

UOT 004.054

Şıxəliyev R.H.¹, Yunusov T.E.²

AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan

¹ramiz@sciencez.az, ²turaly@mail.ru

KOMPÜTER SİSTEMLƏRİNİN TƏHLÜKƏSİZLİYİNİN QIYMƏTLƏNDİRİLMƏSİ METODLARI

Məqalədə kompüter sistemlərinin təhlükəsizliyinin qiymətləndirilməsinin bəzi standart və metodları, o cümlədən Ümumi Meyarlar standartı, sistemin zəiflik indeksi, çoxpilləli hücum modelləşdirməsi, hücumun aşkarlanması metodları analiz edilmiş və bəzi mövcud problemlər müəyyən edilmişdir.

Açar sözlər: kompüter sistemləri, təhlükəsizliyin qiymətləndirilməsi, təhlükəsizlik metrikaları, təhlükəsizliyin qiymətləndirilməsi metodları.

Giriş

Kompüter sistemləri (KS) enerji, rabitə, maliyyə və s. kimi əsas sənaye sektorlarında geniş istifadə olunur. Bu sektorlarda əsas əməliyyatlar KS ilə aparıldığından, onlar bu sistemlərdən çox asılıdır. Nəticədə, bu sistemlərin təhlükəsizliyi əsas məsələlərdən birinə çevrilir. 2001-ci ildən etibarən müxtəlif sektorlarda KS təhlükəsizliyinə çəkilən xərclərin miqdarı əhəmiyyətli dərəcədə artmışdır [1]. Buna görə də KS təhlükəsizliyi sahəsində tədqiqatların aparılması çox vacibdir.

KS təhlükəsizlik səviyyəsi onlardan asılı olan hər bir şirkət və ya təşkilatın normal fəaliyyəti üçün əsasdır. Şirkət və təşkilatların maliyyə gəlirləri əhəmiyyətli dərəcədə KS-in istifadəsinə əsaslandığı üçün təhlükəsizlik sistemlərinə böyük maliyyə xərclənir. Lakin təhlükəsizlik və xərclər arasında müəyyən kompromis olmalıdır.

Çox yüksək təhlükəsizlik KS-i əlçatmaz, qeyri-funksional edir və çox baha başa gəlir, lakin çox aşağı təhlükəsizlik ucuz başa gəlsə də, KS-i hücumlara qarşı son dərəcə zəif edir və onun qeyri-funksionallığına gətirib çıxarır. Buna görə də, təhlükəsizliyi aşağı salmadan xərcləri azaltmaq məqsədilə hər bir hal üçün “nə qədər” təhlükəsizliyin tələb olunduğunun müəyyən edilməsinə böyük ehtiyac vardır.

KS-in gündəlik həyat fəaliyyətlərimizə nüfuz etməsinə baxmayaraq, çox az adam təhlükəsizliyin əhəmiyyəti barədə məlumatla malikdir. Hər gün müxtəlif növ KS-ləri (telefon, şəxsi kompüterlər, kredit kartları, bankomatlar və s.) istifadə olunsa da, istifadəçilər öz fəaliyyətləri ilə bağlı olan etibar və təhlükəsizlik məsələlərini başa düşmürlər. Bu sahədə məlumatlandırma çox vacibdir və KS təhlükəsizliyinin əhəmiyyətini göstərən bir üsul olmadıqda, onun vacibliyi daha da artır. Təhlükəsizliyin qiymətləndirilməsi metodları bu istiqamətdə etibarın yaradılması vasitəsi rolunu oynaya bilər.

KS-in mühasifzəsi zərurəti yeni olmadığından, kompüter təhlükəsizliyi termini artıq innovativ termin kimi səslənmir. Əksər müasir KS-lər onların və saxlanılan məlumatların təhlükəsizliyinin müəyyən səviyyədə təmin olunmasına imkan verən aparat və proqram təminatları ilə təchiz olunmuşdur.

