Big Data Tətbiqinin Kibercinayətlə Mübarizədə Potensialı və Məhdudiyyətləri

Elvin Balacanov
Lids Universiteti, Lids, Böyük Britaniya və Şimali İrlandiya Birləşmiş Krallığı
Hüquq və Yeni Texnologiyalar Araşdırma Qrupu
lw11eb@leeds.ac.uk

***Xülasə* — Müasir dövrdə rəqəmsal innovativ texnologiyaların tətbiqi digər sahələrin inkişafı ilə yanaşı, cinayət mühakimə icraatının vəzifələrinin, xüsusilə də kibercinayətlə effektiv və səmərəli mübarizənin realizəsində mühüm rola və imkanlara malikdir. İnformasiya və kommunikasiya texnologiyalarının (İKT) insan həyatına inteqrasiyası fonunda artan kibercinayət halları ilə mübarizənin təşkili İKT-nin özünəməxsus xüsusiyyətlərinin mübarizə alət və vasitələrinin yaradılması, inkişafı və tətbiqi prosesində ehtiva olunması zərurətini yaratmışdır. Bu məqalədə kibercinayətlə mübarizədə Big Data-nın bəzi imkanları və perspektivləri, habelə tətbiqinin hüquqi və faktiki problemləri nəzərdən keciriləcəkdir.**

Açar sözlər — kibercinayət; İKT-spesifik mühafizə mexanizmləri; Big Data; Big Data Mining; Big Data analitika; şəxsi məlumatların toxunulmazlığı.

I. GİRİŞ

İnformasiya erasında rəqəmsal məlumatların böyük hissəsi Big Data formasında təşəkkül tapır. Yüksək emal sürəti, böyük həcm və forma müxtəlifliyi ilə xarakterizə olunan bu rəqəmsal informasiyanın (Big Data-nın) yaddaş qurğularında saxlanılması, effektiv istifadə və analiz olunması üçün tələb olunan səviyyə bu informasiyaya çıxışı olan subyektlərin müvafiq imkanlarını xeyli üstələyir. Nəticədə mövcud informasiya əsasında ənənəvi üsul və metodların tətbiqi vasitəsilə vaxtında və düzgün qərarların verilməsində bir sıra çətinliklər yaradır. Rəqəmsal texnologiyalar tərəfindən 2015-ci ildə emal olunan qlobal illik informasiya həcminin 2009-cu illə müqayisədə təxminən 10 dəfə artıq olduğunu, 2020-ci ildə isə bu göstəricinin 44 dəfədən daha yüksəkdə qərarlaşacağı proqnozunu [1] nəzərə aldıqda Big Data konsepsiyasının qaçılmazlığını, həmçinin mövcud uzlaşma fərqinin aradan qaldırılması yönündə sürətlə artan əhəmiyyətini və tətbiqi zərurətini anlamaq olar.

II. İKT: KİBERCİNAYƏTLƏ MÜBARƏZİNİN TƏRKİB ELEMENTİ KİMİ

Hüquq-mühafizə orqanları tərəfindən elm və kompüter texnologiyalarının imkanlarından analitik, əməliyyat-tətbiqi və qərarvermə kimi proseslərdə istifadə edilməsinə baxmayaraq, ümumilikdə "big data" konsepsiyasının ətraflı qəbulu və onun potensialından geniş istifadə olunması sahəsində özəl sektorla müqayisədə daha mühafizəkar bir mövqe tutulmuşdur.. Əlavə olaraq qeyd etmək lazımdır ki, hüquq-mühafizə orqanları məlumat toplama sahəsində geniş təcrübə və imkanlara malik olsalar da, toplanmış məlumatların analizi və istifadə oluna bilməsinin təmini zamanı hər bir halda yüksək səviyyədə sərişte nümayiş etdirmirlər [2]. Bu da öz-özlüyündə İKT-spesifik elementlərin mühafizə mexanizmlərinin yaradılması, inkişafı və tətbiqi zamanı nəzərə alınmasını şərtləndirir. Kibercinayətlə mübarizə isə bu tip alət və vasitələrin tətbiqindən xüsusilə asılıdır.

