UOT 327

ELŞAD HƏSƏNLİ
AMEA-nın Fəlsəfə və Sosiologiya İnstitutunun aparıcı elmi işçisi,
siyasi elmlər üzrə fəlsəfə doktoru, dosent
elshadhasanli1968@mail.ru

KİBERTƏHDİD: DÖVRÜN AKTUAL PROBLEMİ

DOI: https://doi.org/10.36719/2708-065X/109/102-106

Texnoloji yeniliklərin hər bir fəaliyyət sahəsinə tətbiq olunduğu indiki dövrdə kibertəhdidlərin artması ciddi problem kimi aktualdır. Bununla bağlı tədbirlərin görülməsi, təhlükənin neytrallaşdırılması və qabaqlayıcı addımların atılması həm dövlət qurumları, həm də tədqiqat mərkəzlərinin qarşısında bir vəzifə kimi durur. Araşdırmada kibertəhdid üsulları, kibercinayətkarların əməllərinin ifşası, onlarla mübarizə yolları,bu yolda əldə olunmuş təcrübənin mübadiləsi, dövlətlərarası və qurumlararası əməkdaşlıq məsələləri, hüquq mühafizə orqanlarının fəaliyyəti, eləcə də qanunvericilik bazasının təkmilləşdirilməsi ilə bağlı işlər təhlil olunub, dəyərləndirilib.

Açar sözlər: Təhlükəsizlik, kibercinayət, kibertəhlükəsizlik, kompüter sistemləri, dövlət, münaqişə, sülh, siyasət.

Giriş. Dövrün ayrı-ayrı mərhələlərində dövlətlər və cəmiyyətlər müxtəlif təhdid və çağırışlarla üzləşiblər. Yeni texnologiyaların yaranması ilə müasir dövr həm də yeni təhlükə ilə üzləşib. Kiberterror, kibercinayət, kiberhücum kimi xarakterizə olunan bu təhdidlər dövlət qurumlarının ahəngdar fəaliyyətinə, cəmiyyətin və ayrı-ayrı fərdlərin yaşam tərzinə yeni-yeni maneələr, pozuntu, çökmə və digər mənfi çalarlar qatır. əm maddi, həm də mənəvi cəhətdən cəmiyyətə zərər vuran bu amillər onlara qarşı ciddi tədbirlər görülməsini zəruri edir. Artan təhlükə və təhdidlərin qarşısını almaq və yaxud da onların təsirini minimuma endirmək üçün həm elmi-texniki, təşkilati, həm də hüquqi müstəvidə tədbirlər görülməsi zərurəti yaranır. Təhlükə mənbələri və üsullarını müəyyənləşdirmək, təhlil etmək və qabaqlayıcı addımlar atmaq üçün həm ölkədaxili, qurumlararası, həm də beynəlxalq səviyyədə, dövlətlərarası mexanizmlərin işlək vəziyyətə gətirilməsi, yenilənməsi, hüquqi sahədə əməkdaşlıq məsələləri günün tələbi kimi qarşıda duran əsas məsələlərdir. Kibertəhdidlərin əsasən xarici ölkələrdən gəlməsi, bu işlərin icraçılarının çoxunun xarici dövlətlərdə olması beynəlxalq əməkdaşlığı da ön plana çıxarır.

