи страдающему от болезни ребенку, получил доступ к банковскому счету жительницы г.Петропавловска и похитил* ***7 млн. тенге****. По результатам расследования он осужден к 3,6 годам лишения свободы*

В октябре т.г. при проведении оперативно-розыскных мероприятий задержаны два жителя г.Костанай, которые совершали интернет-мошенничества путем размещения ложных объявлений на сайте «Колеса.кз» *(под предлогом поставки автозапчастей, авторазбор)*.

В ходе проведения обысков на съемных квартирах изъяты вещественные доказательства *(15 сотовых телефонов, 13 СИМ-карт, 2 ноутбука, 9 пластиковых карт и т.д.)*, которые использовались для совершения преступлений.

В настоящее время им вменяется совершение 34 мошенничеств в отношении жителей семи регионов Казахстана. Проводится дальнейшая работа по установлению причастности к аналогичным нераскрытым преступлениям.

В целях выявления фактов размещения интернет-пользователями противозаконной информации на постоянной основе проводится мониторинг сети Интернет. В случае установления зарубежных пользователей либо ресурсов, принимаются меры к их блокированию.

За прошлый год органами внутренних дел выявлено 1419 зарубежных противозаконных ресурсов, в т.ч. 703 – экстремистского характера, 402 – по линии противодействия наркобизнесу, 259 – ресурсов по распространению порнографии, 53 – по нелицензионным программам, 2 – по изготовлению ядовитых веществ.

С начала т.г. всего выявлено 1007 противоправных интернет-ресурсов *(413 по распространению порнографических, 349 экстремистских материалов, 171 материал, пропагандирующих суицид в соц.сетях и 74 сайтов, распространяющих контрафактную продукцию)*.

Информация о них направлена в Министерство информации и коммуникации для принятия мер по блокированию доступа казахстанским пользователям сети Интернет.

В части, касающейся внедрения технологий «блокчейн», в настоящее время в Республике Казахстан вопросы, касающиеся развития и использования «криптовалют» законодательно не урегулированы.

Министерством внутренних дел изучается мировой опыт, касающийся внедрения, использования, оборота криптовалют, в т.ч. технологии «Эфириум».

Справочно:

«Эфириум» (Ethereum) – технология которая позволяет создать алгоритм, с которым множество операций может быть выполнено программно, с помощью майнинга «Эфириума» на GPU мощностях. Это попытка разработчиков создать блокчейн, который был бы наиболее эффективным и удобным при операциях с денежными средствами и основана на децентрализованной майнинговой сети, основой «Эфириума» является Blockchain, который позволяет разрабатывать приложения.

«Эфириум» обладает уникальным отличием, которое заключается в использовании умных контрактов или смарт-контрактов. Каждая транзакция системы осуществляется с использованием компьютерной программы. Она проверяет условия сделки и выполнение обязательств между отправителем и получателем. Поскольку за соблюдением всех пунктов следят не люди, а машины, это обеспечивает честность и беспристрастность. Таким образом, «умный контракт» невозможно обойти или отменить.

В ходе мониторинга открытых источников установлено, что имевшие место хищения «токенов» (монет) сообщества «Ethereum» совершены при помощи фишинговых атак, где владельцы «кошельков» сами выдали свои логины и пароли.

Вместе с тем, по стране хищений «токенов» либо других видов криптовалют не зарегистрировано.

В-целом, задачи по противодействию киберпреступности в системе органов внутренних дел возложены на Управление «К» Департамента криминальной полиции и его структурные подразделения в г.г.Астана, Алматы и областных центрах.

Штатная численность сотрудников указанных подразделений по стране составляет 59 единиц *(центральный аппарат – 13, в территориальных подразделениях «К» – 46 единиц, в т.ч. ДВД г. Астаны – отделение «К» УКП (5 ед.), ДВД г. Алматы – отдел «К» УКП (11 ед.), ДВД Алматинской обл. – отдел «К» УКП (4 ед.). В остальных ДВД группы «К» по 1-2 сотрудника).*

Из общего количества сотрудников подразделений «К» имеют стаж службы в ОВД: *до 3 лет* – 2, *от 3 до 5 лет* – 3, *от 5 до 10 лет* – 12, *от 10 до 15* лет – 20, *свыше 15 лет* – 17 сотрудников.