KS-in informasiya təhlükəsizliyinin qiymətləndirilməsi zamanı bir çox amillər nəzərə alınmalıdır. Bu problemin dəqiq həlli üçün xüsusiyyətlərin və ölçülərin müfəssəl və son dərəcə dəqiq siyahısının tərtib edilməsi çox çətin məsələdir. KS-nin təhlükəsizliyinin qiymətləndirilməsi zamanı real irəliləyiş əldə etmək üçün eksperimental metodlar, təhlükəsizlik metrikaları və qabaqcadan xəbər vermək imkanına malik etibarlı təhlükəsizlik modelləri yaradılmalıdır.

KS-in təhlükəsizliyinin qiymətləndirilməsi probleminin həllinə adətən nəzəri cəhətdən yanaşırlar. Çox zaman təklif olunan nəzəri metodlar ilə real həyat arasındakı ziddiyyətin mövcud olması elmi tədqiqatın nəticələrini mübahisə mövzusunə çevirir. Hətta daha çox praktiki perspektivə malik olan tədqiqatlar belə bəzən lazımi nəticələr verə bilmir.

KS-in təhlükəsizliyinin qiymətləndirilməsi problemini bir-biri ilə əlaqəli olan iki müxtəlif hissələrə ayırmaq olar: müvafiq təhlükəsizlik metrikasının müəyyən edilməsi və bu təhlükəsizlik metrikalarına uyğun olaraq KS təhlükəsizliyinin düzgün və dəqiq ölçülməsinə imkan verən metodların işlənməsi.

Hazırda, kompüter sistemlərinin təhlükəsizliyinin qiymətləndirilməsi üçün müxtəlif metodlar təklif edilmişdir [2–5]. Məqalənin əsas məqsədi bu metodların analizi və mövcud problemləri müəyyən etməkdir.

Kompüter sistemlərinin təhlükəsizliyinin qiymətləndirilməsi

KS təhlükəsizliyinin və onun elementlərinin analizi onu tam olaraq müəyyənləşdirməyə imkan vermir. Heç sözsüz ki, onu qiymətləndirmək daha da çətinidir. Buna baxmayaraq, KS-in təhlükəsizliyini yoxlamaq üçün nəyi nəzərə almağın lazım olduğunu müəyyənləşdirmək istiqamətində işlər mövcuddur. Təhlükəsizliyin qiymətləndirilməsi prosesinin müvəffəqiyyətli olması üçün vacib hesab edilən aşağıdakı aspektlər müəyyən edilmişdir [6]:

- təhlükəsizliyin mənası;
- sistemin əhatə dairəsi;
- təhlükəsizliklə bağlı sistemin xüsusiyyətləri;
- qiymətləndirmə prosesinin əhatə dairəsi;
- qiymətləndirmənin etibarlılığı.

Yuxarıdakıların hamısı göstərir ki, qiymətləndirmə prosesinə başlamamışdan əvvəl kifayət qədər çox amil nəzərə alınmalıdır. KS-nin təhlükəsizliyinin ölçülməsi və qiymətləndirməsinin səbəbini, bu prosesin hansı şəraitdə həyata keçirilməsi və hansı nəticələr verəcəyini bilmədən bu prosesə başlamaq yanlış olardı.