Kibercinayətlə mübarizə mexanizmlərinin yaradılması, inkişafı və tətbiqinin bütün mərhələlərində onun tərkib elementlərinin xüsusiyyətlərinin nəzərə alınması bu mexanizmlərin effektivliyinin və səmərəliliyinin təmini üçün zəruridir. Qeyd etmək lazımdır ki, Azərbaycan Respublikasının Cinayət Məcəlləsinin "Kibercinayətlər" fəslində öz əksini tapmış bütün cinayət əməllərinin obyektini birbaşa və ya bilavasitə kompüter sistemi, bu sistemin normal fəaliyyətinin təmini və ya kompüter məlumatlarının mühafizəsi sahəsində yaranan ictimai münasibətlər təşkil edir. Həmçinin, bu cinayətlərin predmeti də, ya kompüter sistemi (proqramları, qurğuları), ya da bu sistemin tərkibində olan məlumatlardır (və ya məlumat daşıyıcılarıdır). Kibercinayətlərin obyektiv cəhəti də hər bir halda bu və ya digər formada kompüterlə bağlı anlayışları ehtiva edir [3]. Bütün bunlar isə bu cinayətlərlə mübarizənin və cinayət mühakimə icraatının tamlığının təmin edilməsinin İKT-spesifik mexanizmlərdən asılılığı kimi şərh oluna bilər.

Bundan başqa, bu əməllərin subyektiv cəhətdən yalnız birbaşa qəsdlə törədilməsi halında cinayət əməli kimi tövsif olunması onun obyektiv cəhətinin ifadə olunduğu əməllərin icrasındakı kompleks və planlı fəaliyyət zərurətindən irəli gəlir. Belə ki, kibercinayətlər kompüter sisteminə qanunsuz daxil olma, məlumatların qanunsuz ələ keçirilməsi, saxtalaşdırılması, bu məqsədlərlə kompüter qurğu və ya proqramlarının yaradılması, dövriyyəsi formasında həyata keçirilir ki, bunlar da bir sıra digər cinayətlərin subyektlərindən fərqli olaraq, kibercinayətin subyektlərindən daha yüksək biliklərə və təcrübəyə malik olmağı tələb edir. Nəticədə isə bu cinayətlərlə mübarizə hüquq-mühafizəni təşkil edən subyektlərdən adekvat səviyyədə inkişaf etdirilmiş və daha spesifik rəqəmsal alət və vasitələrin tətbiqini tələb edir.

Əlavə olaraq qeyd olunmalıdır ki, İKT-spesifik mexanizmlərin rolu təkcə "Kibercinayətlər" fəslinə daxil

edilmiş müddəalarla bağlı cinayət-mühakimə icraatının həyata keçirilməsi ilə məhdudlaşmır. Müasir dövrdə digər bir sıra cinayət əməlləri ilə mübarizənin də tərkibində kiber elementlər ehtiva olunduğu üçün bu üsul və vasitələrin əhəmiyyəti və onlara olan zərurət günü-gündən daha da artır.

III. KİBERCİNAYƏTLƏ MÜBARİZƏDƏ BİG DATA

Kiberməkanda sürətli təkamül prosesi keçən informasiyanın həcmi, mürəkkəbliyi, emalı və dövriyyə sürəti verilənlərin ənənəvi üsul və metodlarla səmərəli analizinin həyata keçirilməsini az qala mümkünsüz edir. Hüquqi və faktiki cəhətdən tətbiqi məhdudiyyətlər və uyğunsuzluqlarla müşayiət olunsa da, Big Data kibercinayətlə mübarizədə bir sıra texniki imkanlara malikdir.

A. Texniki aspektlər

Kibercinayətlə mübarizənin IKT-spesifik mexanizmlərin tətbiqindən asılılığını nəzərə alaraq iddia etmək olar ki, Big Data-nın bu istiqamətdəki imkanlarından istifadə etməklə mübarizənin effektivliyini və səmərəliyini əhəmiyyətli dərəcədə artırmaq olar. Çünki Big Data konsepsiyası məhz İKT sahəsində vüsət alan innovasiyalar sayəsində böyük həcmli məlumatların yaradılması, emalı, yadda saxlanması və ötürülməsi önündə analoq məlumatlarla bağlı mövcud bir sıra çətinliklərin aradan qaldırması nəticəsində diqqət mərkəzinə keçmişdir [4] . Buna görə də, mürəkkəb və böyük həcmli (peta və ekzabaytlarla ölçüyə malik həcmdə) verilənlərin emalı və analizi məqsədilə inkişaf etdirilən texniki və metodoloji üsul və vasitələrin müasir kompüterlər və kompüter sistemlərinin gücü vasitəsilə tətbiqi və realizəsi həm cinayətkar əməllərlə mübarizə, həm də bu məqsədlə ayrılan resursların daha səmərəli istifadəsində böyük potensiala malikdir. Bu anlamda Big Data Mining və Big Data analitika diqqətəlayiq bir mövqeyə sahibdir.