Высшее техническое образование имеют 9 сотрудников *(информационные системы-2, вычислительная техника и программное обеспечение- 3, радиотехника- 1, инженер-системотехник- 3)*.

На постоянной основе проводятся курсы повышения квалификации. Сотрудники указанных подразделений принимают участие на обучающих курсах как за рубежом, так и на территории Республики Казахстан с приглашением зарубежных и отечественных экспертов.

В рамках реализации Соглашения о подготовке кадров для правоохранительных, противопожарных, аварийно-спасательных органов и специальных служб государств-членов ОДКБ ежегодно с 2012 года сотрудники подразделений «К» ОВД *(по 2-3 сотрудника)* проходят курсы повышения квалификации в Воронежском институте МВД России.

По согласованию с российской стороной, в программу занятий включены актуальные вопросы по раскрытию киберпреступлений *(тактика, методика проведения оперативно-розыскных мероприятий)*, информирование о новых способах совершения киберпреступлений, практические работы со специализированным программным обеспечением и оборудованием.

По договоренности с правоохранительными органами зарубежных стран проведены обучающие курсы в Турции *(Турецкая национальная полиция – в 2011 году)*, Китае *(Министерство общественной безопасности, в 2014 году – 15 сотрудников, в 2015 году – 8, в 2016 году – 15)*.

В 2012-2014 годы в г. Астане сотрудники ОВД принимали участие на обучающих курсах, организованных Посольством США в Республики Казахстан для правоохранительных и специальных органов Казахстана по вопросам выявления, пресечения и раскрытия киберпреступлений.

В 2015-2016 годы по договоренности с Посольством США в три этапа на базе Алматинской академии МВД проведены курсы с привлечением специалистов Секретной службы США для сотрудников ОВД, Генеральной прокуратуры, Минюста *(специалисты-эксперты)* и МФ *(КГД)*.

Ежегодно с 2014 года в Алматинской академии МВД проводятся специализированные курсы повышения квалификации для сотрудников территориальных подразделений по линии борьбы с киберпреступностью.

В целом, ежегодно курсы повышения квалификации по рассматриваемой линии проходят сотрудники каждого территориального ДВД *(г.г. Астаны, Алматы и областей и на транспорте)*.

<u>Взаимодействие с госорганами и частным сектором</u>

- В 2016 году при Министерстве оборонной и аэрокосмической промышленности создана межведомственная рабочая группа, в составе которой принято активное участие в разработке Концепции кибербезопасности «Киберщит Казахстана» на 2017-2020 годы *(далее – Концепция)*.

Справочно: *Концепция разработана в соответствии с Посланием Президента Республики Казахстан «Третья модернизация Казахстана: Глобальная конкурентоспособность».*

В План мероприятий по реализации Концепции включено предложение МВД о проработке вопроса о получении доступа к сведениям о соединениях казахстанских пользователей зарубежных социальных сетей и мессенджеров.

Данная мера предполагает размещение их серверов на территории Республики Казахстан либо заключение договоров с казахстанскими операторами связи.

Кроме того, предусмотрены мероприятия по обучению, повышению квалификации специалистов по кибербезопасности и исследованию цифровых доказательств

• В состав рабочей группы Министерства национальной экономики *(далее – МНЭ)* по развитию электронной торговли включены сотрудники Управления «К» Департамента криминальной полиции. Соответствующие предложения касательно деятельности интернет-магазинов, мер по предотвращению совершения мошенничеств, направлены в МНЭ.

• На постоянной основе осуществляется взаимодействие с Комитетом национальной безопасности по вопросам противодействия киберпреступлениям. В целях обеспечения оперативности получения сведений о соединениях казахстанских пользователей, по согласованию с КНБ получен канал по проверке принадлежности IP-адресов отечественных интернет-провайдеров (в т.ч. операторов сотовой связи).

• Осуществляется тесное взаимодействие с банками второго уровня *(службы безопасности)* по оперативному обмену информацией в целях своевременного реагирования на электронные хищения.

Так, в 2015 году в г.Астане во взаимодействии со службой безопасности Народного банка задержаны граждане Молдавии, которые с использованием «скимминговых устройств» похитили информацию с карточек 90 клиентов Народного банка. Ущерб составил свыше 9 млн. тенге.