Əsas hissə. Dövrümüzdə informasiya texnologiyaları inkişaf etdikcə əldə olunan yeni imkanlardan fürsətcil istifadə etmək istəyənlərin sayı da artır. Bu qeyri-obyektiv mövqe, həm də qrup şəklində olan insanlar, eləcə də təşkilatlar tərəfindən özünü biruzə verir, təxribat, casusluq, mənimsəmə, pozuculuq məqsədi güdür. Başqa sözlə desək, kibertəhdid 21-ci əsrin yeni bəlasına çevrilib. Şəxsi məlumatların ələ keçirilməsi, kəşfiyyat, iş ahənginin pozulması, nazirlik, idarə və müəssisələrin proqram təminatının sındırılması və maliyyə vasitələrinin mənimsənilməsinə qədər geniş əhatəli bu fəaliyyətə qarşı mübarizə tədbirləri gücləndirilsə də mütəmadi olaraq yeni təxribat əməlləri ilə üzləşmək faktı meydana çıxır və bu da özlüyündə yeni əks tədbirlərin görülməsinə ehtiyac yaradır. Kibertəhlükəsizliklə mübarizə məqsədilə Azərbaycanda bu sahədə qanunvericilik bazasının təkmilləşdirilməsi ilə yanaşı, hüquq mühafizə, təhlükəsizlik orqanları, eləcə də Rəqəmsal İnkişaf və Nəqliyyat Nazirliyinin müvafiq strukturlarında mühüm işlər görülür. "İnformasiya təhlükəsizliyinin milli təhlükəsizliyin ayrılmaz hissəsi kimi qiymətləndirildiyi ölkələrdə kibertəhlükəsizlik sahəsində yaranmış insidentləri araşdırmaqla məşğul olan və bu sahədə ən yaxşı mütəxəssislərdən ibarət olan xüsusi təşkilat və qruplar yaradılır. Belə ekspert qruplarının qarşısında duran əsas vəzifə həm ayrı-ayrı təşkilatlar, həm də dövlət miqyasında kibermühitdə təhlükəsizliyin təmin edilməsidir" [3, s.246-247].

Bu sahədə Xüsusi Rabitə və İnformasiya Təhlükəsizliyi Dövlət Xidmətinin üzərinə mühüm vəzifələr düşür. Xidmətin tabeliyində olan Kompüter İnsidentlərinə qarşı Mübarizə Mərkəzi CERT dövlət orqanlarına məxsus şəbəkələrdə kompüter insidentlərinin idarə olunması və onların qarşısının alınması üçün əlaqələndirmə funksiyasını icra edir, insdentlərin aradan qaldırılması yönündə xidmət

göstərir. Mərkəzin vəzifə və funksiyalarına istifadəçilərdən kompüter təhlükəsizliyinə müasir təhdidlər barədə məlumatların alınması, kompüter texnikası və proqram təminatı istehsalçılarından, xarici dövlətlərdəki anoloji qurumlardan informasiyaların toplanılması, eləcə də kompüter insidentlərinə reaksiyaların verilməsi, kompüter sistemlərinin qorunması üçün tətbiq edilən proqramların səmərəsinə dair materialların əldə olunması, təhlili və onların məlumat bazasında yığılması daxildir. İnsidentlərə qarşı mübarizə ilə bağlı beynəlxalq təcrübənin öyrənilməsi, bu yöndə yeniliklərin əxz olunması və tətbiqi, haker hücumlarının qarşısının alınması, beynəlxalq əməkdaşlıq, kompüter cinayətləri və ümumilikdə informasiya təhlükəsizliyi ilə bağlı qabaqlayıcı tədbirlərin görülməsi, xarici ölkələrin "CERT" mərkəzləri və şöbələri ilə qarşılıqlı fəaliyyət və əməkdaşlıq, kompüter viruslarının tətbiqi zamanı əks tədbirlərin görülməsi və yeni dayanıqlı proqram təminatı kimi məsələlər də Kompüter İnsdentlərinə qarşı Mübarizə Mərkəzinin funksiya və vəzifələrinə aiddir. Bu mərkəz şəbəkə və iri server resurslarının iş qabiliyyətinin pozulması, sistemə edilmiş müdaxilə hallarına qarşı tədbirlər görür, ayrı-ayrı hostlara DOS və DDOS hücumlarını təhlil və emal edir, lazımi addımlar atır, parolların sındırılması, məqsədyönlü şəkildə göndərilmiş virusların zərərsizləşdirilməsi, zərərli proqramların qarşısının alınması ilə bağlı addımlar atır. Kompüter İnsidentlərinə qarşı Mübarizə Mərkəzinin nəzdində fəaiyyət göstərən Zərərvericilərin Tədqiqi Laboratoriyası zərərverici vasitələri analiz edir və araşdırır. Mərkəzin saytı isə istifadəçilərlə qarşılıqlı informasiya mübadiləsini təmin edir, kompüter sistemlərinin mühafizəsi və qorunması, təhlükəsizliyinə dair tövsiyə olunan sistem və proqramların siyahısını, bununla əlaqədar yenilikləri təqdim edir, lazımi informasiya və sorğuları öz səhifələrində yerləşdirir.

