PARADIGMA, No.1, 2025, səh.106-110
https://doi.org/10.30546/30015.2025.1.038

OBYEKTLƏRİN VƏ İNFORMASİYANIN ÇOXSƏVİYYƏLİ MÜDAFİƏSİNİN KONSEPTUAL MƏSƏLƏLƏRİ

H.V. Əlibəyova, L.F. Ağamalıyeva
Azərbaycan Universiteti, Ceyhun Hacıbəyli, 71, Bakı, Azərbaycan
e-mail: Humay.Alibayova@student.au.edu.az

Xülasə. Məqalədə obyektlərin və informasiyanın təhlükəsizliyinin təmin edilməsi problemlərinin həlli üçün nəzərdə tutulmuş çoxsəviyyəli təhlükəsizlik sistemlərinin qurulmasının konseptual məsələləri araşdırılır. Göstərilir ki, bu cür mühafizə sistemlərinin qurulmasına təklif olunan yanaşma bizə mühafizə sistemlərinin iki əsas sinfi - informasiyanın mühafizəsi sistemləri və informasiya infrastrukturunun mühafizəsi sistemləri arasında çəkilmiş mövcud sərhədi aşmağa imkan verir, onların struktur təşkili üçün vahid nəzəri əsas yaradır. Məqalədə çoxsəviyyəli mühafizə sistemlərinin əsas funksiyalarının təhlili verilmiş və onun əsaslandığı əsas prinsiplər verilmişdir. Müəyyən edilmişdir ki, mühafizə prosesində məzmununa görə şərti olaraq beş səviyyəyə bölünə bilən subproseslər olmalıdır. Göstərilən alt proseslərin əsas məzmunu verilir. Bu halda, hər səviyyənin alt prosesləri prosedurlara birləşdirildi. İnformasiyanın toplanması və emalı səviyyəsində həyata keçirilən prosedurlara xüsusi diqqət yetirilir, çünki mühafizənin effektivliyi ilk növbədə onların keyfiyyətindən asılıdır.

Açar sözlər: İnformasiya təhlükəsizliyi, çoxsəviyyəli mühafizə, təhlükə, ümumi model, performans göstəricilərinin vektoru.

Giriş

Çoxsəviyyəli mühafizənin əsas məqsədi texniki avadanlıq və proqram təminatından, eləcə də obyektlərin və informasiyanın mühafizəsi üsullarından istifadə etməklə, mövcud texnologiyalar çərçivəsində bu obyektlərdə saxlanılan, emal olunan və ötürülən informasiyanın idarəetmə və rabitə vasitələrinin informasiya infrastrukturuna qeyri-sabitləşdirici amillərin təsirindən lazımi səviyyədə müdafiəni təmin etməkdir. İndiki mərhələdə idarəetmə və rabitə vasitələrinin informasiya təhlükəsizliyinin yaxşılaşdırılması məsələlərində bu istiqamət ən perspektivli və iqtisadi cəhətdən əsaslandırılmış kimi görünür.

Aydındır ki, bu məqsədə nail olmaq Çoxsəviyyəli mühafizənin nəzəri əsaslarının işlənib hazırlanması şərtilə mümkündür [1, 2].

Çoxsəviyyəli mühafizənin əsas istifadə sahəsi fiziki və məntiqi idarə olunan zonaların təmin edilməsinə ənənəvi yanaşmanı dəstəkləyən idarəetmə və rabitə vasitələri üçün informasiya təhlükəsizliyi sistemlərinin tətbiqidir. İnformasiya təhlükəsizliyinin ümumi nəzəriyyəsi çərçivəsində Çoxsəviyyəli mühafizə sistemlərinin yaradılmasına yanaşma, göründüyü kimi, mühafizə sistemlərinin iki ən vacib sinfi - informasiyanın mühafizəsi sistemləri və informasiya infrastrukturunun mühafizəsi sistemləri arasında çəkilmiş mövcud sərhədi aşmağa, onların struktur təşkili üçün vahid nəzəri əsas təmin etməyə imkan verir.

