UOT 2969 M 251 K

C. İ. MƏMMƏDOV, texnika ü. f. d.; Z. M. MƏMMƏDOV; E. E. BƏDƏLOV

Heydər Əliyev adına AAHM

KRİTİK İNFRASTRUKTURLARDA İNFORMASİYANIN QORUNMASI İSTİQAMƏTLƏRİNİN MÜƏYYƏN EDİLMƏSİ

Məqalədə kritik infrastruktur obyektlərinin informasiya sistemlərinə qarşı yönələn təhdidlər, risklər təhlil edilmiş, bu obyektlərdə informasiyanın qorunması istiqamətləri müəyyənləşdirilmişdir.

Kritik vacib obyekt dedikdə fəaliyyətinin pozulması və dayandırılması ölkənin, dövlət subyektinin, idarə-ərazi vahidinin iqtisadiyyatının idarə olunmasının itirilməsinə və ya əhalinin həyat fəaliyyətinin təhlükəsizliyinin azalmasına gətirib çıxaran obyekt nəzərdə tutulur. Kritik informasiya infrastrukturu vacib obyektlərin texnoloji və istehsal proseslərinin avtomatlaşdırılmış idarəetmə sistemlərinin cəmi olub, onların dövlətin idarəçiliyinin, müdafiə qabiliyyətinin, təhlükəsizliyinin təmini üçün nəzərdə tutulmuş informasiya-telekommunikasiya şəbəkələri, eləcə də rabitə şəbəkələri və infomasiya sistemləri ilə qarşılıqlı əlaqəsini təmin edir.

Beynəlxalq praktikada kritik infrastruktur obyektlərinə (KİO) atom sahəsi, enerji şəbəkələri, enerji istehsal edən və paylayan şəbəkələr, nəqliyyat sistemləri kənd təsərrüfatı məhsulları istehsal edən, saxlayan və ərzaq təminatı sistemi, dövlət idarəçiliyi və hökumət kommunikasiya, neft-qaz kompleksləri, əsas telekommunikasiya sistemləri, şəbəkələri, proqram-texniki təminat və rabitə sistemləri, kimya kompleksləri, maliyyə-kredit sektoru, su təminatı və təchizatı, səhiyyə və s. sistemləri aid edilir [1]. Bu obyektlər KİO kimi dünyanın əksər ölkələrinin qanunvericilik aktlarında öz əksini tapmışdır. Lakin bu obyektlərdən bəziləri bir ölkədə KİO siyahısına daxil edilə, digər ölkədə daxil edilməyə bilər.

Azərbaycan Respublikası Nazirlər Kabinetinin 2016-cı il 30 dekabr tarixli 531 nömrəli qərarı ilə təsdiq edilmiş "Təhlükə potensiallı və dövlət əhəmiyyətli tikinti obyektlərinin siyahısı"nda göstərilən obyektləri KİO-ya aid etmək olar [2]: su və istilik elektrik stansiyaları, su hövzələri (anbarları) və onların bəndləri (hidrotexniki qurğuları), neft emalı maddələrinin istehsalı zavodları, maye qaz, neft və neft məhsullarının rezervuar parkları, dəniz şelfində quraşdırılan neft və qazçıxarma platformaları, dövlət əhəmiyyətli hidrotexniki qurğular, yanacaqdoldurma (neft və qaz) məntəqələri, metro stansiyaları və tunelləri, Xəzər dənizi akvatoriyasında inşa edilən obyektlər, telekommunikasiya şəbəkələri və qurğuları, yerüstü peyk idarəetmə mərkəzləri, dövlət və beynəlxalq əhəmiyyətli neft-qaz boru kəmərləri, 110 kilovat və ondan yuxarı gərginlikli elektrikötürücü xətlər, tutumu 10 min kubmetr və daha artıq olan neft, neft və kimya məhsullarının saxlandığı qurğular və s.

Baş vermiş hadisələr barədə açıq mətbuatda verilən məlumatların təhlili göstərir ki, KİO-nun sıradan çıxarılması və ya onların işinə ciddi zərərin vurulması, əsasən bu obyektlərin informasiya təhlükəsizliyinin pozulması ilə reallaşdırılır.

