UOT 1615 Q 436 A

N. N. QASIMOVA

Heydər Əliyev adına Azərbaycan Ali Hərbi Məktəbi
E-mail: nazaket-qasimova@mail.ru

AVTOMATLAŞDIRILMIŞ İDARƏETMƏ SİSTEMLƏRİNDƏ KİBERTƏHLÜKƏSİZLİYİN ELMİ-TEXNİKİ PROBLEMLƏRİ VƏ ONLARIN HƏLL YOLLARI

Məqalədə kibertəhlükəsizliyin təmininin aktual problemlərinə baxılır, hərbi və dövlət idarəetmə orqanlarının avtomatlaşdırılmış idarəetmə sistemlərində müasir təhdidlərə qarşı kibertəhlükəsizliyinin təminində adekvat yanaşma sistemləri təklif edilir.

Açar sözlər: kibertəhlükəsizlik, informasiya təhlükəsizliyi, kiberfəza, informasiya qarşıdurması.

Dövlətlərin milli, hərbi və iqtisadi təhlükəsizliyinin təmin edilməsi məsələlərinin həllində yüksək inkişaf mərhələsi keçmiş informasiya texnologiyaları, kompüter şəbəkələri və sistemləri tətbiq olunur.

İnformasiya resurslarının kütləvi istifadəsi və proqramlaşdırma texnologiyalarının təkmilləşməsi informasiya təhlükəsizliyinin təmin olunması üçün daha böyük əmək tələb edən və baha başa gələn bir prosesə çevrilmişdir.

Kompüter sistemlərinin və şəbəkələrinin işinə qeyri-qanuni müdaxilə, kompüter informasiyasının oğurlanması, mənimsənilməsi, zorla, şantaj yolu ilə alınması kimi təhlükələr "kompüter cinayətkarlığı" və "kompüter terrorçuluğu" kimi ad almış, "kiberhücum", "kibertəhdid" və "kibertəhlükəsizlik" kimi anlayışların yaranmasına səbəb olmuşdur [1].

Yüksək texnologiyalara əsaslanan kompüter terrorçuluğu inkişaf etmiş informasiya mübadiləsi infrastrukturuna malik olan ölkələrdə sistemli kritik vəziyyətlərin yaranmasına səbəb olmaq qabiliyyətinə malikdir. Bu zaman kompüterlər və onların bazasında yaradılmış xüsusi sistemlər, o cümlədən bank, arxiv, tədqiqat və idarəetmə sistemləri, eləcə də televiziyadan və rabitə peyklərindən tutmuş radiotelefonlara və peycerlərə qədər müxtəlif kommunikasiya vasitələri terrorçuların hədəfinə tuş gələ bilir. Yəni kibercinayətlər xarakter və xüsusiyyətlərinə görə iqtisadiyyat sahəsini və bank strukturlarını, hərbi, atom energetikası, kosmik tədqiqatlar, informasiya texnologiyaları, tibb sahələrini əhatə etməklə bir-birindən fərqlənir.

Azərbaycanın kibermәkanı dünya kibermühitinin bir hissəsidir. Elektron hökümətin yaradılması, dövlətin sosial və vergi siyasətinin avtomatlaşdırılması informasiya təhlükəsizliyi məsələsini aktuallaşdırmışdır [2].

Müasir şərtlərlə kibertəhlükəsizlik təhdidlərinin qarşısının alınması və kiberhücumlara mümkün cavab tədbirlərinin təmin olunması məqsədilə hərbi və dövlət idarəetmə orqanlarının avtomatlaşdırılmış idarəetmə sistemləri (HDİO AİS) avtomatlaşdırma və kompüterləşdirmə istiqamətində daha da mükəmməlləşdirilməlidir. Bunu nəzərə alaraq həm sülh, həm də müharibə dövründə kibertəhlükəsizliyin təmin olunması baxımından HDİO AİS-nin qurulma prinsiplərinin yenidən işlənməsi vacib tələb kimi qarşıda durur.