Çoxsəviyyəli mühafizənin konseptual əsasları

Potensial təhlükələrin fiziki xarakterindən asılı olmayaraq, idarəetmə və rabitə vasitələrinin informasiya təhlükəsizliyi sistemi aşağıdakı əsas funksiyaları yerinə yetirməlidir:

– mümkün təhlükələrin həyata keçirilməsinə səbəb olan amillərin hərəkətlərinin qarşısını almaq və ya əhəmiyyətli dərəcədə çətinləşdirmək, yəni mühafizə olunan obyektin təhlükə altında olan ehtiyatlarının birbaşa mühafizəsini təmin etmək;

– təhlükəli hadisələrin vaxtında və etibarlı aşkar edilməsini, o cümlədən onların baş verməsinin mühafizə olunan obyekt üçün hər hansı təhlükənin həyata keçirilməsi üçün real imkanlar açmasını təmin etmək;

– nəzarət və rabitə obyektinin informasiya təhlükəsizliyinə təhlükə yaradan amillərin hərəkətlərinin qarşısının alınması.

Aydındır ki, bu funksiyaların yerinə yetirilməsi üçün texniki baza çox səviyyəli, çox mövqeli mühafizə sistemi ola bilər ki, onun yaradılması aşağıdakı əsas prinsiplərə əsaslanır [2].

1. Potensial təhlükənin fiziki xarakterindən asılı olmayaraq, mühafizə sistemi müəyyən (tələb olunan) etibarlılıq dərəcəsi ilə onun həyata keçirilməsinə qarşı durmalıdır.

2. Sistem əsas funksiyası təhlükəli hadisələrin vaxtında və etibarlı aşkar edilməsi olan mühafizə olunan obyektin təhlükəsizlik vəziyyətinə nəzarət etməlidir.

3. Sistem aşkar edilmiş təhlükəli hadisəni müəyyən etməli və mühafizə olunan obyektin informasiya təhlükəsizliyinə təhlükə yaradan amillərin hərəkətlərinin qarşısını almaq üçün yaranan konkret vəziyyətlə bağlı ən rasional qərar qəbul etməlidir.

4. Sistem elə qurulmalıdır ki, həyata keçirilən təhlükənin növündən asılı olmayaraq, onun qarşısını almaq üçün lazım olan şərait həmişə mövcud olsun.

5. Sistem mühafizə olunan obyektin informasiya təhlükəsizliyinə təhlükə yaradan amillərin hərəkətlərinin qarşısının alınmasını tələb olunan etibarlılıq dərəcəsi ilə təmin etməlidir.

Nəzərdən keçirilən funksiya və prinsiplərə uyğun olaraq idarəetmə və rabitə obyektinin informasiya təhlükəsizliyi sistemi aşağıdakı səviyyələrdən ibarət ola bilər:

– obyektin qorunan resursuna fiziki və ya məntiqi hücumların təsirinin qarşısının alınmasını və ya əhəmiyyətli dərəcədə maneə törədilməsini təmin edən birbaşa mühafizə səviyyəsi;

– təhlükəli hadisənin baş verməsinin vaxtında və etibarlı aşkar edilməsini və mümkün təhlükənin qarşısının alınmasını təmin etmək üçün bu hadisə haqqında məlumatın qərar qəbul edən orqana ötürülməsini təmin edən aşkarlama səviyyəsi;

– informasiyanın toplanması və emalı səviyyəsi;

– təhlükəli hadisənin və onun baş verməsi nəticəsində yaranan təhlükənin zərərsizləşdirilməsi üçün şəraitin vaxtında yaradılmasını təmin edən mühafizə sisteminin operativ reaksiya səviyyəsi;

– təhlükəli hadisənin zərərsizləşdirilməsi səviyyəsi və onun baş verməsi nəticəsində yaranan təhlükə.

Mühafizə sisteminin müəyyən edilmiş səviyyələrinin hər biri mühafizə sisteminin yüksək məntiqi, texniki və əməliyyat dayanıqlığını təmin etməklə, onların çoxmövqeli istifadəsi ilə müxtəlif texniki və proqram vasitələrindən istifadə etməklə həyata keçirilə bilər.

Maddi səviyyədə çoxsəviyyəli mühafizənin həyata keçirilməsi ardıcıllığı aşağıdakı kimi təqdim olunur.

Birinci səviyyədə sabitliyi pozan amillərin bütün spektrinin təsirindən mühafizənin inzibati-təşkilati, mühəndis-texniki və proqram-məntiqi tədbirləri həyata keçirilir.