В марте 2016г. задержан житель г.Актобе, который установил скимминговое устройство на банкомат «Казкоммерцбанка» и похитил информацию с пластиковых карточек 51 клиента.

Международное сотрудничество

Как правило, при совершении киберпреступлений используются зарубежные сервера, пользователи регистрируются на зарубежных сайтах, социальных сетях. В этой связи большое внимание уделяется развитию и укреплению международного сотрудничества.

• Для обмена оперативной информацией с правоохранительными органами зарубежных стран в МВД с 2007 года функционирует Национальный контактный пункт *(далее – НКП)*, позволяющий осуществлять

взаимодействие *(инициативные сообщения, запросы)* с подразделениями по борьбе с киберпреступностью более чем 70 иностранных государств.

Аналогичный обмен информацией с правоохранительными органами других государств осуществляется по отдельному каналу НЦБ Интерпола, выделенному Управлению «К» ДКП. Так, в 2016 году посредством данного канала получена информация, позволившая изобличить жителя г.Актау в развращении малолетней и распространении в сети Интернет детской порнографии.

• В рамках реализации ряда нормативных актов о сотрудничестве государств – участников СНГ, через БКБОП осуществляется взаимодействие по вопросам противодействия киберпреступности.

Справочно:

25 октября 2013 года Решением Совета Глав государств-участников СНГ принята Концепция сотрудничества государств-участников СНГ в борьбе с преступлениями, совершаемыми с использованием информационных технологий, предусматривающая основные направления сотрудничества в регионе.

16 сентября 2016 года решением Совета Глав государств – участников СНГ в г.Бишкек утверждена Программа сотрудничества в борьбе с преступлениями, совершаемыми с использованием информационных технологий на 2016-2020 гг.. Программа направлена на укрепление сотрудничества в данном направлении.

В настоящее время государствами – участниками СНГ проработан проект Соглашения о сотрудничестве государств-участников СНГ в борьбе с преступлениями в сфере информационных технологий (планируется к подписанию Главами государств в 2018 г.).

• Ряд организационных и практических мероприятий проводится в рамках Межгосударственной программы совместных мер борьбы с преступностью на 2014-2018 годы, утвержденной Решением Совета Глав государств СНГ от 25.10.2013 года.

Так, во исполнение п.2.1.13 Программы дважды в год на территории страны проводятся широкомасштабные оперативно-профилактические мероприятия, направленные на противодействие киберпреступности, нарушениям авторских и смежных прав.

• Ежегодно, в рамках реализации Протокола о взаимодействии государств-членов ОДКБ по противодействию преступной деятельности в информационной сфере *(подписан 23.12.2014г, ратифицирован 28.03.2016г.)*, принимается участие в проведении постоянной операции «Прокси» *(Национальный штаб операции в КНБ)*. Данная операция постоянного действия и направлена на улучшение взаимодействия специальных и правоохранительных органов в противодействии преступлениям в сфере информационных технологий *(в т.ч. против основ конституционного строя и безопасности, мира)*.

• Согласно программ УНП ООН принимается участие в международных региональных семинарах по вопросам противодействия киберпреступности *(2013 год - Иран, г. Тегеран, 2015 год – Туркменистан,*

Таджикистан). Аналогичные семинары для практических работников проведены МВД совместно с УНП ООН и ОБСЕ в г.Алматы в 2015 и 2016 г.г.

Проблемные вопросы

В ходе проведения мероприятий по противодействию киберпреступности возникает ряд проблемных вопросов.

- Внедрение информационных технологий, онлайн-услуг, доступность компьютерных средств и гаджетов, а также увеличение пользователей сети интернет влечет за собой рост киберпреступлений, появление новых способов их совершения.

Расследование таких правонарушений существенно отличается от расследования других «традиционных» преступлений и требует от сотрудников проведения грамотных первоначальных действий, оперативного анализа, осмотра и изучения предметов и документов – возможных орудий преступления *(программ, баз данных, отдельных файлов и других электронных документов и т.д.)*.

С учетом постоянного развития технологий и появления новых способов совершения киберпреступлений, необходимо постоянно повышать уровень знаний и профессионального мастерства сотрудников.

