DİN-in Polis Akademiyası "DİO-nun inzibati fəaliyyəti" kafedrasının baş müəllimi, polis polkovnik-leytenantı Heydər Heydərov

İNFORMASİYA CƏMİYYƏTİ VƏ İNFORMASİYA TƏHLÜKƏSİZLİYİ

Açar sözlər: informasiya cəmityyəti, informasiya təhlükəsizliyi, milli təhlükəsizlik, informasiya texnologiyaları, kibercinayətkarlıq.

Cəmiyyətin inkişafının müasir mərhələsi informasiya mühitinin artan rolu ilə xarakterizə olunur. İnformasiya mühiti dövlətin siyasi, iqtisadi, müdafiə və digər sistemlərinə aktiv təsir edən cəmiyyətin həyatının ən vacib faktorlarından biridir. Dövlətin milli təhlükəsizliyi informasiya təhlükəsizliyinin təmin edilməsindən əhəmiyyətli dərəcədə asılıdır. Hal-hazırda informasiya milli strateji resurs olub, dövlətin ən əsas sərvətlərindən biri sayılır. İnformasiyalaşdırmanın təsiri altında cəmiyyətin bütün sahələri çeviklik və dinamiklik kimi yeni keyfiyyətlər almaqdadır. Lakin eyni zamanda informasiya təsirindən ictimai proseslərin potensial zəifliyi artır.

İnformasiya təhlükəsizliyinin təmin edilməsi müasir dövrdə hər bir dövlətin ən prioritet vəzifələrindən birinə çevrilmişdir.

Elmi-texniki tərəqqinin inkişafı artdıqca şəxsiyyətin, cəmiyyətin, dövlətin informasiya təhlükəsizliyi riski artmaqdadır və onun təhlükəsizliyi dövlət siyasətində müvafiq yeri tutmalıdır.

Hər bir dövrün özünəməxsus mütərəqqi texnologiyaları cəmiyyətin formalaşmasına təsir göstərmişdir. Bu texnologiyalar zamanın tələbinə uyğun olaraq inkişaf etmiş və bu tendensiya bu gün də davam etməkdədir.

Yeni yaradılan texnologiyalar yalnız mövcud dövrün tələblərinə cavab verirsə də bir neçə ildən sonra bu texnologiyalar inkişafdan geri qaldığı üçün tələbələrə cavab verməyəcəkdir. Yəni, hər bir yeni yaradılan texnologiyalar çox qısa bir zamanda tələblərə cavab vermək imkanında olur. Başqa sözlə desək, texnologiyalar çox sürətlə qocalır.

Məhz bu baxımdan hazırkı dövrü – müasir, çox sürətlə yeniləşən dövr kimi də adlandırmaq olar.

Müasir dövrdə cəmiyyətin inkişafına təsir göstərən əsas amillərdən biri də informasiya-kommunikasiya texnologiyalarıdır.

Hazırda informasiya-kommunikasiya texnologiyaları cəmiyyətin bütün sahələrinə geniş nüfuz etməkdədir. Bunun nəticəsində bəşəriyyət yeni inkişaf mərhələsinə – informasiya cəmiyyətinin formalaşması dövrünə qədəm qoyur.

Son zamanlar dövlət orqanları ilə vətəndaşlar arasında qarşılıqlı kiber əlaqələrin yaradılması informasiya cəmiyyətinin ən vacib, prioritet istiqamətlərindən birinə çevrilmişdir.

Yeni informasiya texnologiyaları bu gün elə sürətlə inkişaf edir ki, onun doğuracağı fəsadlar ya əvvəlcədən təsəvvürə belə gəlmir, ya da cəmiyyət tərəfindən bu problemlər çox gec dərk edilir.

Ümumiyyətlə belə bir fikir mövcuddur ki, elmi-texniki tərəqqi hər hansı kritik həddi aşdıqdan, inkişafın müəyyən mərhələsinə çatdıqdan sonra bəşəriyyət əleyhinə işləməyə başlayır. Bu fikrin sübutu kimi nüvə texnologiyasını, sənayenin inkişafı nəticəsində yaranmış ciddi ekoloji problemləri, texnogen qəzaları və s. göstərmək olar [7].