Kibertəhlükəsizlik sahəsində mütəxəssislərin fikrincə texniki cəhətdən tam adekvat kibermühafizə aşağıdakı altsistemlərin qurulmasını və istifadəsini nəzərə almalıdır:

-mühafizə altsistemi (Protection Capabilities)-kompüter təhlükəsizliyi (Computer Security),

- informasiya təhlükəsizliyi (İnfoSec), rabitə sistemləri və vasitələrinin təhlükəsizliyi təmin edir;

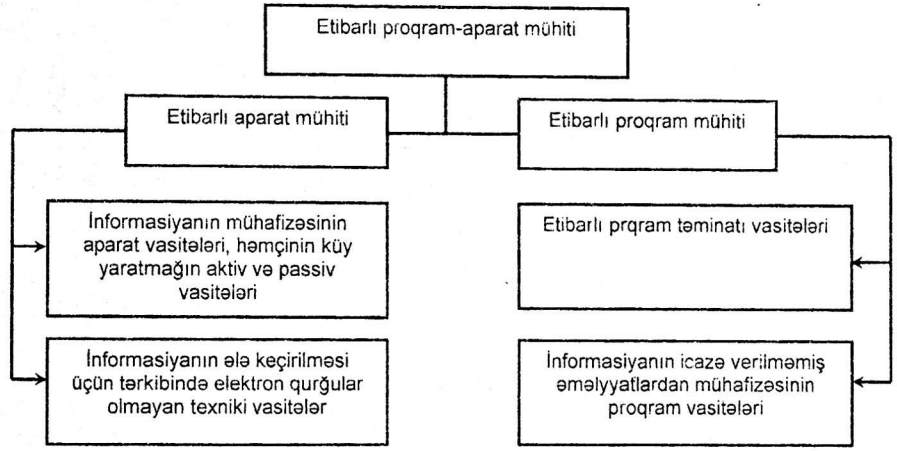
- tanıma altsistemi (Detection Capabilities) - şəbəkədə müxtəlif anomaliyaları müəyyən etməyə imkan verir;

- vəziyyət və texniki parametrlərin dəyişməsinə reaksiya verən altsistem (Reaction Capabilities) [3].

Lakin göstərilən bu tələblərlə qurulan kibermühafizə sistemi informasiyalaşdırma obyektinin, ilk növbədə HDİO AİS-də kibertəhlükəsizliyi tam təmin edə bilmir. HDİO AİS kibertəhlükəsizliyi informasiya təhlükəsizliyinin bir hissəsi olan kibertəhlükəsizliyin vahid intellektual sistemi ilə yerinə yetirilməllidir. Buna görə də qurulan bu sistemin əsasına sistemin təkamülü anlayışı da daxil edilməlidir, yəni sistemin bütün həyat dövrü ərzində daxili və xarici kibertəhlükələrin (kiberhücumların) təsiri ilə parametrlərin dəyişməsinə sistemin adaptasiya qabiliyyəti nəzərə alınmalıdır.

HDİO AİS intellektual sistemi kiberfəzada nəinki yeni və məlum olmayan kiberhücumları aşkar edə bilməlidir, həm də onları analliz etməli, bundan asılı olaraq AİS fəaliyyət parametrlərini avtomatik seçə bilməlidir.

HDİO AİS-də kibertəhlükəsizlik sistemləri qurularkən vacib şərtlərdən biri etibarlı aparat-proqram vasitələrinin tətbiqidir. Etibarlılıq – müasir informasiya qarşıdurması şəraitində müəyyən texnoloji müstəqillik şərtlərini qorumaqla informasiya təhlükəsizliyi sahəsində qoyulan tələblərə ciddi və təminatlı uyğunluqdur [4]. Etibarlı proqram-aparat mühiti dedikdə texniki və proqram vasitələrinin toplusu, informasiya təhlükəsizliyinin tələblərinə uyğun sistemin dayanıqlı fəaliyyətini təmin edən təşkilatı tədbirlərin məcmusu başa düşülməlidir (şəkil1).