Nəzərdən keçirilən mühafizə prosesinin ikinci səviyyəsində monitorinq həyata keçirilir - toplanması, saxlanması və bəlkə də mühafizə sisteminin vəziyyətinin göstərilməsi və təhlükəli hadisələrin əlamətlərinin və ya baş vermə faktının aşkarlanması.

Üçüncü səviyyədə aşkar edilmiş təhlükəli hadisənin yoxlanılması və identifikasiyası aparılır və onun necə zərərsizləşdirilməsi barədə qərar qəbul edilir. Obyektin və onun mühafizə sisteminin istismarı zamanı bəzi təhlükəli hadisələrin təkrarlana biləcəyini güman etmək məqsədəuyğundur: mühafizə vasitələrinin xüsusi nasazlıqları [3], müdaxilə edən şəxs tərəfindən onların aradan qaldırılmasına uğurlu cəhdlər və s. Belə olan halda, bu tip təhlükəli hadisənin olması faktı müəyyən edildikdən sonra onun zərərsizləşdirilməsi üçün əvvəllər qəbul edilmiş variantlardan istifadə etmək olar.

İdentifikasiya probleminin həllinə aşağıdakı yanaşmalar mümkündür [3]. Birincisi, fiziki mühafizə sistemləri üçün video monitorinq vasitələri, informasiya sızmasından mühafizə vasitələri üçün ölçü alətləri və avadanlıqları, kompüter hücumlarının yoxlanılması və identifikasiyası üçün xüsusi proqram məhsulları kimi əlavə xüsusi vasitələrin istifadəsinə əsaslanır. İkinci yanaşma situasiya şablonlarının istifadəsinə əsaslanır. Bu şablonlara mühafizə sisteminin və mühafizə olunan obyektin vəziyyətini, kibercinayətkaların davranışını, xarici amilləri və s.-ni təsvir edən parametrlər daxil edilməlidir. Vəziyyətlə şablonlardan birində göstərilən vəziyyət arasında uyğunluq təhlükəli hadisənin mövcudluğunu göstərməlidir. Bu yanaşmanın üstünlükləri identifikasiyanın nisbi sadəliyi və sürəti ilə bağlıdır. Bu yanaşmanın həyata keçirilməsi aspekti coxsəviyyəli mühafizənin bütün məqbul vəziyyətlərini və kibercinayətkarların hərəkətlərini təsvir edən şablonlar toplusunun qurulmasının mürəkkəbliyi ilə məhdudlaşdırıla bilər. Bundan əlavə, şablonlara daxil edilmiş parametrlərin seçilməsi qeyri-trivial bir işdir: onların kiçik bir hissəsi vəziyyəti adekvat təsvir etmək iqtidarında deyil, çox sayda daha mürəkkəb monitorinq sisteminə səbəb olacaqdır.

Kompromis həll yuxarıda göstərilən yanaşmaların birləşməsində görünür. Tipik əvvəlcədən təyin edilmiş vəziyyətlər şablonlardan istifadə etməklə təsvir edilir. Bundan əlavə, təhlükəli hadisələrin yoxlanılması və müəyyənləşdirilməsi xüsusi vasitələrdən istifadə etməklə həyata keçirilir. Yanaşmaların kompleks istifadəsi həm tipik, həm də fövqəladə təhlükəli hadisələrin balanslaşdırılmış şəkildə müəyyənləşdirilməsinə imkan verəcək və onların zərərsizləşdirilməsi zərurətinə səbəb olacaqdır.

Sonra təhlükəli hadisəyə cavab variantı hazırlanır. Onun həyata keçirilməsi təhlükəli hadisənin və onu həyata keçirən proseslərin zərərsizləşdirilməsinin effektivliyinə dair tələblərin yerinə yetirilməsi meyarına cavab verən mümkün variantların sintezindən ibarətdir. Sintez problemi optimallaşdırma problemi kimi formalaşdırıla bilər. Bu halda yeganə ən yaxşı həll yolu (cavab variantı) tapılır. Bunu belə bir formalaşdırmada həll etmək mümkün olmadıqda, müəyyən formal və/və ya evristik qaydalara uyğun olaraq, məqbul alternativ cavab variantları yaradılır, ardınca onların qiymətləndirilməsi və ən üstün olanı seçilir.