Analoji vəziyyət informasiya texnologiyaları sahəsində də yaranmışdır. İnformasiya texnologiyalarının informasiya cəmiyyətinə inteqrasiyanın müsbət tərəfləri ilə yanaşı, informasiya təhlükəsizliyi kimi mənfi tendensiyaların da təşəkkül tapmasına, ayrı-ayrı şəxslərin, təşkilatların və bütövlükdə dövlətlərin informasiya resursları üçün ciddi təhlükələrin meydana gəlməsinə səbəb olmuşdur.

Elmi-texniki tərəqqinin inkişafı artdıqca şəxsiyyətin, cəmiyyətin, dövlətin informasiya təhlükəsizliyi artmaqdadır və onun təhlükəsizliyi dövlət siyasətində müvafiq yeri tutmalıdır. İnformasiya irimiqyaslı qəzalara, hərbi konfliktlərə, dövlət idarəçiliyi, maliyyə sistemi və elmi

mərkəzlərin fəaliyyətinin pozulmasına səbəb ola bilən faktora çevrilmişdir. Cəmiyyətin informasiyalaşdırılması səviyyəsinin artması onun informasiya təhlükəsizliyini daha etibarlı edir.

Müasir cəmiyyətin inkişafı informasiya mühitinin artan rolu ilə xarakterizə olunur. İnformasiya mühiti dövlətin siyasi, iqtisadi, müdafiə və digər sistemlərinə aktiv təsir edən cəmiyyətin həyatının ən vacib faktorlarından biridir. Hazırda informasiya milli strateji resurs olub, dövlətin ən əsas sərvətlərindən biri hesab edilir. İnformasiyalaşdırmanın təsiri altında cəmiyyətin bütün sahələri çeviklik və dinamiklik kimi yeni keyfiyyətlər almaqdadır.

İnformasiya cəmiyyətinin uğurlu, dayanıqlı inkişafının təmin edilməsi informasiya təhlükəsizliyinin təmin olunması səviyyəsindən birşbaşa asılıdır. Müasir dünyada rəqəmsallaşdırma və virtual münasibətlər genişləndikcə informasiya təhlükəsiliyinin rolu da artmaqdadır.

Cəmiyyətin, dövlətin və əhalinin informasiyadan asılılığının getdikcə artdığı bir dövrdə kibertəhlükəsizliyin təmin edilməsi strateji məsələyə çevrilir, informasiya resurslarının dayanıqlı və təhlükəsiz fəaliyyətinin təmin olunmasının vacibliyi aktuallaşır.

Hazırda hər bir dövlətin maraqları yalnız coğrafi məkanda deyil, eyni zamanda virtual aləmdə də qorunması xüsusi əhəmiyyət daşımağa başlayır. İnformasiya təhlükəsizliyi milli təhlükəsilik sisteminin ən mühüm istiqamətlərindən birinə çevrildiyi müasir dövrdə informasiya təhlükəsizliyinin kompleks təminatını həyata keçirmədən milli suverenliyin qorunması, beynəlxalq terrorizm, kibercinayətkarlıq, iqtisadi sahədə cinayətlərlə mübarizə, şəxsi həyatın toxunulmazlığının təmin edilməsi kimi problemlərin həlli mümkün deyil.

İnformasiya texnologiyalarının, coğrafi cəhətdən paylanmış kompüter sistemlərinin və şəbəkələrinin, ümumi istifadə üçün nəzərdə tutulmuş informasiya və şəbəkə resurslarının sürətli inkişafı sahəsində informasiya təhlükəsizliyinin təmin edilməsi çox ciddi məsələyə çevrilmişdir.

Kompüter sistemlərinin və şəbəkələrinin gündəlik xidməti fəaliyyəti və şəxsi məqsədlər üçün geniş istifadəsi cəmiyyətin müxtəlif təbəqələrində informasiya texnologiyalarına, o cümlədən informasiya resurslarına münasibətdə ciddi dəyişiklər yaratmışdır. Nəticədə, şəxsi maraqların, niyytələrin və tələbatların ödənilməsi məqsədilə informasiya sistemlərinin işinə qanunsuz müdaxilə, qəsdən və ya təsadüfən, qərəzli və qərəzsiz şəkildə bu sistemlərə daxil olmaq, onları sıradan çıxartmaq, informasiya resurslarında və sistem parametrlərində dəyişiklər aparmaq, onları istifadə və məhv etmək kimi təhlükəli hallar günbəgün çoxalır.