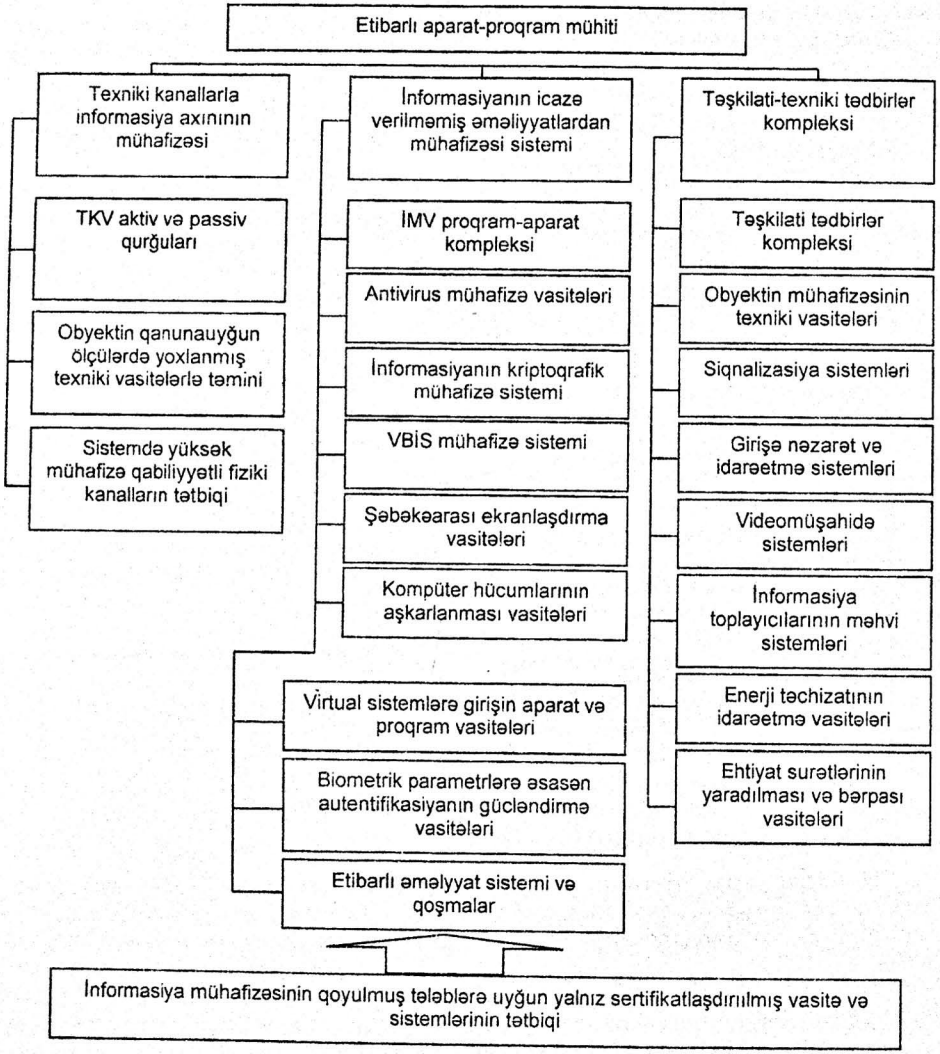
Şəkil 1. Etibarlı proqram-aparat mühitinin təminin əsasları

Etibarlılığın əsas kriteriyası müasir informasiya qarşıdurması şərtlərində AİS-nin informasiya təhlükəsizliyinin tələblərinə cavab verməsidir. Aparat-proqram mühitinin etibarlılığı faktiki istifadə olunan aparat (proqram-aparat) vasitələrinin və proqram təminantının etibarlılığı ilə təyin olunur.

HDİO AİS obyektlərində informasiya təhlükəsizliyini təmin etmək üçün effektiv kibertəhlükəsizlik sistemlərinin qurulması kompleks yanaşmanı tələb edir. Şəkil 2-dən göründüyü kimi buna təşkilati-texniki tədbirlər kompleksinin işlənməsi və reallaşdırılması, informasiyanın texniki kanallar vasitəsilə axınının mühafizəsi, informasiyanın icazə verilməmiş əməliyyatlardan mühafizəsinin proqram-aparat vasitələrinin rasional birləşdirilməsi ilə nail olmaq olar.

Bu baxımdan HDİO AİS-də kibertəhlükəsizlik sistemləri öz aralarında əlaqəli olan bir neçə funksional sistemdən ibarət olmalıdır: kiberfəzanın monitorinqi (kəşfiyyatı), informasiyanın kompleks mühafizəsi, kiberhücumlar haqqında xəbərdarlıq və kiberhücumlara qarşı aktiv fəaliyyətlər sistemi. Bunları nəzərə alaraq HDİO AİS kibertəhlükəsizlik sistemlərinin təklif edilən struktur sxemi şəkil 3-də göstərimişdir.