- На качестве исследования *(экспертизы)* компьютерной техники и иных носителей информации отражается нехватка судебных экспертов в этой области, несовершенство методики исследования устройств *(в т.ч. кустарного производства)* для считывания информации с различных носителей. Имеют место случаи, когда судебные эксперты не могут ответить на вопросы о наличии вредоносной программы на носителе либо ее предназначении *(хищение персональных данных, удаленный доступ и т.д.)*.

К примеру, в 2013 году у задержанных в г.Астане граждан Молдавии изъяты шиммингговые устройства *(самодельные устройства для негласного считывания информации с пластиковых карточек)*. При назначении экспертизы из Центрального института судебной экспертизы МЮ г. Астана (ЦИСЭ) получен ответ об отсутствии методики исследования. Аналогичные проблемы по отдельным видам исследований имеются практически во всех областных Центрах судебной экспертизы МЮ.

В этой связи, для повышения эффективности работы по раскрытию компьютерных преступлений необходимо увеличить в регионах количество судебных экспертов, специализирующихся на исследовании носителей электронной информации с расширением круга проводимых исследований.

- Наиболее острой проблемой является использование социальных сетей, мессенджеров *(Facebook, Twitter, В контакте, одноклассники, WhatsApp, Viber, Line и т.д)* и иных зарубежных интернет-ресурсов, в т.ч. для распространения противоправной информации *(порнография, материалы экстремистского характера, комментарии с признаками разжигания межнациональной религиозной и иной розни и т.д.)*.

Зарубежные *(в основном российские и американские)* социальные сети имеют большую популярность, что приводит к неконтролируемому доступу к различным видам интернет-ресурсов. Их пользователи зачастую скрывают себя, регистрируя подложные страницы, аккаунты.

Для получения интересующих сведений о зарегистрированных в них казахстанских пользователях *(регистрационные данные, номера телефонов, IP-адреса и т.д.)* необходимо направление запросов. При этом запросы либо международные следственные поручения исполняются длительное время, что не обеспечивает оперативность действий сотрудников ОВД либо теряется сама актуальность *(смена владельца телефона, компьютера, уничтожение информации и т.д.)*.

Справочно: *В Закон Республики Казахстан «О персональных данных и их защите» с 2016 года внесены изменения, предусматривающие хранение персональных данных собственником и (или) оператором, а также третьим лицом в базах, расположенных на территории Республики Казахстан (ст.12, ч.2 указанного Закона), т.е. обязывающие располагать сервера социальных сетей, мессенджеров в Казахстане. Однако, данная мера в настоящее время не работает и требует дополнительной проработки.*

В случаях выявления зарубежных ресурсов (сайтов, ссылок и т.д.) принимаются меры к их блокированию.

Справочно: *при мониторинге сети Интернет в 2016 году выявлено 1419 зарубежных противозаконных ресурсов, с начала т.г. 1007 противоправных интернет-ресурсов (413 по распространению порнографических, 349 экстремистских материалов, 171 материал, пропагандирующих суицид в соц.сетях и 74 сайтов, распространяющих контрафактную продукцию)*.

- При совершении хищений преступники все чаще используют электронные средства оплаты *(Qiwi-кошельки и т.д.)*. Как правило, для их регистрации достаточно лишь SIM-карты, которая зачастую используется только один раз для создания «кошелька» *(разовые номера)*. При этом необходимости в предоставлении анкетных данных либо других установочных сведений не имеется. *(Имеются случаи использования «кошельков», созданных через абонентские номера зарубежных операторов связи)*.

Кроме того, в п.19 Правил оказания услуг сотовой связи *(утверждены Приказом Министра по инвестициям и развитию Республики Казахстан от 24 февраля 2015 года № 171)* предусмотрена обязательная регистрация владельцев абонентских номеров. Однако, имеют место факты регистрации абонентских номеров на дилеров либо посторонних лиц.

В этой связи, полагается целесообразным проработать вопрос о закреплении норм *(правил)*, предусматривающих обязательную идентификацию *(авторизацию)* владельца «электронного кошелька» помимо привязки к абонентскому номеру.

С учетом изложенного, в настоящее время МВД принимает необходимые меры к повышению эффективности работы по противодействию киберпреступности. Данное направление является приоритетным и находится на контроле.

Министерство внутренних дел