Mövcud olan təhdid və təhlükələrin qarşısını almaq, onlara qarşı hazır olmaq məqsədilə Kompüter İnsidentlərinə qarşı Mübarizə Mərkəzi öz işini yeniləyir, daha çevik mexanizmlərin yaradılmasına səy göstərir. Bu baxımdan Xüsusi Rabitə və İnformasiya Təhlükəsizliyi Dövlət Xidməti tərəfindən yaradılan "Blacklist.gov.az" layihəsi xüsusi əhəmiyyət daşıyır. Bu layihə özündə "Qara siyahı" saytını ehtiva edir. Bu saytın əsas funksiyası isə internet istifadəçilərinin işini əngəlləyən, problem yaradan hallar barədə məlumat vermək, haker hücumları ilə bağlı xəbərdarlıq etmək, haker səhifələrinin adlarını açıqlamaqdır. Beləki, hər bir istifadəçi qurum və yaxud fərd həmin sayta daxil olaraq qara siyahı barədə məlumat əldə edə və öz faəliyyətini daha təhlükəsiz şəkildə qura bilər. Həmin siyahıda olan zərərverici saytların adı göstərilir və bildirilir ki, onlara daxil olmaq problem yaradacaq. Bununla yanaşı, istifadəçilər şübhəli hesab etdikləri saytlar barədə Xüsusi Rabitə və İnformasiya Təhlükəsizliyi Dövlət Xidmətinin kompüter insidentlərinə qarşı Mübarizə Mərkəzinə məlumat verə bilərlər ki, bu qurum zərərli saytları analiz edib siyahıya əlavə etsin. Zərərli məzmun daşıyıcısının skrinşot görüntüsü, zərərli məzmunun növü, digər əlamətlər və xarakteristikası da siyahıda öz əksini tapır. Bu məlumatları əldə edən mütəxəssislər müxtəlif sistem və şəbəkə qurğuları üçün funksiyaları tətbiq etməklə zərərli saytın faəliyyətini bloklamaq imkanı qazanırlar.

Aparılmış statistikaya əsasən, 2022-ci ildə kiberhücumlar nəticəsində dünya iqtisadiyyatına ümumilikdə 8 trilyon dollarlıq ziyan vurulub. Bu, dünya üzrə Ümumi Daxili Məhsulun 8 faizi qədərdir. Ölkəmizdə 2023-cü ildə 120 mindən çox insanın fərdi məlumatlarının haker və digər zərərli istifadəçilər tərəfindən oğurlanması halları aşkarlanıb. 2022-ci ildə ölkəmizin milli resurslarına 1300-dən çox kiberhücum qeydə alınıb. Bu cür halların qarşısının alınması və onların minimum həddə endirilməsi üçün ölkə prezidenti Cənab İlham Əliyev "Azərbaycanın informasiya təhlükəsizliyi və kibertəhlükəsizliyinə dair 2023-2027-ci illər üçün strategiya"nı təsdiq edib. Həmin strategiya bu sahədə işlərin planlı və mərhələli surətdə həyata keçirilməsi məqsədi daşıyır. "Təbii ki, İnternet üzərindən hücumların qarşısının alınması üçün mütəmadi olaraq təhlükəsizlik məqsədilə nəzərdə tutulmuş protokolların üzərində təkmilləşdirmə işləri aparılır. Lakin bu dəyişikliklər ondan xəbər verir ki, hakerlər dayanmadan protokolları analiz edir və sonda yenə də hücum üçün yol tapırlar. Deməli, nə qədər dəyişiklik olsa da təhlükəsizliyi ideal səviyyədə təmin etmək mümkün deyil. Nəticə etibarı ilə qeyd etmək olar ki, müasir sənaye idarəetmə sistemlərinin təhlükəsizliyini İnternet üzərindən cloud ilə əlaqələndirilməsində müxtəlif şifrələmə metodları kifayət etmir [1, s.9-12].