Kiberfəzanın monitorinqi (kəşfiyyatı) sistemi kiberfəzada vəziyyətin qiymətləndirilməsini, mümkün kibertəhlükələrin mənbəyi, xarakteri, məzmunu, miqyası, vaxtı haqqında informasiyanın mütəmadi toplanmasını və emalını, informasiya infrastrukturuna kiberhücumların reallaşdırma texnologiyaları və mümkün variantların proqnozlaşdırılmasının ixtisaslaşdırılmış aparat-proqram vasitələrini ehtiva etməlidir.



Şəkil 2. İnformasiya təhlükəsizliyinin təminində kompleks yanaşmanın effektiv sistemi

İnformasiyanın mühafizəsinin kompleks sistemi özündə informasiya mühafizəsinin müasir sistemlərini (İMS) və onların effektivliyinin yoxlanması vasitələrini birləşdirməlidir. Bura aid edilir:

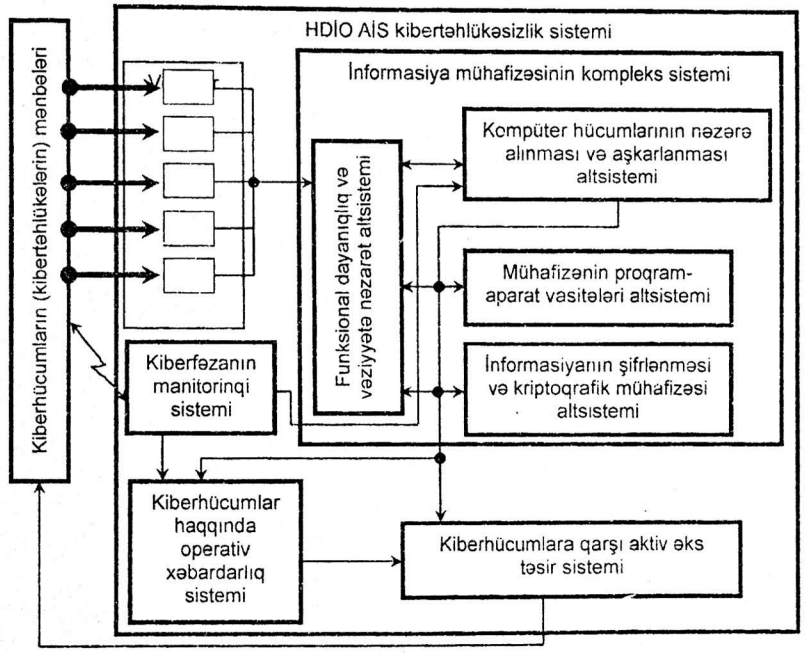
- kompüter hücumları haqqında xəbərdarlıq və aşkarlanması sistemləri;
- icazə verilməmiş əməliyyatlardan mühafizənin proqram-aparat vasitələrinin altsistemi;
- informasiyanın kriptoqrafik mühafizəsi və şifrlənmsi altsistemi;
- funksional dayanıqlıq və vəziyyətə nəzarət altsistemi.

Kiberhücumlar haqqında xəbərdarlıq və kiberhücumlara qarşı aktiv fəaliyyətlər sistemi informasiyanın vaxtında əldə edilməsi və idarəetmə orqanlarına çatdırılmasını təşkil etmək üçün bir-biri ilə əlaqəli proqram-aparat və telekommunikasiya vasitələrinin məcmusudur.

Kiberhücumlara qarşı aktiv əks təsir sistemi hücum hərəkətlərinə qarşı müqavimət vasitələrinin optimal strategiyasını planlaşdırmalı, həmçinin qarşı tərəflərin informasiya obyektlərinin məhvetmə vasitələrini cəmləməlidir.

Kiberhücumlar haqqında operativ xəbərdarlıq sistemi real zamanda mümkün kiberhücumlar, kibertəhlükələr haqqında əlaqələndirilmiş aparat-texniki və telekommunikasiyia vasitələrinin məcmusunu təşkil edir [5].

Bütün bu sistem və altsistemlərin işi hüquqi-normativ sənədlərlə tənzimlənməlidir.