KİO-nun informasiya sistemlərinin əsas xüsusiyyətləri. Ümumi halda, ərazicə paylanmış və öz aralarında verilənlər və idarəetmə üzrə qarşılıqlı əlaqədə olan lokal şəbəkələrdən və ayrıca kompüterlərdən ibarət bu sistemlərin informasiyanın toplanılması, emalı, saxlanılması və ötürülməsi baxımından əsas xüsusiyyətləri aşağıdakılardır:

-sistemin komponentlərinin ərazicə səpələnməsi və onlar arasında intensiv informasiya mübadiləsinin mövcudluğu;

-informasiyanın saxlanılması və ötürülməsi, həmçinin, təsvir edilməsi üsullarının istifadəsinin geniş spektri;

-müxtəlif subyektlərə məxsus olan müxtəlif təyinatlı verilənlərin vahid verilənlər bazası

çərçivəsində cəmləşməsi və əksinə, müəyyən sybyektlərə lazım olan verilənlərin şəbəkənin müxtəlif uzaqda olan qovşaqlarında yerləşdirilməsi;

-məlumat sahiblərinin fiziki strukturlardan və verilənlərin yerləşdirilməsi yerindən təcrid edilməsi;

-verilənlərin paylanmış emalı rejimlərindən istifadə;

-informasiyanın avtomatlaşdırılmış emalı prosesində çoxlu sayda istifadəçilərin və müxtəlif kateqoriyalı personalın iştirakı;

-informasiya resurslarına çoxlu sayda müxtəlif kateqoriyalı istifadəçilərin eyni zamanda və birbaşa əlyetərliliyi;

-istifadə olunan kompyuter texnikası və rabitə vasitələrinin, həmçinin onların proqram təminatının müxtəlifliyinin yüksək səviyyədə olması;

-sistemdə geniş istifadə olunan əsas texniki vasitələrin əksəriyyətində xüsusi aparat mühafizə vasitələrinin olmaması.

Bu xüsusiyyətlərin təhlili KİO-nun informasiya sistemlərinin zəif yerlərini, təhlükəsizliyə yönəlmiş təhdidlərin əvvəlcədən müəyyən edilməsinə, risklərin qiymətləndirilməsinə və idarə edilməsinə, risk dərəcələrinə uyğun mühafizə tədbirlərinin görülməsinə imkan verir.

İnformasiya sistemlərinin təhlükəsizliyinə olan risklərin təhlili və qiymətləndirilməsi. Risk, özünün müəyyən qiyməti və başvermə ehtimalı olan arzuolunmaz (mənfi) hadisənin baş verməsi imkanıdır. Risklərin qiymətləndirilməsi prosesinin məqsədi informasiya sisteminə və onun resurslarına münasibətdə risklərin xüsusiyyətlərinin müəyyən edilməsidir. Qiymətləndirmə nəticəsində əldə edilmiş məlumatlar əsasında zəruri müdafiə vasitələri seçilə bilər. Riskləri qiymətləndirərkən aşağıdakı əsas faktorlar nəzərə alınır: resursların dəyəri, təhdid və zəifliklərin səviyyəsi, mövcud və planlaşdırılmış vasitələrin səmərəliliyi və s.

KİO-nun informasiya təhlükəsizliyinin əsas riskləri aşağıdakılardır:

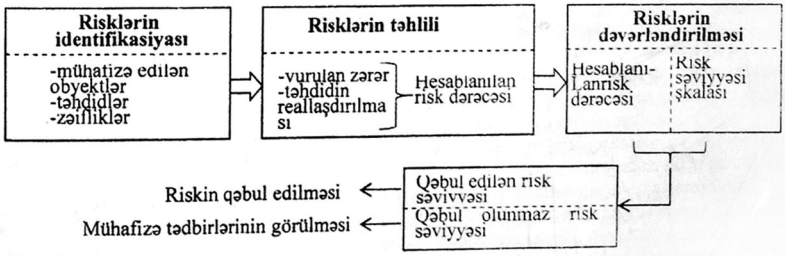
-məxfi informasiyanın sızması riski;

-vacib məlumatların itirilməsi və ya əlyetərliyin pozulması riski;

-natamam və ya təhrif edilmiş informasiyadan istifadə riski.