Dördüncü səviyyədə təhlükəli hadisəyə operativ reaksiya onu zərərsizləşdirmək məqsədi ilə həyata keçirilir. Bu səviyyədə prosedurların həyata keçirilməsi mühafizənin idarə edilməsinin təşkilindən və təhlükəli hadisələrin qarşısını almaq üçün mühafizə sisteminin məkan və texnoloji imkanlarından asılıdır. Bu səviyyədə həyata keçirilən tədbirlər yalnız təhlükələrin zərərsizləşdirilməsi xüsusi tədbirlərin təşkili zərurəti ilə əlaqəli olan mühafizə sistemləri üçün məcburidir, məsələn, rabitə xətləri üzərindən ötürülən məlumatların təhlükəsizliyinin pozulmasının qarşısının alınması.

Son beşinci səviyyə təhlükəli hadisələrin birbaşa zərərsizləşdirilməsini nəzərdə tutur.

Bu səviyyəli hadisələr mühafizə sistemləri üçün xüsusilə mürəkkəbdir, onlar üçün xarakterik olan təhlükəli hadisələrin zərərsizləşdirilməsi münaqişəli vəziyyətin həlli yolu ilə həyata keçirilir və xüsusi resursların istifadəsini tələb edir. Baxılan bu səviyyədə tədbirlərin ardıcıllığı təhlükəli hadisənin zərərsizləşdirilməsinin nəticələrinin monitorinqi və müəyyən edilmiş meyarlara uyğun qiymətləndirilməsi ilə tamamlanır.

Nəticə. Çoxsəviyyəli mühafizə prosesinin bu cür təqdimatı bizə aşağıdakı nəticələr çıxarmağa imkan verir. Çoxsəviyyəli mühafizə müxtəlif təyinatlı obyektlərin informasiya təhlükəsizliyinin təmin edilməsi problemlərinin həlli üçün həm obyektin özünün, həm də informasiyanın mühafizəsi baxımından istifadə edilə bilər.

Ədəbiyyat

1. Никифоров, О. Г. О научно-методическом подходе к оцениванию эффективности функционирования многоуровневых систем защиты. [Текст] // Вопросы радиоэлектроники. –Сер. СОИУ. – 2012. – Вып. 2. – С. 120–123.
2. Никифоров, О. Г. О некоторых концептуальных вопросах построения многоуровневых многопозиционных систем защиты объектов и информации [Текст] // Труды XI Российской научно-технической конференции «Новые информационные технологии в системах связи и управления», 6 июня 2012. Секция 2. Теория и технологии создания аппаратуры систем связи и управления. – Калуга: Изд-во ООО «Ноосфера», 2012. – С. 583–585.
3. Масановец, В. В., Фисун, А. П., Никифоров, О. Г. Методы комплексного контроля безопасности информации на объектах телекоммуникационных систем органов государственного управления: Монография. Под общей ред В. В. Масановца. – М.: Управление делами Президента Российской Федерации, 2009. – 368 с.

4. Советов, Б. Я., Яковлев, С. А. Моделирование систем: Учебник.– М.: Высшая школа, 1998. – 319 с.
5. Бусленко, Н. П. Моделирование сложных систем.– М.: Наука, 1978.– 399 с.

CONCEPTUAL ISSUES OF MULTILEVEL PROTECTION OF OBJECTS AND INFORMATION

H.V. Alibayova, L.F. Aghamaliyeva
Azerbaijan University, Ceyhun Hajibeyli 71, Baku, Azerbaijan

Abstract. The article examines the conceptual issues of building multilevel security systems designed to solve the problems of ensuring the security of objects and information. It is shown that the proposed approach to building such security systems allows us to overcome the existing boundary between the two main classes of security systems - information security systems and information infrastructure security systems, and creates a single theoretical basis for their structural organization. The article provides an analysis of the main functions of multilevel security systems and the basic principles on which it is based. It is determined that the security process should include subprocesses that can be conditionally divided into five levels according to their content. The main content of the specified subprocesses is given. In this case, the subprocesses of each level were combined into procedures. Special attention is paid to the procedures carried out at the level of information collection and processing, since the effectiveness of protection primarily depends on their quality.

Keywords: Information security, multi-level protection, threat, general model, vector of performance indicators.