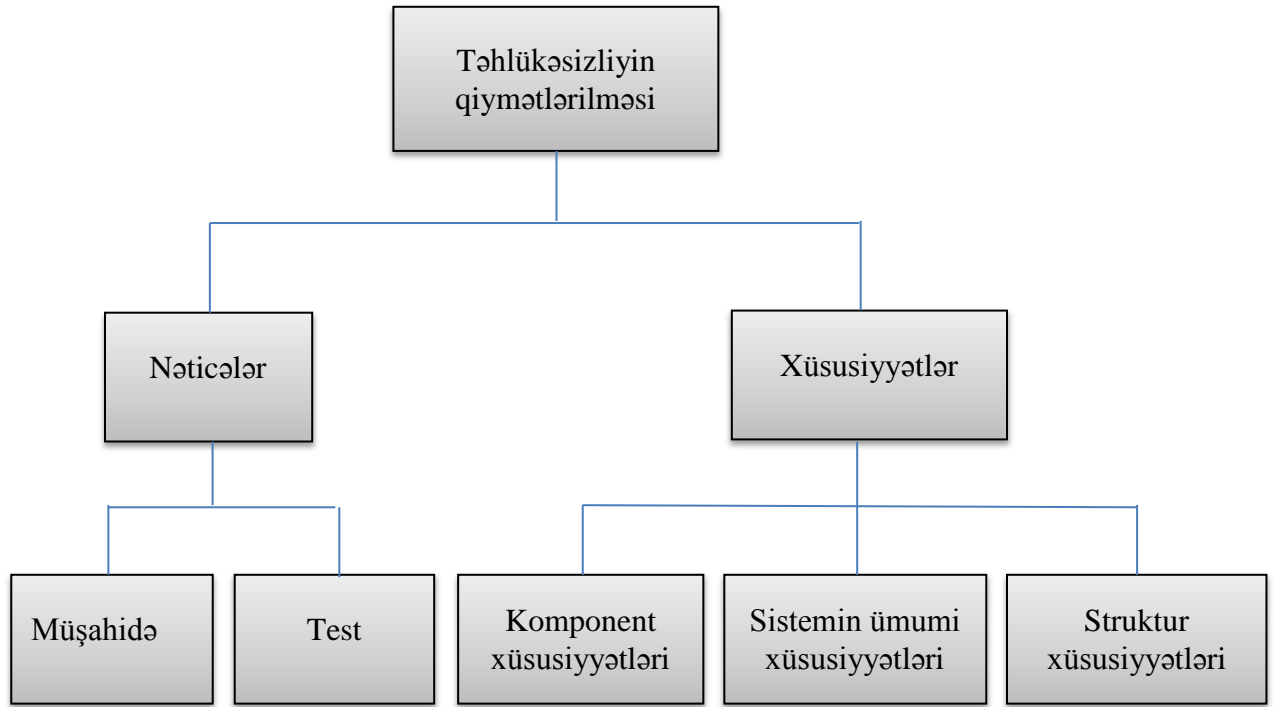
Bundan başqa, təhlükəsizliyin qiymətləndirilməsi prosesi dörd prinsipə əsasən həyata keçirilir [7]:

- sistemin müşahidə olunması – sistemin daxili funksiyaları təhlil edilmədən xaricdən təhlil edilir;
- sistemin kompleks yoxlanılması – sistemin təhlükəsizlik səviyyəsini yoxlamaq üçün əsas mənbə təhlükəsizlik sisteminin keçilməsi testidir (penetrasiya testi);
- sistem təhlükəsizliyinin funksionallığı – sistem təhlükəsizlik zəifliklərinin qarşısını almaq üçün təhlükəsizlik mexanizmləri və tədbirlərinin müəyyən olunması yolu ilə yoxlanılır;
- sistemin strukturu – sistem elementləri və həmin elementlər arasındakı əlaqələr toplusu kimi nəzərə alınır.

Bu yanaşmalar hal-hazırda mövcud olan müxtəlif metodlarda tətbiq olunur və bir-birinə rəqib olmaqdan daha çox tamamlayıcı kimi hesab edilə bilər. Onların bəziləri isə təhlükəsizliyin qiymətləndirilməsi prosesində istifadə oluna bilər.

Paylanmış informasiya sistemləri üçün bu dörd sinif iki əsas kateqoriyaya bölünərək şəkil 1-də göstərilən beş yanaşma təklif edilmişdir [8]. Burada əsas yanaşma ondan ibarətdir ki, sistem ya daxili funksionallığı qeyri-məlum olan qara qutu (nəticələr) və yaxud da sistem xüsusiyyətləri məlum olan tərkib hissələri (xüsusiyyətlər) kimi göstərilir.