İnformasiya təhlükəsizliyinə xələl gətirən hallardan biri də ayrı-ayrı fərdlərin sosial şəbəkələrdəki qanunazidd, həqiqətə əsaslanmayan informasiya və videogörüntülər yaymasıdır. Vaxtilə baş vermiş hadisəni yeni kimi təqdim etmək, onu yeni tarixlə vermək hallarına tez-tez rast gəlinir. Cə-

miyyətimiz üçün çox həssas məsələ olan müharibə mövzusunda görüntüləri paylaşmaq, guya Ermənistan-Azərbaycan sərhəddində silahlı toqquşmaların olması və ordumuzun itkilər verməsi barədə informasiya, xəbər, məlumatlar təqdim olunması ictimaiyyətdə çaşqınlığa və əhali arasında xof yaratmağa xidmət edir. Bu cür hallara "Teleqram", "Tik-tok" və "Yutobe" şəbəkələrində rastlaşırıq. Baxmayaraq ki, müvafiq dövlət qurumları, Müdafiə və Daxili işlər nazirlikləri, Dövlət Təhlükəsizliyi Xidməti, Medianın İnkişafı Agentliyi və Mətbuat Şurası bununla bağlı müraciətlər edir və bu cür feyk xəbər, eləcə də görüntülər yayan şəxslərə xəbərdarlıq edir, bununla belə onlar bu çirkin əməllərindən əl çəkmir, baxış sayını artırmaq üçün bu fəaliyyəti davam etdirirlər. Ölkəmizin hüquq-mühafizə orqanları bu cür "vətənpərvərlərə" qarşı tədbirlər görüb, onları məsuliyyətə cəlb etsələr də belə hallara son qoyulmur.

Kiberhücumlar ölkələrin maliyyə və bank sahələri üçün də ciddi problemlər yaradır. Kiberdələduzlar tərəfindən hazırlanan bu hücumlar tərtib edilən saxta sayt və digər platformaların tətbiqi ilə maliyyə və bank qurumlarının işini pozmaqla bərabər, vətəndaşları da öz torlarına sala bilirlər. Məsələn, kibercinayətkarlar "Teleqram" tətbiqində ölkənin ən iri banklarından olan "Kapitalbank"ın adından saxta səhifə yaradıb və öz çirkin əməllərini həyata keçirməyə nail olublar. Onlar müxtəlif elektron səhifələrdə saxta kampaniyalar barədə məlumatlar paylaşır, insanları çaşdırırlar. Həmin keçidlər bankın rəsmi domen ünvanı ilə oxşar olduğundan linki klik etdikdə vətəndaşların bank kartı və digər fərdi məlumatları oğurlanır, saxta veb-sayta yönəldilir. Belə hallarla dünyanın hər bir ölkəsində üzləşilir. 2022-ci ildə Böyük Britaniyada kiber fırıldaqçılar tərəfindən vurulan ziyanın məbləği 1 milyard 200 milyon funt sterlinq olub. Ölkəmizdə bu cür halları minumuma endirmək üçün müəyyən tədbirlər görülür. Azərbaycan Mərkəzi Bankının hazırladığı strategiya müvafiq təhlükəsizlik tədbirlərinin icrası üçün nəzərdə tutulub. Bu strategiya 2023-2026-cı illəri əhatə edir. Bu planın məqsədi maliyyə bazarlarında kibersabitliyi, dayanıqlığı təmin etməkdir. Strategiyanın digər istiqaməti bu sektorda informasiya təhlükəsizliyinin gücləndirilməsidir. Bu strategiyaya əsaslanan başqa bir vəzifə isə kibernetika sahəsində yüksək ixtisaslı mütəxəssislərin hazırlanması ilə kadr potensialının artırılmasıdır. "Kibertəhlükəsizliyin etibarlı təmin edilməsi dövlətin təkbaşına imkanları xaricindədir, bu problemin həlli bütün maraqlı tərəflərin-dövlətin, özəl sektorun və vətəndaşların tərəfdaşlığını və əməkdaşlığını tələb edir. Kibertəhdidlərin transsərhəd xarakteri ölkələri kibertəhlükəsizlik sahəsində sıx əməkdaşlığa sövq edir" [4].