KİO-nun informasiya təhlükəsizliyinə olan riskin qiymətləndirilməsi prosesini digər informasiya sistemlərinin təhlükəsizliyinə yaradılan risklərin qiymətləndirilməsi prosesində olduğu kimi [3], şərti olaraq üç mərhələyə bölmək olar (şəkil): riskin müəyyən edilməsi (identifikasiyası), riskin təhlili, riskin dəyərləndirilməsi.

Riskin müəyyən edilməsi riskin elementlərinin (mühafizə olunan obyektlər, təhdidlər, zəifliklər) təsvir edilməsindən və siyahıların hazırlanmasından ibarətdir.



İnformasiya təhlükəsizliyi risklərinin qiymətləndirilməsi prosesinin funksional sxemi

İdentifikasiya mərhələsində alınan informasiya risklərin təhlili prosesində istifadə olunur və bu zaman əsas məqsəd obyektə vurulan zərərin həcminin, təhlükəsizliyin pozulması ehtimalının və riskin səviyyəsinin müəyyən edilməsidir.

Risklərin təhlilində növbəti mərhələ təhdidlərin reallaşdırılması ehtimalının qiymətləndirilməsidir. Mümkün zərərin həcmi və təhdidlərin reallaşdırılması ehtimalı müəyyən edildikdən sonra riskin səviyyəsi müəyyənləşdirilir. Risklərin hesablanması ehtimal olunan zərərlə təhdidlərin reallaşdırılması ehtimalının kombinə edilməsi yolu ilə həyata keçirilir.

Risklərin qiymətləndirilməsi prosesində qəbul edilən risk səviyyəsi də müəyyən edilməlidir və hesablanılan risk həmin səviyyədən böyük olmadıqda əlavə mühafizə tədbirlərinin görülməsinə ehtiyac qalmır, bütün digər hallarda əlavə tədbirlər görülməlidir. Risklərin qiymətləndirilməsinin nəticələri risk səviyyələrini azaldan mühafizə tədbirlərinin seçilməsi üzrə əsaslı qərar vermək üçün istifadə olunur. Bununla bərabər, qiymətləndirilmənin nəticələri əsasında risklərin idarə edilməsi üzrə fəaliyyətlərin prioritetləri və həyata keçirilməsinin iqtisadi cəhətdən məqsədəuyğunluğu müəyyən edilir.

KİO-nun informasiya sisteminə və onun subyektlərinə olan təhdidlər. KİO-nun informasiya sistemlərinin xüsusiyyətlərini nəzərə alaraq, bu sistemlərin informasiya təhlükəsizliyinə olan təhdidləri təbii və süni təhdidlər kimi iki qrupa bölmək olar. İnsan fəaliyyətinin nəticəsi olaraq yaranan süni təhdidlər öz növbəsində iki qrupa bölünür:

-qəsdən törədilməyən (qərəzsiz və ya təsadüfi yaranan);

-qəsdən törədilən (qərəzli).

Kibercinayətkarlıq səviyyəsinin gündən-günə artmasını və bu cinayətlərin əsasən KİO-ya qarşı yönəlməsini nəzərə alaraq, qəsdən törədilən təhdidlərə daha çox diqqətin ayrılmasının məqsədəuyğun olması qeyd edilməlidir. KİO-nun informasiya isteminin işinin pozulmasına, sıradan çıxarılmasına, sistemə və informasiya resurslarına icazəsiz daxilolmaya, qanuni istifadəçilərin təcrid olunmasına və s. səbəb olan, düşünülmüş şəkildə törədilən təhdidlərə aşağıdakıları aid etmək olar:

-sistemin fiziki məhv edilməsi (partladılma, yandırılma və s.), onun bütün və ya bəzi daha vacib komponentlərinin (qurğuların, vacib sistem məlumatları daşıyıcılarının, xidməti personaldan olan şəxslərin və s.) sıradan çıxarılması;

-sistemin fəaliyyətini təmin edən alt sistemlərin (elektrik qidalanması, soyutma, əlaqə xətləri və s.) söndürülməsi və ya sıradan çıxarılması;