Təhlükəsizlik sisteminin keçilməsi testi (penetration test) yanaşmasından istifadə zamanı sistemlər və şəbəkələr ya zəiflikləri yoxlayan skanerlərin (avtomatlaşdırılmış kompüter proqramı), ya da istifadəçilərin təhlükəsizlik təcrübəsindən istifadə edərək sistemlərə “əl ilə” nüfuz etməyə çalışan “qırmızı komandalər”ın (təhlükəsizlik ekspertləri qrupu) köməyi ilə məlum proqram təminatı və ya potensial sistem konfigurasiyası səhvləri yoxlanılır.



Şəkil 1. Təhlükəsizliyin qiymətləndirilməsinə əsas yanaşmalar

Bununla belə, bu metodun zəif cəhəti təkə verilmiş məlumat və vaxt çərçivəsində sistemin və ya şəbəkənin nə dərəcədə təhlükəsiz olduğunu deyil, həmçinin mövcud, lakin yoxlayıcılar məlum olmayan məlumatlardan istifadə etməklə gələcəkdə meydana çıxacaq təhlükələrə qarşı necə təhlükəsiz olduğunu müəyyən edə bilməməsidir.

Təhlükəsizliyin qiymətləndirilməsi metrikaları

Təhlükəsizliyin qiymətləndirilməsi üçün müxtəlif tələb və aspektləri əhatə edən, təklif edilmiş bir neçə metrika mövcuddur [9–11]. Ümumi təyinatlı təhlükəsizlik metrikasını yaratmaq üçün göstərilən hər bir cəhd “ideal” metrika anlayışının bütün sistem və istifadəçilərə tətbiq oluna bilən metrikanı təşkil edən xüsusiyyətlər toplusunun olmadığını sübut etməyə yönəlmişdir [12].

Təhlükəsizlik metrikaları KS-in təhlükəsizliyinin ölçülməsi və əldə olunan nəticələrin şərh edilməsini yerinə yetirir. Onlar təkə emal üçün məlumatın toplanması üsulu deyil, həm də toplanmış məlumatların mənasının izah edilməsi üçün dəyərli bir vasitədir. Buna baxmayaraq, bu vaxta qədər aparılmış əksər tədqiqatlar təhlükəsizliyin idarə edilməsinə və yaxud insan davranışı aspektlərinə yönəlmişdir. Lakin kifayət qədər qənaətbəxş texniki nəticə əldə olunmamışdır, bunun səbəbi hələ də həll edilməmiş iki (ən azı) problemin olmasıdır. Birinci problem metrikanın müəyyən edilməsi və hesablanması üçün hansı məlumatından istifadə edilməsi, ikinci problem isə etibarlı metrikanın müəyyən edilməsi ilə bağlıdır.

Birinci problemin həlli üçün xeyli sayda müxtəlif yanaşmalar təklif edilmişdir. Bəzi tədqiqatçılar hesab edirlər ki, müəyyən məlumatın müəyyən fraqmentlərinin toplanması daha spesifik və etibarlı nəticələr verəcəkdir. Digərləri hesab edir ki, toplanmış məlumatın ölçüsünü genişləndirməklə daha real və reallığa yaxın nəticələr əldə etmək olar, nəticədə, onlar daha dəqiq olar. Buna görə də KS-in təhlükəsizliyinin qiymətləndirilməsi zamanı qarşıya qoyulan məsələdən asılı olaraq, müvafiq miqdarda və növdə məlumat toplanmalıdır.

[13]-də etibarlı metrikanın müəyyən edilməsi probleminin həlli üçün yanaşma təklif edilmişdir.

Müəlliflər etibarlı təhlükəsizlik metrikasının əldə edilməsi üçün beş xüsusiyyətin nəzərə alınmasını təklif edirlər:

- ardıcıl şəkildə ölçülməli, eyni məlumat blokundan istifadə etməklə müxtəlif insanlar eyni nəticələr əldə edə bilməlidir;
- toplanılması ucuz başa gəlməli, asan toplanmalı və hesablama vaxtı çox olmamalıdır;
- yalnız nisbi məhsuldarlıq qiymətləndirilməsi üçün yaxşı olan formada (yüksək, orta, aşağı və s.) deyil, ədədi kəmiyyət və ya faiz kimi də ifadə olunur;
- ən azı bir ölçü vahidindən istifadə etməklə ifadə olunur və nəticələr ölçülənlərin xüsusiyyətlərini ardıcıl şəkildə göstərməklə ifadə olunur;
- anlamaq üçün asan, yararlı, eyni zamanda mənalı və kifayət qədər spesifik olması üçün məzmun baxımından konkret olmalıdır.