Bu üsul və vasitələr həm vahid struktura malik, həm də natamam strukturlu və struktursuz formada mövcud olan verilənlərin avtomatlaşdırılmış emalı və analizi nəticəsində onlar arasında adi halda çətin izlənilə bilən münasibət və əlaqələrin müəyyən olunması məqsədilə istifadə oluna bilər [5]. Ümumilikdə, bu cür münasibət və əlaqələr ibtidai araşdırmanın həyata keçirilməsi zamanı zəruri araşdırma istqamətlərinin daha aydın müəyyən olunmasında, cinayətlərin inkişaf istiqamətlərinin və onlarla mümkün mübarizə üsulları ilə bağlı daha düzgün seçimlərin edilməsində, habelə bu məqsədlə resursların daha səmərəli şəkildə bölüşdürülməsində mühüm rol oynaya bilər.

Risk profilləşdirilməsi məqsədilə tətbiq olunduğu təqdirdə isə bu üsul və vasitələr əvəllər izlənilməmiş əlaqə və münasibətlərin aşkara çıxarılması yolu ilə ayrı-ayrı cinayətlərin subyektlərinin, onların daxil olduğu mümkün şəbəkələrin, habelə şübhəli şəxslərin və ya onların dairəsinin müəyyən olunmasında geniş imkanlara malikdir. Şəxsin cinayətin icraçısına və ya cinayətin digər formada iştirakçısına çevrilmə riski, cinayətin baş verməsinə potensial şərait yaradan hallar və zərərçəkənlərin dairəsinin müəyyən olunmasında da Big Data Mining və Big Data analitika tətbiq oluna bilər [6].

Bunlarla yanaşı, Big Data əsasında həyata keçirilən risk profilləşdirilməsi profillərlə bağlı obyektivliyin daha yuxarı səviyyədə təmin olunmasına imkan yaratmasına baxmayaraq, analitikaya yönləndirilmiş verilənlərin məhdudluğu, natamamlığı və qeyri-dəqiqliyi qərarın subyektivliyinə və beləliklə, fərdlər üzrə tətbiq olunduğu təqdirdə ayrı-seçkiliyə gətirib çıxara bilər [7].

Qeyd etmək lazımdır ki, kibercinayətlərin araşdırılması və istintaqı üçün zəruri proseslərdən sayılan elektron/rəqəmsal sübutların toplanılması, emalı və sənədləşdirilməsi prosesi müvafiq kompüter avadanlıqları və proqramlar vasitəsilə avtomatlaşdırıla bilir. Hal-hazırda istifadə olunan bu avadanlıq və proqramların verilənlərin yalnız informasiyaya çevrilməsində iştirak etməsini və bu informasiyanın faydalılığının təmini və düzgün qərarvermənin araşdırmanı həyata keçirən şəxsdən asılı qalması bu sahədə əsas problemlərdən biri kimi qəbul olunur [8]. Lakin bu çətinliyin aradan qaldırılmasında Big Data analitikanın rolu rəqəmsal ekspertizanın həyata keçirilməsində mühüm potensial imkanlara malik bir üsul kimi nəzərə çatdırılmalıdır. Belə ki, digər ənənəvi analitika vasitələrindən fərqli olaraq, Big data analitikası araşdırmanı həyata keçirən şəxsdən araşdırmanın obyekti barədə əvvəlcədən məlumatlara malik olmanı, verilənlər arasında konkret münasibət və əlaqələrin axtarılmasını tələb etmir. Bunun əksinə olaraq son model inkişaf etmiş rəqəmsal analitika texnologiyaları vasitəsilə tətbiq olunduğu təqdirdə Big Data analitika verilənlərin modelləşdirilməsini aparır və nəticədə lazımı məlumatlar nümayiş olunur. Yekun olaraq araşdırmanı həyata keçirən şəxslərin üzərinə yalnız bu məlumatların məqsədəuyğunluğunun müəyyən olunması və araşdırma üçün faydalı məlumatların seçilib götürülməsi düşür [9]. Əvəzində isə doğru proqram və həllərin tətbiqi, habelə onların tətbiqi sahəsində yüksək bilik və peşəkarlıq tələb olunur.