-sistemin işinin pozulmasına səbəb olan fəaliyyətlər (qurğuların və ya proqramların iş rejimlərinin dəyişdirilməsi, sistem qurğularının iş tezliklərinə uyğun güclü radiomaneələrin qoyulması və s.);

-sistemin işçi personalı arasına (o cümlədən təhlükəsizliyə cavbdeh olan inzibatçılar qrupuna) agentlərin yeridilməsi;

-müəyyən səlahiyyətlərə malik olan personalın və ya istifadəçilərin İS-in təhlükəsizliyinə təhdid yaratmaq məqsədilə, işbirliyinə cəlb edilməsi (maddi maraqlandırmaq, hədə-qorxu gəlmək və s. yolla);

-qulaqasma, uzaq məsafədən şəkilçəkmə və videoçəkmə qurğularının tətbiqi;

-qurğulardan və rabitə xətlərindən kənar elektromaqnit, akustik və digər şüalanmaların tutulması, eləcə də informasiya emalında bilavasitə iştirak etməyən texniki vasitələrin (telefon və elektrik xətlərinin, qızdırıcı qurğuların və s.) istifadəsi;

-rabitə kanalları vasitəsilə ötürülən məlumatların tutulması və mübadilə protokollarının, əlaqəyəgirmə və istifadəçilərin avtorizə edilməsi qaydalarının öyrənilməsi və gələcəkdə sistemə daxil olmaq üçün istifadəsi;

-informasiya daşıyıcılarının (yaddaş qurğularının, onların ayrı-ayrı hissələrinin və ya bütövlükdə kompyuterin) oğurlanması;

-informasiya daşıyıcılarının məzmunlarının icazəsiz köçürülməsi;

-istehsal tullantılarının (çap vərəqlərinin, qeydlərin, yararsız avadanlıq kimi silinmiş (istehsaldan çıxarılmış) informasiya daşıyıcılarının) oğurlanması;

-əməli yaddaşdan və xarici yaddaş qurğularından qalıq informasiyanın oxunması;

-parolların və girişi məhdudlaşdıran digər rekvizitlərin qeyri-qanuni yolla (agentlərin köməyi ilə, istifadəçilərin səhlənkarlığından istifadə etməklə, seçmə üsulu ilə, sistemin interfeysini imitasiya etməklə və s.) ələ keçirilməsi və sonradan qeydiyyatdan keçmiş istifadəçinin adı altında

maskalanma;

-istifadəçilərin unikal fiziki xassələrə malik olan terminallarının (işçi stansiyanın şəbəkədə nömrəsinin, fiziki ünvanın, rabitə sistemində ünvanın, kodlaşdırma üçün aparat blokunun və s.) icazəsiz istifadəsi;

-çoxməsələli əməliyyat sistemlərinin və proqramlaşdırma dillərinin çatışmazlıqlarını istifadə etməklə asinxron rejimdə əməli yaddaşın əməliyyat sistemi (o cümlədən digər proqramlar) və ya digər istifadəçilər tərəfindən istifadə olunan hissələrindən informasiyanın oxunması;

-informasiyanın kriptoqrafik mühafizəsi şifrlərinin açılması;

-xüsusi aparat vasitələrinin, proqram və aparat qoyuluşlarının, eləcə də virusların (o cümlədən "troya atları"nın və "qurd"ların) tətbiqi, nəzərdə tutulmuş funksiyaların yerinə yetirilməsi üçün lazım olmayan, lakin mühafizə sistemini keçmək, qeydiyyata düşmək, vacib məlumatları ötürmək və ya sistemin fəaliyyətini pozmaq məqsədilə sistem resurslarına gizli və qeyri-qanuni daxilolma imkanlarını reallaşdıran proqramların istifadəsi;

-qanuni istifadəçinin adı altında yanlış məlumatların daxil edilməsi və ya ötürülən məlumatların dəyişdirilməsi üçün həmin istifadəçi sistemdə işləyən zaman fasilələrdən və sistemdə baş verən nasazlıqlardan istifadə etməklə "sətirlərarası" işləmək məqsədilə rabitə xətlərinə qeyri-qanuni qoşulma;

-dezinformasiya aparmaq və yanlış məlumatları yaymaq məqsədilə qanuni istifadəçi sistemə daxil olduqdan sonra onun kompyuterini şəbəkədən fiziki ayırmaq və sonradan onun adı altında autentifikasiya proseduralarını uğurla keçmək (adlamaq) yolu ilə bilavasitə bu istifadəçini əvəz etmək üçün rabitə xətlərinə qeyri-qanuni qoşulma.

