DOI: https://www.doi.org/10.36719/2706-6185/03/32-35

İxtiyar Bəxtiyar oğlu Xanızadə
Milli Aviasiya Akademiyası
magistrant
ixtiyar_xanizade@mail.ru

İNFORMASİYA TƏHLÜKƏSİZLİYİNİN TƏMİNİ PROBLEMLƏRİ

Açar sözlər: *informasiya, informasiya təhlükəsizliyi, kiberterrorizm*

Problems of information security

Summary

The present stage of development is characterized by strong scientific and technical development, which includes high-tech industries. Thus, information and communication technologies (ICT) are one of the main factors influencing the formation of 21st century society. Their revolutionary influence is constantly growing on the security of people's livelihoods, their work and education, and the interaction between the state and civil society. ICT is becoming more and more important stimulus for world community development. However, more precisely, ET development is always accompanied by negative social impacts, including various types of crimes. The rapid development of computer technology, in particular, has led to the expansion of crimes related to electronic processing of information, including crime-related types of terrorism.

The article explores the problems of Information Security at the Airports, and cyber security caused by information security. Particular attention is paid to the illegal acquisition of information, the methods used to protect information, the use of illegally obtained information for personal gain, and the interference in the operation of life support facilities.

Key words: *information, information security, cyberterrorizm*

Giriş

İnformasiya təhlükəsizliyi mülki aviasiya obyektləri üçün ümumi təhlükəsizlik sisteminin ayrılmaz hissəsi kimi son zamanlar davamlı olaraq ortaya çıxan problemlərə görə getdikcə daha çox diqqəti cəlb edir ki, bu da insan həyatının bütün sahələrində informasiya texnologiyalarının tətbiqi ilə əlaqədardır. Beynəlxalq Mülki Aviasiya Təşkilatı (ICAO) getdikcə daha çox mülki aviasiya obyektlərinin informasiya təhlükəsizliyinin təmin edilməsi məsələlərini həll etməyə yönəlmiş müəyyən tədbirlər həyata keçirir. Mülki aviasiya obyektlərinin informasiya təhlükəsizliyi sistemi məlumatların icazəsiz girişdən etibarlı qorunmasını təmin edən mütəşəkkil orqanlar, vasitələr, metodlar və tədbirlər kompleksidir.Bundan əlavə, informasiya təhlükəsizliyini təmin etmək üçün ən vacib şərtlər qanunauyğunluq, yetərlilik, şəxsiyyətin, cəmiyyətin və dövlətin maraqları tarazlığının qorunması, informasiya təhlükəsizliyinin təmin edilməsindən məsul işçilərin peşəkarlığı, məsuliyyəti, dövlət qurumları ilə qarşılıqlı əlaqəsidir. Bütün bu şərtlərə riayət edilmədən, heç bir informasiya təhlükəsizliyi sistemi potensial və real təhdidlərə qarşı lazımi səviyyədə qorunma təmin edə bilməz.

Terroroloqların fikrincə kiberterrorizm son dövrlərdə daha kəskin xarakterdir. **Kiberterrorizm (informasiya terrorizmi)–** kompyuterin yaddaşında saxlanılan və ya kompyuterlərin vahid sistem, şəbəkəyə birləşdirilən rabitə kanalları üzrə sirkulyasiya edən məlumata siyasi məqsədli hücumla ifadə olunan kompleks aksiyalı terror aktıdır. Kiberterrorizmin təhlükəsi ondadır ki, o milli sərhəd tanımır, bu növ terror aktları dünyanın istənilən yerindən həyata keçirilə bilər. İnformasiya fəzasında terroristi aşkara çıxartmaq çox çətindir, çünki, o bir neçə kompyuter vasitəsi ilə həyata keçirilir ki, bu da onun identifikasiya edilməsini və yerləşdiyi məkanın müəyyən edilməsini çətinləşdirir.