Hal-hazırda ən geniş yayılmış Big Data həlləri qismində NoSQL, Apache Cassandra və Hadoop, xüsusilə də IBM Crime Information Warehouse (CIW) Big Data analitika və Big Data mining sahəsində müəyyən imkanlar vəd edir. Lakin hüquq-mühafizə və təhlükəsizlik orqanları tərəfindən cinayətlərin proqnozlaşdırılması və cinayət hallarının müəyyən olunmasında mühüm rola malik olmasına baxmayaraq, Big Data tətbiqlərinin (applications) sırf bu məqsədlərlə istifadəsinin yüksək effektivliyi barədə təsdiqləyici təcrübi məlumatlar çox azdır [7]. Halbuki, texniki həllər kibercinayətlə mübarizədə qanuni üsul və vasitələr qədər vacibdir və yalnız bu iki komponentin vəhdəti hüquq-mühafizə mexanizminin tamlığını təmin edir. Bu mexanizmin çatışmazlığı isə cinayətin baş verməsinə şərait yaradan üç əsas səbəbdən biridir [10].

Əlavə olaraq qeyd olunmalıdır ki, hüquq-mühafizə orqanlarının fəaliyyətinin təşkilində və cinayətkarlıqla mübarizə alət və vasitələrinin yaradılması, inkişafı və tətbiqində innovasiyaların inteqrasiyası prosesi ümumilikdə

aşağı sürətlə gedir. Həmçinin, baxmayaraq ki, rəqəmsal ekspertiza alət və vasitələri cinayət-mühakimə icraatının vəzifələrinin daha effektiv və daha səmərəli formada icrası üçün imkanlar yaradır, müasir texnologiyaların tətbiqi həm öz-özlüyündə mürəkkəb olması, həm də bu texnologiyaların tətbiqi üçün zəruri bilik və bacarıqlara malik insan resurslarının çatışmazlığı səbəbindən daha da çətinləşmişdir [11].

B. Hüquqi aspektlər

İKT-nin insan həyatının bütün sferalarına sürətli inteqrasiyası öz təsirini cinayət əməllərinin də kiberməkana transformasiyası formasında göstərmişdir. Kiberməkanda isə həyata keçirilmiş fəaliyyətin bütün mərhələləri rəqəmsal izlərlə müşayiət olunur ki, bunlar da onların izlənilə bilənliyini təmin edir. Kibercinayətlə mübarizə aspektindən götürüldükdə bu izlər sübuti əhəmiyyətə malikdir.

Lakin, Big Data konsepsiyası araşdırma üçün lazımi məlumatlara limitsiz çıxışın əldə olunması və bütün onlayn fəaliyyətlərin izlənilməsi vasitəsi kimi qəbul edilməməlidir. Bir tərəfdən, onlayn fəaliyyətin izlənilə bilənliyi cinayətlərin sayını azaldan 3 prinsipial faktordan biri kimi mühüm əhəmiyyət daşıyır. Belə ki, bütün hallarda izlənilmə və müəyyən oluna bilmə imkanının yüksək olduğunu dərk etmə şəxsin cinayətkar əməlin icrasından çəkinməsilə nəticələnə bilər [12]. Digər tərəfdənsə bu, əsassız onlayn nəzarət və internet trafiki barədə məlumat bazalarındakı məlumatların asanlıqla ələ keçirilməsinə zəmin yaradır. Nəticədə yuxarıda qeyd olunmuş texniki imkanlarla yanaşı Big Data şəxsi məlumatların subyektiv və qərəzli məqsədlər üçün əldə olunması və istifadəsi üçün də potensiala çevrilmişdir. Edward Snowden tərəfindən ABŞ Milli Təhlükəsizlik Agentliyinin Big Data analitikasından fərdlərin və təşkilatların kommunikasiya və yazışmalarının sistemli şəkildə izənilməsi ilə bağlı ictimaiyyətə ötürülmüş məlumatlar bu cür sui-istifadə hallarına misal kimi göstərilə bilər. Onu da əlavə etmək lazımdır ki, Snowden tərəfindən verilmiş məlumatlar ümumilikdə Big Data analitikasının nüfuzuna da mənfi təsir göstərmişdir [13].