Kibertəhlükələrlə mübarizə məqsədilə beynəlxalq təşkilatlarla əməkdaşlıq və müvafiq konvensiyalara qoşulmaq da zəruri məsələlərdən biridir. Ölkəmiz 2008-ci il 30 iyun tarixində Budapeşt Konvensiyasına qoşulub. "Kibercinayət haqqında" Konvensiyaya qoşulan ölkələrin əksəriyyəti Avropa Şurasına üzv olan dövlətlərdir. 2001-ci il noyabrın 23-də qəbul edilən bu konvensiya kibercinayətkarlıqla mübarizə üçün çox vacib sənəd olsa da, onun bəzi maddələrinin tələbləri bir çox ölkələr tərəfindən bəyənilmir. Belə ki, konvensiyanın 32 b bəndinin dövlətlərin milli suverenlik prinsipinə zidd olduğu bildirilir. Çünki, konvensiyaya qoşulan ölkə digər dövlətlərə öz ərazisində təhqiqat aparmağa icazə verməklə öz suverenlik hüququnu qismən itirmiş hesab olunur. Bununla belə, konvensiyaya üzv ölkələr öz qanunlarını bu sənədin tələblərinə uyğunlaşdırır, əməkdaşlıq üçün hüquqi zəmin yaradırlar. Qeyd edək ki, kibertəhdidlərlə səmərəli mübarizə üçün cinayət hüququ ilə bərabər, cinayət-prosessual hüquqi mexanizmlərin və müvafiq araşdırma texnikalarının inkişaf etdirilməsi zərurəti də həmin konvensiyanın izahedici mətnində yer alıb. "Həcmindən və hədəf obyektlərinin sayından asılı olmayaraq yalnız bir və ya eyni anda bir neçə mənbədən, avtomatlaşdırılmış formada idarə oluna bilən transmilli xarakterli kibercinayətkarlıqla mübarizə daha intensiv və adekvat mübarizə tədbirlərinin və mexanizmlərinin tətbiqini zəruriləşdirir. Buna görə də informasiyalaşdırmaya yatırılmış investisiya ilə informasiya infrastrukturunun və vətəndaşların mühafizəsinə ayrılmış resurslar arasındakı mütənasibliyin asılılıqla risk arasındakı mütənasibliyə əsasən müəyyən olunması vacibdir" [2].

Zamanın tələbi ilə ayrı-ayrı dövlətlərdə kibertəhlükələrlə mübarizə üçün yeni qoşun növləri də formalaşdırılıb. ABŞ ordusunda müstəqil qoşun növü kimi yaradılan Kiber Qüvvələrin 20 mindən çox heyəti var. Onu da qeyd edək ki, kiber müharibənin əsas taktika və strateji istiqamətləri ABŞ-ın Hərbi Doktrinasında öz əksini tapıb. "Artıq dünyanın bir çox orduları kiber hücumlara qarşı praktiki döyüş təlimlərini döyüş hazırlığı proqramlarına daxil edirlər. 2008-ci ildə yaradılan NATO-nun Kiber Təhlükələrə Qarşı Mübarizə üzrə Təcrübə Mərkəzinin (CCDCOE) təşkil etdiyi təlimlərdə o za-

man üçün yenilik sayılan, hərəkətdə olan sürət qatarını dayandırmağa nail olublar". Bu, təlimlərdə iştirak edən hakerlərdən bir qrupu tərəfindən həyata keçirilib. Hazırda isə informasiya-kommunikasiya texnologiyaları o dərəcədə inkişaf edib ki, indi hətta nüvə sənayesi və istənilən kritik informasiya sistemlərinə müdaxilə etmək, onların işini pozmaq, hətta əks məqsədlər üçün istifadə etmək mümkündür" [6].