İnformasiya təhlükəsizliyinin qiymətləndirilməsinin mövcud metodları

Təhlükəsizliyin qiymətləndirilməsi problemini bir çox tədqiqatçılar tədqiq edir və bu məsələyə müxtəlif yanaşmalar mövcuddur. Ümumi meyarlar (ÜM) kimi bu yanaşmaların bəziləri hətta ISO (Beynəlxalq Standartlaşdırma Təşkilatı) standartlarına da çevirilmişdir [14], lakin hələ də təhlükəsizliyin tam olaraq dəqiq qiymətləndirilməsi problemini həll etməmişdir, çünki onlar müxtəlif suallara müxtəlif şəkildə cavab verir. Təhlükəsizlik termininin müxtəlif izahlarını nəzərə alsaq, bunu başa düşmək elə də çətin olmaz.

Aşağıda kompüter sistemlərinin təhlükəsizliyinin qiymətləndirilməsinin bəzi metodlarının qısa analizi verilmişdir.

Ümumi meyarlar – informasiya texnologiyaları (İT) məhsullarının (aparat təminatı, proqram texniki təminatı, proqram təminatı) təhlükəsizlik səviyyəsini qiymətləndirmək və müqayisə etmək üçün geniş istifadə olunan bir standartdır. ÜM ISO beynəlxalq standartı kimi qəbul edilmişdir (ISO 15408) və onun ən son variantı 3.1.CCv4-dir [14]. Onun əsas məqsədi izafi qiymətləndirmə fəaliyyətlərinin aradan qaldırılması, məhsulun zəmanətliyinə çox az təsir edən fəaliyyətlərin azaldılması/aradan qaldırılması, anlaşılmazlıqların azaldılması üçün ÜM terminologiyasının aydınlaşdırılması, təhlükəsizlik zəmanətinin əldə olunduğu sahələrə qiymətləndirmə fəaliyyətlərinin strukturunun və istiqamətinin dəyişdirilməsi, həmçinin lazım olduqda yeni ÜM tələbləri əlavə etməkdir.

ÜM üç hissədən ibarətdir. Birinci hissə texnologiyaya giriş verir və ümumi modeli təqdim edir, ikinci hissə İT məhsullarının təhlükəsizliyi üçün zəruri olan tələblər toplusunu təsvir edir, üçüncü hissə isə qiymətləndirmə prosesi zamanı həmin məhsullara tətbiq olunan zəmanətlik tədbirlərini təmin edir.

ÜM-in 2-ci hissəsi geniş təhlükəsizliyin funksional tələblərinin (TFT) müəyyən edilməsi ilə başlayır. İT məhsulun kateqoriyasından (məsələn, şəbəkələrarası ekranın aparat təminatı, müdaxilələrin aşkarlanması üzrə proqram təminatı, rəqəmsal müəllif hüquqlarının tətbiqi və s.) asılı olaraq arzu olunan formanı və təhlükəsizlik baxımından bu məhsulların tətbiqini təsvir edən müdafiə profili (MP) yaradılır. Növbəti addım qiymətləndirilən spesifik məhsulun arzuolunan təhlükəsizlik funksionallığını təmin edəcək təhlükəsizlik hədəfinin (TH) təsvir edilməsindən ibarətdir. TH MP tərəfindən verilən ümumi təsvirə əsaslanaraq, məhsulun yekun qiymətləndirilməsi və onun TH-in qoyduğu funksiyalar və qaydalara əsaslanaraq təsdiq olunub-olunmamasını yoxlamaq üçün istifadə olunur. Əvvəlcədən müəyyən olunmuş qiymətləndirmə zəmanəti səviyyələrinə (QZS) uyğun olaraq qiymətləndirməni başa çatdırmaq məqsədilə ÜM-a ümumi qiymətləndirmə metodologiyası adlı standartlaşdırılmış metod əlavə olunur. QZT-nin səkkiz səviyyəsi mövcuddur (QZS 0-dan QZS7-yə qədər) və onlar TFT-nə uyğunluq səviyyəsinin ölçüsüdür.