İnformasiya – təqdimat formasından asılı olmayaraq şəxslər, əşyalar, faktlar, hadisələr, təzahürlər, proseslər və anlayışlar haqqında məlumatlar və biliklərdir. İnformasiya kompyuterə daxil edilmiş verilənlər, proqram kodları, məktub, yaddaş qeydləri, işlər, düsturlar, sxemlər, çertyojlar, dioqramlar, məhsulun modelləri, prototiplər, elmi işlər, məhkəmə sənədləri və.s formalarda ola bilər. Öz şəxsi maraqlarını, o cümlədən iqtisadi, kommersiya və.s məqsədlərini reallaşdırmaq üçün insanlarda informasiyaya tələbat yaranır, həmin insanları informasiyanın istehlakçısı adlandırırlar.

İnformasiya təhlükəsizliyi - şəxslərin, təşkilatların və cəmiyyətin maraqlarına uyğun olaraq, informasiya mühitinin qorunmasının vəziyyəti, həmçinin informasiya təhlükəsizliyinin pozulması təhdidlərinin, bu təhdidlərin mənbələrinin, reallaşdırılması üsullarının və məqsədlərinin, təhlükəsizliyinin

pozulmasına gətirib çıxaran digər şərait və hərəkətlərin vaxtında aşkar edilməsi və qarşısının alınması vəziyyəti başa düşülür (1).

Kiberhədələr bəzən ən güclü silah qədər təhlükəlidir. Kiberterrorçuların istifadə etdiyi bu növ silahları hətta informasiya silahları adlandırmaqla onları yeni növ kateqoriya kimi (silah növlərindən biri) qiymətləndirmək olar. İnformasiya silahı seçim üzrə fəaliyyət göstərə bilər. O, transsərhəd rabitəsi vasitəsilə həyata keçirilə bilər ki, bu da hücum mənbəyinin aşkar edilməsini qeyri-mümkün edir. Ona görə də informasiya silahı terrorçular üçün ideal vasitədir. İnformasiya terrorizmi isə bütöv bir dövlət üçün təhlükə ola bilər. Bu isə milli və beynəlxalq təhlükəsizlik üçün informasiya təhlükəsizliyini vacib faktor kimi dəyərləndirməyə zərurət yaradır.

İnformasiya – kommunikasiyası, o cümlədən kompyuter texnologiyalarının yaranması ilə eyni zamanda meydana gələn cinayətkarlıq problemləri içərisində kiberterrorizm xüsusi yer tutur. Kompyuter terrorçuluğunun arsenalına və ya onun əsas istiqamətlərinə - müxtəlif virusları, məntiqi bombaları - əvvəlcədən proqram üzrə qurulmuş və lazım olan anda işə düşə bilən komandaları və s. aid etmək olar. Müasir terrorçu interneti yeni silah kimi deyil, əsasən təşviqat aləti, informasiya ötürülməsi vasitəsi kimi istifadə edir. Ona görə də kompyuter terrorizmini, daha doğrusu kiberterrorçuluğu cəmiyyət üçün real təhlükə hesab etmək olar. Hal-hazırda etibarli müdafiə oluna bilən sistemlər demək olar ki, yox səviyyəsindədir. Deməli, kompyuter terrorizmi reallıqdır. Buna görə də bu istiqamətdə dövlət strukturları tərəfindən işlənən və tətbiq edilən texniki, hüquqi və təşkilati tədbirlərin həyata keçirilməsinə böyük ehtiyac vardır. Belə tədbirlər isə öz növbəsində kompyuter sistemlərinin müdafiəsinə fayda verə bilər (1).

Kiberterrorizm anlayışının mahiyyətinə müxtəlif yanaşmalar mövcuddur. Yeni və kifayət qədər öyrənilməmiş bir cinayət hadisəsi olaraq kiber terrorizm xüsusi diqqət və bəşəriyyət üçün təhlükəli olan bu problemin həllinə xüsusi yanaşma tələb edir. Saytları zəbt etməklə, kiber terrorçular gizli məlumatlar da daxil olmaqla müxtəlif növ məlumatlar əldə edir. Narahatçılıq yaradan əsas problem terrorçuların internet, kiber resurslardan istifadə etməklə kütləvi qırğın silahını əldə etmək cəhdləridir. Növündən və xarakterindən asılı olmadan baş verə biləcək istənilən təhlükələrin qarşısının alınması, başqa sözlə sistemdə toplanan, saxlanan və emal olunan, eləcə də şəbəkə vasitəsi ilə ötürülən informasiyanın təhlükəsizliyinin təmin olunması məqsədilə indiyədək çoxlu sayda müxtəlif üsullar, vasitələr və tədbirlər sistemi işlənib hazırlanmışdır.