Dünyanın yüksək reytinqli şirkətlərinin hazırladıqları hesabata əsasən, 2023-cü ildə təhsil və səhiyyə sektoru kiberhücumlara daha çox məruz qalıb. "Checkpoint (Çekpaynt) şirkətinin hesabatına əsasən, 2023-cü ildə təhsil və tədqiqat müəssisələri(institutlar) ən çox hədəflənən sektor olaraq qalıblar, bununla yanaşı Səhiyyə sektoruna hücumlar əvvəlki illə müqayisədə 74% artıb"[5]. Bununla belə, son vaxtlar qarşıdurmalar nəticəsində müəyyən olunub ki, "AzStateNet" şəbəkəsi istifadəçiləri də tətbiq edilən antivirus sistemi və "Candbox" mühafizə sistemi sayəsində sayı milyonlarla ölçülən zərərverici tərkibli elektron sənəd bloklanıb və zərərsizləşdirilib.

Nəticə. Kibertəhlükələrin qarşısını almaq, onların təsirini azaltmaq və nəticələrini aradan qaldırmaq üçün həm dövlətin, həm də elmi ictimaiyyətin üzərinə mühüm vəzifələr düşür. Bu məsələdə hakimiyyət orqanları idarəedici və hüquqi zəmin əsasında fəaliyyət göstərirsə, elmi qurumlar, tədqiqatçı və texnoloqlar dövrün tələblərinə uyğun araşdırma aparırır, hakerlər və kibercinayətkarlığa qarşı əks tədbirlər görürlər. 21-ci əsrin bəlası səviyyəsinə gələn kibertəhdidlərin neytrallaşdırılması, kiberfırıldaqçıların şəbəkəsini ifşa etmək, dövlət və fərdlərin maddi və mənəvi sıxıntılarının aradan qaldırılması yollarını tapmaq ən ümdə məsələlər sırasındadır. Bu məsələdə koordinasiyalı fəaliyyət, təcrübə mübadiləsi, beynəlxalq səviyyədə əməkdaşlıq ümumi işin uğurla nəticələnməsinə mühüm töhvələr verir. Bu baxımdan "Kibertəhdid müasir problem kimi" mövzusunda araşdırma xüsusi əhəmiyyət daşıyır. Belə ki, elmi-texnoloji yeniliklər fonunda cinayətkar ünsürlərin cəmiyyətə meydan oxuması, həyat ahənginə manea yaratmalarına imkan verilə bilməz və onları zərərsizləşdirmək üçün səmərəli iş aparılması gündəlikdə duran prioritet mövzudur. Tədqiqat işində müasir problemə çevrilən kibertəhdidlə bağlı məsələlər diqqət mərkəzində saxlanılıb, ona qarşı atılan və atılacaq addımlarla əlaqədar elmi təhlil aparılıb, bu yöndə birgə əməkdaşlığa dair elmi mülahizələr irəli sürülüb. Elmi-texnoloji inkişaf fonunda yaranmış vəziyyətdən cinayətkarlıq məqsədilə istifadənin yolverilməzliyi vurğulanıb, əks tədbirlərin görülməsi üçün zəruri amillər ön plana çıxarılıb, vəziyyətdən çıxış yolları təhlil edilib, statistik məlumatlar əsasında faktlar analiz edilib, nəticələri dəyərləndirilib. Beynəlxalq təcrübəyə əsaslanan fəaliyyətin zəruriliyi haqqında fikirlər əsaslandırılıb, qanunvericilik bazasının təkmilləşdirilməsinə dair fikirlər irəli sürülüb.