Sistemin zəiflik indeksi (SZİ) metodu – [3]-də təhlükəsizliyin qiymətləndirilməsi üçün SZİ metodu təklif edilmişdir. Sistemin zəifliyinə səbəb olan üç müxtəlif amil kateqoriya formalaşdırılır və sistemin zəifliyinin abstrakt ölçülməsi barədə qərar qəbul edilir.

Bu üç kateqoriya: sistemin xüsusiyyətlərindən, potensial etinasızlıq hərəkətlərindən və potensial qərəzli hərəkətlərdən ibarətdir. Metodun kəmiyyətə ifadəsi üçün SZİ 0 və 1 arasında ədədi kəmiyyətlər təyin edilir, lakin bu, imtiyazlı istifadəçilər üçün heç bir statistik və ehtimal əhəmiyyəti kəsb etmir. Bu, növbəti qaydada hesablanır. Müəyyən bir amilin sistemin təhlükəsizliyinə təsirinin əminliyini göstərən əminlik indeksi (Əİ) ölçülür. Başqa sözlə, əgər müəyyən bir amil sistemdə varsa, onda sistemin zəifliyinin olmasına dair Əİ əminliyi mövcuddur. Sonra SZİ müxtəlif Əİ ilə ayrı-ayrılıqda hesablanır. Nəticədə, müəlliflər SZİ-nin qiymətini dörd qrupa bölürlər və bu qrupların hər biri sistemin zəifliyinin müxtəlif spektrlərini göstərir.

Çoxpilləli hücum modelləşdirməsi (ÇPHM) metodu – sistemin təhlükəsizliyini onun hücumlara müqaviməti baxımından da qiymətləndirmək olar [4]. ÇPHM metodu konkret şəbəkəyə sistemin boşluğunun istifadəsinə imkan verən hücumun modelləşdirməsinə əsaslanır. Şəbəkənin, zəifliyin və hücum edənin imkanlarının sistemli ekspertizası vasitəsi ilə şəbəkənin məruz qaldığı təsirin effektivliyini analizi verilir. Hücum və təsirlərin mürəkkəbliyi və təhlükəsizliyi pozulmuş şəbəkə elementlərinin şəbəkənin digər sistemləri ilə qarşılıqlı əlaqəsi nəticəsində şəbəkənin təhlükəsizliyində ciddi hadisələrə səbəb ola bilər. Bu hadisələr hücum zəncirləri adlanır. Bu hücumlardan potensial zəifliklərin və hücum yollarının müəyyən edilməsi üçün istifadə edilə bilər. Bu yolla şəbəkədə hücumun yayılması modelləşdirilir. Hər bir mümkün hücum üçün ehtimal müəyyən etməklə, ehtimal nəzəriyyəsinə əsaslanaraq istifadə etməklə hücumun hücum zəncirinin hər bir mərhələsinə çatmaq ehtimalını hesablamaq olar.

Bu metodun çatışmayan cəhəti ondan ibarətdir ki, şəbəkə kifayət qədər təhlil edilməli və şəbəkəyə olan bütün hücumlar və hallar nəzərə alınmalıdır.