Qeyd olunduğu kimi, Big Data-nın yaratdığı imkanlardan sui-istifadə ayrı-seçkiliyin yaranmasına da gətirib çıxara bilər. Belə ki, diskresion səlahiyyətlərin icrası zamanı hüquq-mühafizə orqanları tərəfindən Big Data analitikası nəticəsində əldə olunmuş məlumatlar əsasında subyektiv və tam əsaslandırılmamış qərarların da qəbul edilməsi mümkündür. Bundan başqa, Big Data anonimlik və konfidensiallığın qorunması önündəki texniki maneələri aradan qaldırdığı üçün bu anlayışlar daha açıq bir hədəf formasını almışdır. Bu isə sui-istifadəyə zəmin yaradan əlavə hallar qismində çıxış etmə imkanının yaranması deməkdir. Big Data-nın bu mənfi cəhətlərinin aradan qaldırılmasında qanunvericiliyin tələbləri müəyyən rola malikdir. Eyni zamanda, bu tələblər Big Data-nın həm də qanuni məqsədlər naminə istifadəsi prosesini mürəkkəbləşdirir.

Belə ki, məhkəmələr və cinayət prosesinin iştirakçıları tərəfindən Azərbaycan Respublikası Konstitusiyasına və Cinayət-Prosessual Məcəlləsinə, Azərbaycan Respublikasının digər qanunlarına, habelə Azərbaycan Respublikasının tərəfdar çıxdığı beynəlxalq müqavilələrə bütün hallarda ciddi riayət olunması qanunçuluq prinsipinin əsasını təşkil edir. Habelə, dövlət hər kəsin yazışma, telefon danışıqları, poçt, teleqraf və digər rabitə vasitələri ilə ötürülən məlumatın sirrini saxlamaq hüququna təminat verir [14]. Cinayət-mühakimə icraatının vəzifələrinin icrası zamanı insan və vətəndaş hüquq və azadlıqlarının qanunsuz məhdudlaşdırılması hallarından müdafiə, habelə hər bir cinayət təqibinin qanuniliyi və əsaslılığının təmini onun əsas prinsipləri və şərtlərinin təyinatı qismində çıxış etdiyini də nəzərə almaq vacibdir [15]. Bunlar isə Big Data analitika və Big Data mining-in praktikada tətbiqi zamanı riayət olunmalı olan standartların yüksəkliyi barədə ilkin mənzərə yaradır.

Onu da qeyd etmək lazımdır ki, Cinayət-Prosessual Məcəllə ilə müəyyən edilmiş hallarda cinayət prosesi prinsiplərinin və ya şərtlərinin pozulması cinayət təqibi üzrə başa çatmış icraatın etibarsız sayılmasına, onun gedişində qəbul edilmiş qərarların ləğvinə, yaxud toplanmış materialların sübutedici qüvvəsinin olmaması qənaətinə gəlməyə səbəb ola bilər [15]. Bu isə o deməkdir ki, Big Data-nın tətbiqinin hər hansı bir elementi və ya mərhələsi qanunvericiliyin tələblərinin pozulması ilə müşayiət olunursa, bu istiqamətdə aparılan prosessual hərəkətlər nəticəsində əldə olunmuş sübut və materialların prosessual qanunvericiliyə görə hüquqi qüvvəsi olmur [15]. Bu isə Big Data–nın tətbiqi ilə bağlı tənzimləmə məsələlərinin milli qanunvercilikdə təsbitini şərtləndirir.

NƏTİCƏ

Big Data kibercinayətlə mübarizə sahəsində potensial imkanlara malik olsa da, onun tətbiqi prosesində bir sıra texniki və hüquqi maneələr ortaya çıxır. Bu maneələrin böyük hissəsi cəmiyyətin idarə olunması üçün yaradılmış mexanizmlərin kiberməkanda tətbiqi üçün tam uyğun olmaması nəticəsində meydana gəlir. Beləliklə də, resurs çatışmazlığı özünü bir neçə müstəvidə daha kəskin şəkildə göstərməyə başlamışdır. Başqa sözlə, texniki, institutsional, hüquqi və insan resurlarının çatışmazlığı İKT sahəsində idarəetmənin və vəziyyəti nəzarət altında saxlamağın çətinləşməsi və mürəkkəbləşməsilə nəticələnmişdir.