ƏDƏBİYYAT

1. Abbasov Ə. Süni intellektin informasiya təhlükəsizliyində tətbiqi:problemlər və perspektivlər / "İnformasiay təhlükəsizliyi: problemlər və perspektivlər" mövzusunda II Beynəlxalq Konfransın materialları. Bakı, 2022, s.9-12.
2. Balacanov E. Kibercinayətlərlə mübarizə: çətinliklər və imkanlar. İnformasiya təhlükəsizliyinin multidissiplinar problemləri üzrə II respublika elmi-praktiki konfransı, 14 may 2015-ci il. - https://ict.az/uploads/konfrans/2_konfrans/13.pdf [25.04.2025].
3. Əliyeva L. Kibertəhlükəsizlik sahəsində əhalinin maarifləndirilməsi və məlumatlandırılması məsələsinə bir yanaşma / İnformasiya təhlükəsizliyinin multidissiplinar problemləri üzrə II respublika elmi-praktiki konfransı, 14 may 2015-ci il.
4. İmamverdiyev Y. Milli kibertəhlükəsizlik strategiyalarının analizi / Ümummilli lideri Heydər Əliyevin 90 illik yubileyinə həsr olunmuş "İnformasiya təhlükəsizliyi problemləri üzrə I respublika elmi-praktiki konfransı", 17-18 may, 2013, s.14-17.
5. İsmayilov A. Haker qurbanı olmuş vətəndaşların sayı ötən dövr ərzində 7000-dən çox olub. - https://oxu.az/cemiyyet/ [25.04.2025].
6. Kibertəhlükəsizliyin əsasları, texnologiya və vacib olan nüanslar. https://ordu.az/az/news/135746 [25.04.2025].

ЭЛЬШАД ГАСАНЛИ
Ведущий научный сотрудник Института философии и социологии НАНА,
Доктор философии по политическим наукам, доцент

КИБЕРУГРОЗА: АКТУАЛЬНЫЕ ПРОБЛЕМЫ СОВЕРЕМННОСТИ

В нынешнее время, когда технологические новшества проникают во все сферы деятельности, рост киберугроз становится серьезной проблемой. В связи с этим принятие мер, нейтрализация опасности и применение превентивных шагов – задача, стоящая как перед государственными органами, так и перед исследовательскими центрами. В исследовании анализируются и оцениваются способы киберугрозы, разоблачение деяний киберпреступников, пути борьбы с ними, обмен опытом, полученном на этом пути, вопросы межгосударственного и межструктурного сотрудничества, деятельности правоохранительных органов, а также работа, связанная с совершенствованием законодательной базы.

Ключевые слова: Безопасность, киберпреступление, кибербезопасность, компьютерные системы, государство, конфликт, мир, политика.

ELSHAD HASANLI
Leading Researcher at the Institute of Philosophy and Sociology of ANAS,
PhD in Political Science, Associate Professor

A CYBER THREAT: THE ACTUAL PROBLEM OF THE TIME

The growth of cyber threats in nowadays, when the technological innovations apply to per activity scope of activity, is actual as a serious problem. Both state authorities and research centers bear duty to take measures regarding it, to neutralize the security and to make preventive steps. Cases such as cyber threat method, exposing of cybercriminals' actions, the method of struggle with them, exchange of experience acquired in this way, intergovernmental and inter-agency cooperation issues, activity of law enforcement authorities and as well as improvement of legislative basis have been analyzed and evaluated in the study.

Keywords: Security, cybercrime, cybersecurity, computer systems, state, conflict, peace, politics.

Məqalənin redaksiyaya daxil olduğu tarix: 25 aprel 2025-ci il.
Məqalənin çapa qəbul olunma tarixi: 15 may 2025-ci il.
Rəyçilər: s.e.ü.f.d. Kərəm Məmmədov, s.e.d. Adil Mirabdullayev.