Hücumun aşkarlanması metodu (HAM) – təhlükəsizlik nöqtəyi-nəzərindən eyni sistemin iki müxtəlif versiyasını müqayisə etmək məqsədi ilə təhlükəsizliyin qiymətləndirilməsi üçün yeni metrika təqdim edilir [5]. Bu metod Microsoft Windows əməliyyat sistemlərinin müxtəlif versiyalarında sınaqdan keçirilmişdir [15] və onun cari inkişaf mərhələsi texniki hesabatda təqdim edilmişdir [16]. Hücumun aşkarlanması sistemdə baş verən hərəkətlər və onların təsir etdiyi sistem resursları ilə müəyyən olunur. Hər bir hərəkət potensial hücum ola bilər. Bu resurslar giriş və çıxış nöqtəsi adlanır və resurslara hücumun aşkarlanmasını təsvir etmək üçün əlavə olaraq hücum qabiliyyəti anlayışı daxil olunur. Hücum sinfi termini resurslar çoxluğu (metodlar, kanallar və yaxud məlumat elementləri) şəkilində də təqdim olunur ki, onları hücum qabiliyyətindən asılı olaraq təsnif etmək mümkün olsun. Bu metod kod səviyyəsində işləyir, yəni proqram təminatının hissələrinin əsas kodundakı boşluqları yoxlayır. O, təhlükəsizliyin pozulmasına səbəb olan potensial problemlə resursların tapılmasına yönəlir və formasında kəmiyyət nəticələri verir.

Üç növ resurs mövcuddur:

- giriş və çıxış nöqtələri (sistemə/proqram təminatına daxil olmaq üçün icazə verən metod və ya funksiyalar);
- açıq kanallar çoxluğu (proqram təminatının xarici mühitlə əlaqə yaratmasına imkan yaradan şəbəkə portları);
- etibarsız məlumat elementləri çoxluğu (təyin olunmuş daxilolma səviyyəsinə görə təhlükəsizlik problemlərinə səbəb olan məlumatlar/fayllar).

Bu metodda, proqram təminatının təhlükəsizlik keyfiyyətinə dair nəticələr çıxarmaq məqsədilə, iki səbəbdən proqram təminatı səhvləri nəzərə alınmır. Bəzi səhvlər yoxlama prosesi zamanı gözdən qaça bilər və buna bütün proqram təminatı səhvlərinə bərabər əhəmiyyət verilir. Əksinə, hücumun aşkarlanması metodu təkə kodun təhlükəsizliyini deyil, həm də hər bir fərdi tətbiq zamanı rast gəlinən konfigurasiya parametrlərini də yoxlayır. Bununla belə, problem ondadır ki, müəyyən olunmuş göstəricilər olmadığından, onlar yalnız müqayisəli metrika kimi istifadə oluna bilər. İstifadə olunan işarələmələr müəyyən proqramlara uyğun gəlir və proqram təminatının bir hissəsinin iki giriş nöqtəsi və ya məlumat elementlərinin digər proqram hissəsinin

ekvivalent resursları ilə eyni çəkiyə malik olduğunu düşünmək yanlış olardı. Bundan başqa, əvvəlcədən verilmiş üçlükdə ikidən artıq parametr olduqda (giriş nöqtələri, kanallar, məlumat elementləri), hətta eyni proqram təminatının iki müxtəlif versiyaları arasında hansının daha təhlükəsiz olmasına dair nəticə çıxarmaq asan olmur. Bu metod elmi cəhətdən güclü olmasına baxmayaraq, yalnız xüsusi hallarda tətbiq oluna bilər.

Nəticə

KS-nin təhlükəsizliyi binar xüsusiyyətə malik deyil. Onun qiymətləndirilməsi zamanı çoxlu sayda faktorlar nəzərə alınmalıdır. KS-nin təhlükəsizliyinin qiymətləndirilməsi üçün müfəssəl, dəqiq funksiyalar və ölçmələr bu gün də problem olaraq qalmaqdadır. KS-in təhlükəsizliyinin qiymətləndirilməsi sahəsində real irəliləyişə nail olmaq üçün problemlərin müəyyən edilməsi və eksperimental metodların, dəqiq təhlükəsizlik metrikalarının və modellərinin yaradılması zəruridir.