Təbii ki, bədniyyətli şəxs (rəqib, düşmən) öz məqsədinə nail olmaq üçün, əksər hallarda, baxılan təhdidlərin bir neçəsindən eyni zamanda istifadə edir.

KİO-nun informasiya təhlükəsizliyinə olan təhdidlərdən mühafizə üsulları. Həyata keçirilmə üsullarına görə KİO-nun informasiya təhlükəsizliyinə olan təhdidlərdən mühafizə tədbirlərini əksər informasiya sistemlərində olduğu kimi [4] **hüquqi (qanunvericilik), mənəvi-etik, təşkilati (inzibati), mühəndis-texniki** növlərə bölünür.

Qanunvericilik tədbirləri özündə dövlət orqanlarının, təşkilatların, əhalinin (ayrı-ayrı şəxslərin) həyat və fəaliyyətinin ayrı-ayrı sahələrinə münasibətdə dövlət tərəfindən müəyyən olunmuş və təsdiq edilmiş ümumi məcburi davranış qaydaları və normaları toplusunu, eləcə də bu normaların pozulduğu halda həyata keçirilən tədbirlər sistemini əhatə edir. Azərbaycan Respublikasında bütün informasiya sistemlərində, o cümlədən KİO-da informasiyanın mühafizəsi üçün hüquqi tədbirlər sistemi "Milli təhlükəsizlik haqqında", "İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında", "Elektron imza və elektron sənəd haqqında", "Dövlət sirri haqqında", "Kibercinayətkarlıq haqqında" Konvensiyanın Təsdiq edilməsi barədə" Azərbaycan Respublikasının qanunlarına, eləcə də Azərbaycan Respublikasının Cinayət-Prosessual Məcəllələrinin müvafiq bəndlərinə əsaslanır.

İnformasiya təhlükəsizliyinin mühafizəsinin **mənəvi-etik tədbirləri** informasiya texnologiyalarının yayılması və istifadəsi dövründə ənənəvi olaraq yaranmış və ya yaranmaqda olan davranış normalarından ibarətdir. Bu normalar, əksər hallarda, qanunla təsdiq edilmiş normativ aktlar kimi mütləq sayılmır, lakin onlara riayət edilməməsi, bir qayda olaraq, ayrı-ayrı şəxsin, bir qrup şəxsin və ya təşkilatın nüfuzuna xələl gətirir.

Təşkilati (inzibati) tədbirlər məxfi informasiyanın hüquqazidd əldə olunmasını, daxili və xarici təhdidlərin meydana gəlməsini istisna etmək və ya əhəmiyyətli dərəcədə çətinləşdirmək məqsədilə təşkilatın və onun əməkdaşlarının fəaliyyətinin, eləcə də icraçıların qarşılıqlı münasibətlərinin normativ hüquqi əsaslarla nizamlanmasını nəzərdə tutur.

KİO-nun informasiya təhlükəsizliyinə olan təhdidlərdən mühafizəsi üçün təşkilati tədbirlərə aşağıdakıları aid etmək olar:

-informasiya sistemlərinin layihələndirilməsi, quraşdırılması, avadanlıqlarla təchiz edilməsi mərhələlərində həyata keçirilən tədbirlər;

-istifadəçilərin sistem resurslarına daxilolma qaydalarının işlənilməsi üzrə tədbirlər;

-sistem üçün personalın seçilməsi və hazırlanması üzrə həyata keçirilən tədbirlər;

-buraxılış rejiminin və mühafizənin təşkili tədbirləri;

-sənədlərlə və sənədləşdirilmiş informasiya ilə işin təşkili tədbirləri;

-məxfi informasiyanın yığılması, emalı, toplanması və saxlanması üçün istifadə olunan texniki vasitələrlə işin təşkili;

-daxilolmanın məhdudlaşdırılması rekvizitlərinin (parollar, şifrələmə açarı və s.) paylanması üzrə tədbirlər;

-istifadəçilərin işinə açıq və gizli nəzarətin təşkili üzrə tədbirlər;

-avadanlıq və proqram təminatının layihələndirilməsi, təkmilləşdirilməsi və təmiri zamanı həyata keçirilən tədbirlər və s.