Şəkil 3. HDİO AİS kibertəhlükəsizlik sisteminin struktur sxemi

HDİO AİS-də kibertəhlükəsizliyin təmini üzrə dünya təcrübəsi onu göstərir ki, vəziyyətin analizinin, proqnozlaşdırılmasının və modelləşdirilməsinin yeni metodlarından istifadə etməklə təşkilati və operativ-texniki tədbirləri nəzərdə tutan bütöv sistemin yaradılması vacibdir. Belə ki, HDİO AİS-də kibertəhdidlərin reallaşması idarəetmə orqanlarına, hərbi qüvvələrə-bütövlükdə dövlətin milli təhlükəsizliyinə ziyan vurmuş olacaq.

HDİO AİS-in kibertəhlükəsizləsizliyinin təkmilləşdirilməsi və inkişafının əsas istiqamətləri dövlət səviyyəsində vahid elmi-texniki siyasət və proqram-aparat vasitələrinin vahid reyestrini hazırlamaq, kibermühitin sistemli monitorinqini və kibertəhlükəsizlik sahəsində kadr siyasətini yerinə yetirməklə həyata keçirilməlidir.

NƏTİCƏ

Hazırki dövrdə nəticə etibarilə ölkənin milli təhlükəsizliyinin təmin olunmasına yönələn kibertəhlükəsizlik hərbi-sənaye komplekslərində, dövlət idarəetmə orqanlarında yeni inkişaf edən sahə kimi daha böyük məna kəsb edir. Həm qlobal, həm də regional səviyyələrdə informasiya qarşıdurmasının və kibertəhlükəsizliyin təmini tədbirlərinin vaxtında planlaşdırılması və reallaşdırılması milli təhlükəsizlik sahəsində ölkənin prioritet istiqamətlərindən biridir.

ƏDƏBİYYAT

1. Qasımov, V.Ə. İnformasiya təhlükəsizliyi: kompüter cinayətkarlığı və kiberterrorçuluq. Monoqrafiya / V.Ə. Qasımov. - Bakı: Elim, - 2007. – 192 s.

2. Qasımova, N.N. Müasir müharibə məkanı - kibermәkanda təhlükəsizlik tədbirləri haqqında // , - Bakı: H.Əliyev adına AAHM, Elmi əsərlər məcmuəsi, - 2016. № 2(27), - s.9-13.

3. Бородакий, Ю.В. Кибербезопасность как основной фактор национальной и международной безопасности XXI века (Часть 1) / Ю.В. Бородакий, А.Ю. Добродеев, И.В Бутусов // Вопросы кибербезопасности, - Москва: - 2013. - № 1. – с.2-9.

4. Бородакий, Ю.В. Кибербезопасность как основной фактор национальной и международной безопасности XXI века (Часть 2) / Ю.В.Бородакий, А.Ю.Добродеев, И.В Бутусов // Вопросы кибербезопасности, - Москва: - 2014. - № 1. – с.5-12.

5. Цирлов, В.И. Основы информационной безопасности автоматизированных систем. Краткий курс / В.И. Цирлов. – Ростов на Дону: Феникс, - 2008. – 253 с.

SUMMARY

N. N. QASIMOVA

Azerbaijan Higher Military School named after Heydar Aliyev

E-mail: nazaket-qasimova@mail.ru

SCIENTIFIC AND TECHNICAL PROBLEMS OF CYBER SAFETY IN AUTOMATED CONTROL SYSTEMS AND THEIR SOLUTIONS

The article reviews the current issues of cyber security, offers systems for an adequate approach to cyber security against modern threats in the automated control systems of military and government bodies.

Key words: cyber security, information security, cyberspace, information confrontation

РЕЗЮМЕ

КАСИМОВА Н. Н.

Азербайджанское высшее военное училище имени Гейдара Алиева

Электронная почта: nazaket-qasimova@mail.ru

НАУЧНО-ТЕХНИЧЕСКИЕ ПРОБЛЕМЫ КИБЕРБЕЗОПАСНОСТИ В АВТОМАТИЧЕСКИХ СИСТЕМАХ УПРАВЛЕНИЯ И ИХ РЕШЕНИЯ

В статье рассматриваются проблемы обеспечения национальной кибербезопасности и предлагаются подходы к созданию адекватной системы обеспечения кибербезопасности автоматизированных систем органов военного и государственного управления.

Ключевые слова: кибербезопасность, информационная безопсность, кибер-пространство, информационное противоборство.

Məqalə redaksiyaya daxil olmuşdur: 17.06 21