Kiberterrorizm – kompyuterin yaddaşında saxlanılan və ya kompyuterlərin vahid sistem, şəbəkəyə birləşdirilən rabitə kanalları üzrə sirkulyasiya edən məlumata siyasi məqsədli hücumla ifadə olunan kompleks aksiyalı terror aktıdır. Kiberterrorizmin təhlükəsi ondadır ki, o milli sərhəd tanımır və terror aktlarını dünyanın istənilən yerindən həyata keçirə bilər. İnformasiya təhlükəsizliyi problemi meydana çıxdığı ilk dövrlərdə informasiyanın qorunması üçün, təşkilati və fiziki tədbirlər həyata keçirilməyə başlamışdır. Lakin informasiya texnologiyalarının, o cümlədən kompyuter texnikasının və kommunikasiya avadanlıqlarının inkişafı informasiyanın qorunması məsələsinə daha ciddi və kompleks yanaşma zərurətini yaratdı. İlk dövrlərdə elə fikir formalaşmışdı ki, informasiyanın emalı və ötürülməsi sistemlərində təhlükəsizlik proqram vasitələrinin köməyi ilə daha asan təmin edilə bilər. Ona görə də həmin dövrlərdə informasiyanın qorunması üçün məhz proqram vasitələri daha çox inkişaf edirdi. Bu vasitələrin etibarlılığını artırmaq üçün əlavə olaraq, zəruri təşkilati tədbirlərin və fiziki qoruma mexanizmlərinin köməyindən istifadə edilir. Lakin təcrübə göstərdi ki, informasiyanın etibarlı qorunması üçün yalnız proqram vasitələrinin reallaşdırılması, hətta əlavə təşkilati tədbirlərin tətbiq edilməsi kifayət etmir. Real həyatda praktiki baxımdan informasiya təhlükəsizliyinə qarşı elə təhlükələr yaranır ki, onların qarşısını almaq üçün bu vasitələrin tətbiqi mümkün olmur, bəzən isə bu mexanizmlər arzu olunan nəticəni vermir. Məhz bu səbəb informasiyanın qorunması üçün texniki qurğuların və sistemlərin, o cümlədən aparat vasitələrinin intensiv inkişafına təkan verdi. (4).

Kiberterrorizm internetin açıqlığından istifadə edərək hökümətləri və dövlətləri diskretidasiya etmək üçün terror istiqamətli saytların yerləşdirilməsi, saxta məlumatları daxil etməklə bu sistemləri işçi vəziyyətdən çıxarılması və s. fəaliyyətlə qorxu və həyəcan yaradır, ənənəvi terrorçuluğu özünəməxsusluğu ilə tamamlayır. Tədqiqatlar kiberterrorizmin 2 növünü fərqləndirirlər:

1. Kompyuter və kompyuter şəbəkələrinin köməyi ilə terrorist fəaliyyətin həyata keçirilməsi (“təmiz növ”).
2. Bilavasitə terror aktı törətmək məqsədi ilə deyil, terrorçu qruplar üçün kiberfəzanın istifadəsi.

Kiberterrorizmin birinci növünü “kiberfəza” və “terror aktı” anlayışlarını birləşdirməklə müəyyən etmək olar (2).