Yer kürəsini bütünlükdə hörmçək toru kimi örtən İnternet şəbəkəsi informasiya təhlükəsizliyi probleminin daha da kəskinləşməsinə təkan verən əsas amillərdən biridir. Dünyanın istənilən nöqtəsindən İnternet şəbəkəsinə qoşulmaq, onun vasitəsilə müxtəlif növ məlumatları ötürmək və almaq mümkünlüyü xidməti istifadəçilərə öz iş yerlərini və evlərini tərk etmədən praktiki olaraq istənilən ölkədə olan müxtəlif informasiya sistemlərinə və məlumat bazalarına qoşulmaq, eləcə də onları maraqlandıran zəruri informasiya ilə tanış olmaq və məlumatları əldə etmək imkanı verir.

İnternet şəbəkəsi istifadəçi qismində onun xidmətlərindən istifadə edən hər bir şəxsə, o cümlədən kibercinayətkarlara da öz cinayət niyyətini həyata keçirmək üçün tamamilə eyni imkanlar yaradır. Bu gün informasiya texnologiyaları, telekommunikasiya sistemləri, İnternet şəbəkəsi müxtəlif kateqoriyalı insanlar, o cümlədən terrorçu qruplar, kibercinayətkarlar, düşmən ölkələrin xüsusi xidmət orqanları tərəfindən informasiya mübarizəsi, qarşıdurması, hətta müharibəsi vasitəsi və aləti kimi istifadə edilir.

İnternetin köməyi vasitəsilə cinayət törədilməsinə yönəlmiş qanunsuz fəaliyyətin diapazonu və imkanları uşaq pornoqrafiyalarının yayılmasından, fərdi məlumatların fişinq edilməsi, silah və narkotik vasitələrin alqı-satqısı, DDoS-hücumlar, ziyanverici proqramların yayılması və dələduzluq kimi sahələri əhatə edir. Qlobal miqyasda kibercinayətkarlıqda artma tendensiyası müşahidə olunur [6].

Kibertəhlükəsizliyin qlobal problemə çevrildiyini və bu problemə qarşı beynəlxalq müstəvidə mübarizə tədbirlərinin gücləndirildiyi bir zamanda rəsmi statistik məlumatlara görə, dünya üzrə kibertəhlükəsizlikdən yaranan itkilərin həcmi təqribən 1 trilyon dollara yaxınlaşır ki, bu da təxminən narkobizneslə müqayisə edilə bilən bir səviyyədir. Eyni zamanda, təxminən 550-

600 milyon insan kibertəhlükələrin qurbanlarına çevrilir. Müasir dövrdə virtual məkanda fəaliyyət göstərən kibercinayətlərin qurbanları nəinki insanlar, eləcə də dövlətlər təşkil edir.

Kibertəhlükəsizliyin artmasının əsas amillərindən biri də bu sahədə yüksək latentliyin olması, bu növ hüquqpozmalarla mübarizədə cinayətlərin açılma dinamikasının getdikcə azalması, İntenet istifadəçilərinin və xidmətlərinin sayının durmadan atrması, təhlükəsizlik tələblərinə cavab verməyən proqram təminatlarının geniş yayılmasını göstərmək olar.

İnformasiya təhlükəsizliyi ilə bağlı hüquqpozmaların inkişaf meylliklərinə nəzər salarkən demək olar ki, bank və maliyyə sahələri ilə bağlı olan kiberhücumlar nisbi azalmış, əvvələr mövcud olamayan Elektron Hökümət kimi sistemlərin, kritik infrastkturların İnternet şəbəkəsinə inteqrasiya olunması prioritet hədəflərə çevirmişdir.

Kritik əhəmiyyətli infrastkturların əsas hədəf kimi seçilməsində məqsəd cəmiyyətin və dövlətin fəaliyyətini iflic vəziyyətə gəriib çıxarmaq olduğu üçün belə hücumların, kibermüharibələrin, kiberqarşıdurmaların təşkili planlı şəkildə xarici ölkələrin xüsusi xidmət orqanları tərəfindən həyata keçirilir.

Kritik infrastkturların əsas hədəf kimi seçilməsində digər səsblərdən biri də paylanmış xidmətlərdən imtina hucumunun (DDoS (Distributed Denial of Service)) təşkilidir.

İnformasiya təhlükəsizliyinin digər mənfi amillərindən biri də onun ictimai təfəkkürə, cəmiyyətin həyatına, davranışına olan mənfi təsiridir.