Kiberməkanda təşəkkül tapmış cinayətlərlə mübarizə mexanizmlərinin yaradılması bu resursların hər biri ilə bağlı çatışmazlığın aradan qaldırılması üçün kompleks tədbirlərin tətbiqini şərtləndirir. Bu cür tədbirlər analoji olaraq Big Datanın da kibercinayətlə mübarizədə effektivliyi və səmərəliliyinin artırılması məqsədilə tətbiq olunması üçün zəruridir.

Big Data-nın tətbiqinin önündə yaranmış maneələrin aradan qaldırılması üçün ilkin olaraq onun tətbiqinin qanuniliyinin təmini üçün addımlar atılmalıdır. Bunun üçün isə müvafiq qanunvericiliyin texnoloji innovasiyaların inkişafı

və tətbiqini, habelə praktikaya sürətli inteqrasiyasını dəstəkləyəcək istiqamətdə inkişaf etdirilməsi zəruridir. Qanunvericiliyin təkmilləşdirilməsi insan hüquq və azadlıqlarının yüksək səviyyədə təminatı məqsədinə xidmət etməklə bütün mərhələlərdə vətəndaşların da prosesdə yaxından iştirakı ilə müşayiət olunmalıdır.

Eyni zamanda, kibercinayətlə mübarizəni həyata keçirən hüquq-mühafizə və təhlükəsizlik orqanları subyektlərinin bu sahədə müvafiq bilik və bacarıqlarının artırılması məqsədilə mütəmadi tədbirlərin həyata keçirilməsi, habelə texnoloji innovasiyalar sahəsində onlar daim yenilənmiş məlumatlarla təmin olunmalıdır. Bu, həmçinin Big Data-nın analitika məqsədilə tətbiqi üçün cəlb olunmuş texniki resursların daha effektiv və daha səmərəli istifadəsi üçün zəruridir.

ƏDƏBİYYAT

[1] Computer Sciences Corporation, 'Data Universe Explosion & the Growth of Big Data', 2015. http://www.csc.com/insights/flxwd/78931-big_data_universe_beginning_to_explode .

[2] B. Akhgar, B. Gregory, Application of Big Data for National Security, Butterworth-Heinemann, 2015.

[3] Azərbaycan Respublikasının Cinayət Məcəlləsi, http://www.e-qanun.az/code/11

[4] R. Walker, From big data to big profits. New York, NY: Oxford Univ. Press, 2015.

[5] SAS, Managing the Intelligence Life Cycle: A More Effective Way to Tackle Crime 2013. http://www.sas.com/en_us/whitepapers/managing-intelligence-life-cycle-106831.html

[6] J. James and F. Breitinger, Digital Forensics and Cyber Crime 2015: 7th International Conference, (Seoul, South Korea, ICDF2C), 2015, pp. 126-139.

[7] Postnote 470, Big Data, Crime and Security, UK Parliament, 2014.

[8] J. James and P.Gladyshev, Challenges with Automation in Digital Forensic Investigations, 2013, CoRR, abs/1303.4498, http://arxiv.org/abs/1303.4498

[9] Sas.com, 'How big data analytics can be the difference for law enforcement', 2015. http://www.sas.com/en_us/insights/articles/risk-fraud/big-data-analytics-for-law-enforcement.html.

[10] L. E. Cohen, M. Felson, “Social Change And Crime Rate Trends: A Routine Activity Approach”, American Sociological Review, 1979, Vol. 44, pp. 588-608.

[11] Crcs.seas.harvard.edu, 'Simson Garfinkel: "Automated Digital Forensics"', 2015. http://crcs.seas.harvard.edu/event/simson-garfinkel-automated-digital-forensics.

[12] M. Ouimet, ‘Internet and crime trends’ in Frank Schmalleger and Michael Pittaro, Crimes Of The Internet, Prentice Hall, 2009.

[13] B. Marr, Big Data: Using Smart Big Data, Analytics and Metrics to Make Better Decisions and Improve Performance, John Wiley & Sons, Ltd, 2015.

[14] Azərbaycan Respublikasının Konstitutsiyası, http://e-qanun.az/framework/897

[15] Azərbaycan Respublikasının Cinayət Prosessual Məcəlləsi, http://e-qanun.az/code/14