Öz məqsədləri üçün partladıcı və ya silahdan istifadə edən adi terrorçudan fərqli olaraq kiberterrorist müasir informasiya texnologiyasından, kompyuter sistem və şəbəkələrindən, xüsusi proqram təminatından

istifadə edir. Hər şeydən əvvəl bunlar məntiqi bombalar adlandırılan kompyuter proqram və resursları, informasiyaları sıradan çıxaran müxtəlif vasitələr "troyan" proqramları və informasiya silahının digər növləridir. Kiberfəzada terror aktını yerinə yetirmək üçün müxtəlif üsullar istifadə olunur:

1. Kiberfəzanın ayrı-ayrı elementlərinə ziyan vurmaq, elektrik qida şəbəkələrini dağıtmaq, maneələr, xüsusi proqramları istifadə etmək;
2. Kiberfəzanın strateji əhəmiyyət kəsb edən informasiya, proqram və texniki resurslarını müdafiə sustemlərinin dağıtmaq yolu ilə virusları tətbiq etməkdə - oğurlamaq və ya məhv etmək.
3. İnformasiya və idarəetmə sistemlərində proqram və informasiya təminatının normal fəaliyyətini pozmaq, dövlətin infrastrukturu haqqında informasiyanın funksional fəaliyyətlə bağlı qapalı informasiyanın açılması və təhlükəli məhvi, o cümlədən ictimai əhəmiyyətli və hərbi informasiya sistemlərinin, şifrələrin, informasiya sistemlərinin işinin pozulması, onların sirrlərinin konfidensiallığının pozulması və s.
4. Telekomunikasiya verilişləri kanallarının dezinformasiyanın genişləndirilməsi məqsədi ilə ələ keçirilməsi və terrorçu təşkilatların gücünü nümayiş etdirmək və öz istəklərini tələblərini elan etmək (5).

2018-ci il			2019-cu il			Sıralamada dəyişiklik
1	Zərərli kodlar/proqramlar*	↑	1	Zərərli kodlar/proqramlar*	↑	⇔
2	Veb-əsaslı hücumlar	↑	2	Veb-əsaslı hücumlar	↑	⇔
3	Veb proqram hücumları	↑	3	Veb proqram hücumları	↑	⇔
4	Botnetlər	↓	4	Botnetlər	↓	⇔
5	Xidmətin imtinası	↑	5	Xidmətin imtinası	↑	⇔
6	Spam	↓	6	Fiziki ziyan/oğurluq/zərər	→	⇧
7	Fişinq (saxta məktublar)	↑	7	Daxili təhdid	↑	⇧
8	Zəiflik müəyyən etmə alətləri	↓	8	Fişinq (saxta məktublar)	→	⇩
9	Məlumat sındırılması	↑	9	Spam	↓	⇩
10	Fiziki ziyan/oğurluq/zərər	↑	10	Zəiflik müəyyən etmə alətləri	↑	⇩
11	Daxili təhdid	→	11	Məlumat sındırılması	→	⇩
12	Məlumatın sızması	↑	12	İdentifikasiya oğurluğu	→	⇧
13	İdentifikasiya oğurluğu	↑	13	Məlumatın sızması	↑	⇩
14	Kiber-casusluq	↑	14	Girov götürmə alətləri	↑	⇧
15	Girov götürmə alətləri	↓	15	Kiber-casusluq	↑	⇩