Çin Xalq Respublikasında sosial media yerli və milli olduğundan, sistem dövlət tərəfindən nəzarətdə saxlanılır və xalqın nə düşündüyünü izləmək xüsusi xidmət orqanları üçün çətinlik yaratmır.

Kembric Analitik Şirkətinin məlumatına görə Facebook tərəfindən tətbiq edilmiş insan xarakterini arama motoru müəyyən tip auditoriyaya yönələ bilən, onların fikirlərini qarışdırmaqla auditoriyanın şüuruna təsir göstərə bilir. Belə sistemlər tərəfindən, eləcə də sosial mediya vasitəsilə yayımlanan məlumatlar sosial şəbəkə istifadəçilərini manipulyasiya etməyə imkan verir.

İnformasiyanın mühafizəsinə yönəlmiş əsas təhlükələrdən biri ziyanverici proqramlardır. Belə ziyanverici proqramlar yalnız verilənlərin tamlığı üçün deyil, eyni zamanda sistemin normal fəaliyyət göstərməsi üçün də təhlükə yarada bilər.

Kompyuter virusları müxtəlif vasitələrlə bir kompyuterdən digər kompyuterə keçməyə cəhd edən, verilənlərin dəyişdirilməsi və ya silinməsinə səbəb olan və ya istifadəçinin işinə mane olan, digər proqramlarda gizlənmiş kiçik həcmli proqramlardır. Virus proqramları özlərini təxminən bioloji virus kimi aparır: çoxalır, maskalanır və ziyanlı təsirlər göstərir. Virus özgə informasiya daşıyıcılarından, elektron poçt və ya İnternet resurslardan istifadə edilən zaman təhlükə yarada bilər. Viruslar bütün kompyuter və şəbəkə mühitlərində yayıla bildiyindən, informasiya hücumlarında onlardan daha geniş istifadə edilir. Hal-hazırda informasiya hücumlarında istifadə olunan vasitələrin bütün növləri arasında kompyuter virusları daha çox təhlükəlidir. G Data Software şirkətinin hesabatında bildirilmişdir ki, dünyada hər 15 saniyədə bir virus yaradılır və təhlükəli virusların sayı 2 milyondan artıqdır. Virusun xüsusiyyətini onun konkret proqrama istiqamətlənmiş olmaması, öz-özünə çoxalma imkanına malik olması, proqramın daxilində yerləşməsi, əlaqə xətləri, kompyuter şəbəkəsi ilə ötürülməsi və informasiya sistemini sıradan çıxara bilməsi və s. təşkil edir.

Sərhədsiz kiberməkan fərdlərə və qruplara dövlətlərin hüquq sistemlərindəki boşluqlardan cinayətkar məqsədlər üçün istifadə etməyə şərait yaradır. Kibercinayətkarlıq əksər hallarda cinayətkar və zərərçəkənin müxtəlif yurisdiksiyalarda yerləşməsi səbəbindən hüquq-mühafizə orqanları tərəfindən bu cür cinayətlərin istintaqı və mühakimə olunmasına manea törədir [1]. Beləliklə, cinayətlərinin kriminallaşmış tərkiblərinin, onların vəziyyətinin təhlili və inkişaf tendensiyalarının qarşısının alınmasında cinayət-hüquqi və təşkilati-texniki vasitələrin kompleksli tədqiqatına zərurət yaranmışdır.

Avropa Şurasının (AŞ) 2001-ci ildə Budapeştdə imzalanmış və 2004-cü ildə qüvvəyə minmiş Kibercinayətkarlıq və ya Budapeşt Konvensiyası kibercinayətkarlıqla mübarizədə tarixi nailiyyət hesab oluna bilər və bu günə qədər müvafiq sahədə aparıcı və ən çox istinad olunan beynəlxalq sənəddir [2].

2018-ci ilə qədər Budapeşt Konvensiyası Avropa Birliyinə qoşuluş bütün ölkələrlə yanaşı, ABŞ, Yaponiya və Avstraliya da daxil olmaqla dünyanın 62 ölkə tərəfindən ratifikasiya edilmişdir [3]. Azərbaycan Respulikası tərəfindən Budapeşt Konvensiyasını 30 iyun 2008-ci ildə imzalamış, 30 sentyabr 2009-cu ildə isə ratifikasiya olunmuşdur. Milli qanunvericiliyin həmin Konvensiyadan irəli gələn öhdəliklərə uyğunlaşdırılması məqsədilə Azərbaycan Respublikası Cinayət Məcəlləsinə və digər normativ-hüquqi aktlara müvafiq əlavə və dəyişikliklər edilmişdir [4].