İnformasiyanın mühafizəsinin **mühəndis-texniki tədbirləri,** bir çox hallarda, fiziki və texniki tədbirlər sistemi kimi iki qrupa bölünür. Fiziki qoruma tədbirləri sistem komponentlərinə və qorunan məlumatlara potensial bədniyyətlilərin daxil olmalarına fiziki maneələr yaratmaq üçün nəzərdə tutulmuş müxtəlif mexaniki, elektromexaniki və ya elektron qurğuların, eləcə də vizual müşahidə, kommunikasiya və təhlükəsizlik siqnalizasiya sistemlərinin texniki vasitələrinin istifadəsinə əsaslanır. Texniki tədbirlər sistemi isə özündə İS-ə daxil olan və mühafizə funksiyasını (istifadəçilərin identifikasiya və autentifikasiyası, informasiya resurslarına daxilolmanın məhdudlaşdırılması, hadisələrin qeydiyyatı, informasiyanın kriptoqrafik mühafizəsi və s.) yerinə yetirən elektron qurğu və xüsusi proqramların istifadəsinə əsaslanır.

KİO-nun xüsusiyyətlərinə görə onun informasiya sistemlərinin qorunması üçün qanunvericilik, təşkilati və mənəvi-etik tədbirlər, həmçinin, mühəndis-texniki tədbirlərin fiziki qoruma hissəsi, bir qayda olaraq, obyektin özünün təhlükəsizlik tədbirləri ilə birgə həyata keçirilir.

Əksər hallarda, kritik infrastruktur obyektləri bir-birindən az ya çox dərəcədə fərqləndiyi kimi, onların informasiya sistemləri, bu sistemlərin zəif yerləri, onlara olan təhdidlər və risk dərəcələri də bir-birindən fərqlənir. Məsələn, "daxilolmanın məhdudlaşdırılması rekvizitlərinin (parollar, şifrələmə açarı və s.) paylanması üzrə tədbirlər" obyektin biri üçün çox vacib olduğu halda, digəri üçün bu tədbir elə də zəruri olmaya bilər. Məhz bu səbəbdən, informasiya təhlükəsizliyinə olan təhdidlərdən mühafizə üsulları konkret obyektin informasiya sisteminin xüsusiyyyətləri nəzərə alınmaqla işlənilməlidir.

NƏTİCƏLƏR

1.KİO-da informasiya təhdidləri və riskləri obyektdə olan informasiya sisteminin və onun alt sistemlərinin xüsusiyyətləri nəzərə alınmaqla aparılmalıdır.

2.Tamamilə eyni struktura və təyinata malik olan KİO-nun informasiya sistemlərinə fərqli mühafizə tədbirləri işlənilə bilər.

3.İS-in mühafizə sistemlərinə tələblərin formalaşdırılması üçün əsas kimi təhlükəsizliyə yönələn mümkün təhdidlər müəyyən edilməli, onların təsnifatı aparılmalı və həyata keçirilməsi ehtimalları qiymətləndirilməlidir.

ƏDƏBİYYAT

1.Понятия, классификация и регулирование критической информационной инфраструктуры (https://rutlib5.com/book/27296).

2.Təhlükə potensiallı və dövlət əhəmiyyətli tikinti obyektlərinin siyahısı (Azərbaycan Respublikası Nazirlər Kabinetinin 2016-cı il 30 dekabr tarixli 531 nömrəli Qərarı).

3.Баранова Е.К. Методики анализа и оценки рисков информационной безопасности // Образовательные ресурсы и технологии, 2015. № 1(9). С.73-79.

4.V.Ə.Qasımov İnformasiya təhlükəsizliyinin əsasları. Dərslik. Bakı: 2009. 340 s.