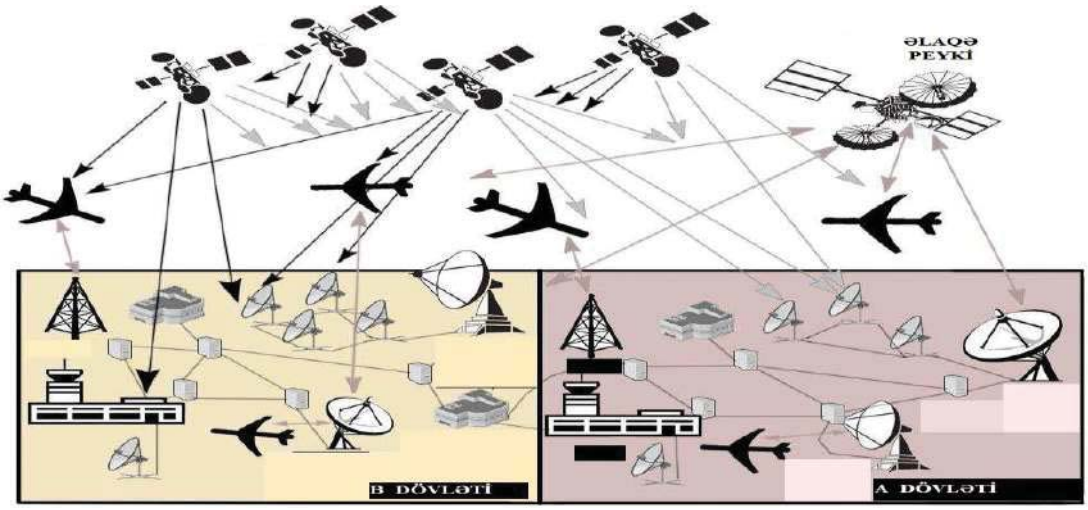
Mənbə: ENISA Təhlükə müstəvisi hesabatı

*soxulcanlar, troya atları, məntiqi bombalar və s.

İzahat:
Trendlər - ↑ artan, ↓ azalan, → stabil
Sıralama - ⇧ yüksəliş, ⇩ düşmə, ⇔ eyni

2018-2019 cu illər üçün hesablanmış cədvələ baxdıqda təhlükənin daima artdığı göz önünə gəlir. 15 faktordan yalnız biri daxili hədələr stabil olaraq qalır. Digər bütün informasiya və elektron idarəetməyə əsaslanan faktorlarda artımlar müşahidə olunur.

MA-da kiberterrorizm o qədər açıq və ciddi şəkil almışdır ki, bu sahədə qeyd edilən problemləri ətraflı tədqiq, təhlil etmək, öyrənmək, sonra isə bu hadisələrin qarşısını ala biləck tədbirlər, aktiv fəaliyyəti həyata keçirmək zərurəti yaranmışdır. Beynəlxalq aviasiya birliyi kiberterrorizmin xəbərdarlıq edilməsi probleminə böyük diqqət verir. Bu istiqamətdə İCAO müəyyən addımlar atmışdır. Belə ki, 1998-ci ilin oktyabrında İCAO-nun assambleyası bu problemin xüsusi olaraq hüquqi və texniki aspektlərinə fikir verilən bir səslə rezolyusiya qəbul etdi. A32-2 rezolyusiyası MA sahəsində əmkdaşlıq edən dövlətləri kiberterrorizmin artan təhlükəsinə qarşı səmərəli əks tədbirlərin tətbiqinə və işlənməsinə çağırır (2).



Nəticə

Nəzərə alsaq ki, kibercinayətkarlığın dili, dini, milliyəti sərhəddi yoxdur və kibercinayətkarlığın xarakterik xüsusiyyətlərə malik olması bu növ cinayətkarlığa qarşı mübarizənin effektivliyini yalnız beynəlxalq əməkdaşlıq çərçivəsində mümkün edə bilər. Bu baxımdan informasiya təhlükəsizliyi və kibercinayətkarlıqla mübarizə Azərbaycan Respublikasının həm yerli qanunvericiliyində həmdə beynəlxalq norma və standartlara uyğun təmin edilməlidir. Kibercinayətkarlıq və kiberterrorizmlə mübarizə aparmağa qadir olan yeni orqanlar və onları istiqamətləndirən təşkilatlar yaratmaqla, özünün milli kadrlarını yaratmaqla kibercinayətkarlıqla məşğul olan trans milli orqanlara və təşkilatlara qoşulmalıdır.

References

1. Okinava Charter for the Global Information Society. Adopted on July 22, 2000. Diplomatic Bulletin 2000. No. 8. (Electronic resource) http://www.mert.ru/index.php?nodeid=1218,
2. V.A. Vasenin Information security and computer terrorism. (Electronic resource) http://www.erime-research.ru,
3. Information Security, Textbook, Baku, "ECONOMIC UNIVERSITY"
4. Vagif Gasimov Basics of information security
5. Golubev V.A. Cyber terrorism is a threat to national security.

Rəyçi: dos. N.Nağıyev

göndərildi 10.02.2021: qəbul edildi 22.02.2021