İnformasiya təhlükəsizliyinin təmin edilməsi sahəsində Azərbaycan Respublikası Prezidentinin 2 aprel 2014-cü il tarixli Sərəncamı ilə təsdiq edilmiş "Azərbaycan Respublikasında informasiya cəmiyyətinin inkişafına dair 2014-2020-ci illər üçün Milli Strategiya" ölkənin informasiya məkanının təhlükəsizliyinin təmin olunması, bu sahəni tənzimləyən normativ hüquqi bazanın inkişaf etdirilməsi, bu istiqamətin əsas məqsədləri kimi müəyyən edilmiş və aşağıdakıların həyata keçirilməsi nəzərdə tutulmuşdur:

- informasiya təhlükəsizliyi sahəsində vahid dövlət siyasətinin, hüquqi bazanın təkmilləşdirilməsi;
- ölkənin milli informasiya məkanının və infrastrukturunun, o cümlədən informasiya təhlükəsizliyini təmin edən sistemin inkişaf etdirilməsi;
- ölkənin informasiya əlaqələrində xarici ölkələrdən texniki və texnoloji asılılığın azaldılması üzrə tədbirlərin həyata keçirilməsi;
- Elektron hökumət infrastrukturunun informasiya təhlükəsizliyinin təmin edilməsi;
- elektron təhlükələr barədə ölkə səviyyəsində məlumatlandırmanın həyata keçirilməsi;
- kibertəhlükəsizliyin gücləndirilməsi istiqamətində müvafiq texniki və metodiki vasitələrin yaradılması, tövsiyələrin hazırlanması və metodiki dəstəyin göstərilməsi;
- uşaqların qanunazidd məzmunlu saytlardan qorunması üçün "təhlükəsiz internet" mexanizminin işlənilməsi və tətbiqi;
- dövlət və qeyri-dövlət informasiya infrastrukturu subyektlərinin kibertəhlükəsizlik üzrə fəaliyyətlərinin əlaqələndirilməsi;
- ölkənin informasiya təhlükəsizliyi sahəsində beynəlxalq əməkdaşlığın təmin olunması.

Müasir dövrdə hər bir dövlətin milli informasiya infrastrukturu qlobal sistemdə birləşmiş internet şəbəkəsi ilə sıx bağlıdır. Məhz buna görə də bu növ cinayətkarlıq dövlətin milli təhlükəsizliyi üçün ciddi təhlükəyə çevrilib. Belə ki, heç bir dövlət bu növ cinayətkarlıqla ayrılıqda mübarizə aparmaq iqtidarında deyil. Bu cinayətkarlıqla səmərəli mübarizə aparmaq üçün beynəlxalq əməkdaşlıq çərçivəsində hüquqi tənzimləmə mexanizmləri hazırlanmalı və dünya birliyinin heç bir dövləti bu sahədə qəbul olunmuş stanradtlardan kənarda qalmamalıdır.

Nəzərə almaq lazımdır ki, əsası Ümummilli Lider Heydər Əliyev tərəfindən 17.02.2003-cü ildə qoyulmuş "Azərbaycan Respublikasının inkişafı naminə informasiya və kommunikasiya texnologiyaları üzrə Milli Strategiya" Azərbaycan Respublikasının Prezidenti cənab İlham Əliyev tərəfindən dövlətin prioritet istiqaməti kimi müəyyən olunmuşdur. Qeyd olunan faktorlar bir daha milli informasiya infrastrukturuna daxil olan mühüm strateji obyektlərin təhlükəsizliyinin təmin edilməsi sisteminin yaradılması üzrə tədbirlər kompleksinin işlənib hazırlanmasının vacibliyini əsaslandırır. 29.03.2018-ci il tarixdə imzalanmış "İnformasiya Təhlükəsizliyi üzrə Koordinasiya Komissiyasının yaradılması haqqında" Sərəncam informasiya təhlükəsizliyinə təhdidlərin qiymətləndirilməsini, o cümlədən belə təhdidlərin əsas mənbələri, istiqamətləri, formaları, vura biləcəyi zərər və təsirləri ilə bağlı təhlillərin aparılmasını, mümkün təhdidlərin qarşısının alınması və qabaqlanması sahəsində müvafiq dövlət orqanlarının fəaliyyətinin əlaqələndirilməsini, birgə tədbirlərin planlaşdırılması və həyata keçirilməsini təmin edəcəkdir. Sərəncam, informasiya sistemlərinə və ehtiyatlarına kiberhücumlar və kibertəhlükə hallarında əlaqələndirilmiş işin təşkili və birgə əks tədbirlərin həyata keçirilməsi, internet informasiya ehtiyatlarında Azərbaycan Respublikasının milli maraqları əleyhinə məqsədyönlü şəkildə yayılan saxta məlumatların mənbəyinin təxirə salınmadan müəyyən edilməsi və bu barədə müvafiq orqanların dərhal məlumatlandırılmasına yönəlmişdir.

Bununla bərabər Avropanın və dünyanın aparıcı ölkələrinin təcrübələri tam şəkildə təhlil edilərək "Azərbaycanın kibertəhlükəsizlik strategiyasının" beynəlxalq təcrübə əsasında qəbul edilməsi ölkədə kibertəhlükəsizlik sahəsində aparılan fəaliyyətin daha da mütəşəkkilləşdirilməsinə və təkmilləşdirilməsinə, milli təhlükəsizlik siyasətinin möhkəmlənməsinə xidmət edəcəkdir. Kibercinayətkarlıqla effektiv mübarizənin aparılması, ölkəmizə qarşı ola biləcək kibertəhdidlər, onların qarşısını almaq üçün tədbirlər, kritik infrastrukturda kibertəhlükəsizlik tədbirlərinin həyata keçirilməsi və elektron hökumət infrastrukturunun təhlükəsizliyinin təmin edilməsi üçün kibertəhlükəsilik strategiyasının hazırlanması və qəbul edilməsi ölkədə kibertəhlükəsizliyin qorunmasında mühüm rol oynayacaqdır.

İstifadə olunmuş ədəbiyyat

1. Wall D. S. The Transformation of Crime in the Information Age, 2007, Wiley, 2007, 288 p.
2. Convention on Cybercrime, Budapest, 21 November 2011, http://conventions.coe.int/ Treaty/en/Treaties/Html/185.htm
3. https://www.coe.int/ru/web/conventions/full-list/-/conventions/treaty/185/signatures
4. "Kibercinayətkarlıq haqqında" Konvensiyanın Təsdiq edilməsi barədə Azərbaycan Respublikasının Qanunu, 30 sentyabr 2009-cu il, http://www.cert.az/konvensiya.html
5. Azərbaycan Respublikası Prezidentinin 2 aprel 2014-cü il tarixli Sərəncamı ilə təsdiq edilmiş "Azərbaycan Respublikasında informasiya cəmiyyətinin inkişafına dair 2014-2020-ci illər üçün Milli Strategiya"
6. https://www.bka.de/DE/UnsereAufgaben/Deliktsbereiche/Internetkriminalitaet/internetkriminalitaet_node.html
7. Qasımov V.Ə. İnformasiya təhlükəsizliyinin əsasları. Dərslik. Bakı 2009, s. 340

КИБЕРПРЕСТУПНОСТЬ И КИБЕРТЕРРОРИЗМ В КОНТЕКСТЕ НОВЫХ УГРОЗ

РЕЗЮМЕ

Ключевые слова: информационное общество, информационная безопасность, национальная безопасность, информационные технологии, киберпреступность.

Глобализация информационных процессов в мировом масштабе привело к появлению общественно опасных деяний – киберпреступности. В отличие от традиционного вида преступлений киберпреступности используется новейшие достижения науки и техники в области компьютерных и информационных технологий. Развитие киберпреступлений угрожает безопасности личности, общества и государства на всех уровнях политики. В условиях развития информационного общества киберпреступность уже давно перерос рамки регионального и национального масштаба. В статье исследуются проблемы, киберпреступности в государственном масштабе, которые являются относительно новыми для международного сообщества.

CYBERCRIME AND CYBERTERRORISM IN THE CONTEXT OF NEW THREATS

SUMMARY

Keywords: information society, information security, national security, information technology, cybercrime.

The globalization of information processes on a global scale has led to the emergence of socially dangerous acts - cybercrime. Unlike the traditional type of cybercrime crimes, the latest achievements of science and technology in the field of computer and information technologies are used. The

development of cybercrime threatens the security of the individual, society and the state at all levels of politics. With the development of the information society, cybercrime has long outgrown the regional and national scale. The article explores the problems of cybercrime on a national scale that are relatively new to the international community.