Məqalədə KS-nin təhlükəsizliyinin qiymətləndirilməsinin bəzi standart və metodları, o cümlədən Ümumi Meyarlar standartı, sistemin zəiflik indeksi, çoxpilləli hücum modelləşdirməsi, hücumun aşkarlanması metodları analiz edilmiş və mövcud problemlər müəyyən edilmişdir. Həmçinin KS-nin təhlükəsizliyinin qiymətləndirilməsinə əsas yanaşmalar və qiymətləndirmə metrikaları analiz edilmişdir. Bu analizin nəticəsi KS-nin təhlükəsizliyinin qiymətləndirilməsi sahəsində mövcud olan bəzi problemlərin həll edilməsinə imkan verəcək.

Ədəbiyyat

1. Olsen F. Input: IT security spending to catch its breath. <http://www.fcw.com/article89546-07-13-05>.
2. Common Criteria for Information Technology Security Evaluation, Part 1: Introduction and General Information, Part 2: Security Functional Requirements, Part 3: Security Assurance Requirements, Version 3.1 Revision 1, September 2006.
3. Foss A.J., Barbosa S., Assessing Computer Security Vulnerability // Operating Systems Review, July 1995, vol. 29, no. 3, pp. 3–13.
4. Clark K., Tyree S., Dawkins J., Hale J. Qualitative and Quantitative Analytical Techniques for Network Security Assessment / Proceedings of the 2004 IEEE Workshop on Information Assurance and Security, June 10-11, 2004, United States Military Academy, West Point, NY, pp. 321–328.
5. Howard M., Pincus J. Wing J. Measuring Relative Attack Surfaces // Computer Security in the 21st Century, D.T. Lee, S.P. Shieh, and J.D. Tygar, editors, Springer, March 2005, pp. 109–137.
6. Hallberg J., Hunstad A., Peterson A. Framework for System Security Assessment / Proceedings of the 2005 IEEE Workshop on Information Assurance, June, 2005, West Point, New York, USA, pp. 224–231.
7. Hallberg J., Hunstad A., Bond A., Peterson M., Pålsson N. System IT Security Assessment, Scientific Report, Swedish Research Agency, Linköping, FOI-R-1468-E, 2004.
8. Gacic D. FSA – Framework for Security Assessment of Distributed Information Systems. Master's thesis, Royal Institute of Technology, Stockholm, Sweden, 2006.
9. Schudel G., Wood B. Adversary Work Factor as a Metric for Information Assurance / Proceedings of the New Security Paradigm Workshop, September 18-22, 2000, Ireland, pp. 23–30.
10. Swanson M., Bartol N., Sabato J. and Hash J. Security metrics guide for information technology systems. Technical Report NIST Special Publication 800-55, NIST, July 2003.
11. Manadhata P., Wing J. An Attack Surface Metric, Carnegie Mellon University, CMU-CS-05-155, 2005.

12. Chew E, Swanson M., Stine K., Bartol N., Brown A. and Robinson W. Performance Measurement Guide for Information Security. NIST Special Publication 800-55 Revision 1, July 2008.
13. Vaughn R., Henning R., Siraj A. Information Assurance Measures and Metrics – State of Practice and Proposed Taxonomy / Proceedings of the 36th Hawaii International Conference on System Sciences, January 6-9, 2003, Big Island, HI, USA.
14. <http://www.commoncriteriaportal.org/cc/>
15. Howard M., Fending Off Future Attacks by Reducing Attack Surface, 2003.
16. Jaquith A. Metrics are nifty / Proceedings of the MetriCon 1.0 Workshop in conjunction with the USENIX Association's Security Symposium, August 1, 2006, Vancouver, British Columbia, Canada.
www.securitymetrics.org/content/attach/Metricon1.0/metricon-1.0-presentations.zip

УДК 004.054

Шыхалиев Рамиз Г.¹, Юнусов Турал Е.²

Институт Информационных Технологий НАНА, Баку, Азербайджан

¹ramiz@sciencez.az, ²turaly@mail.ru

Методы оценки безопасности компьютерных систем

В статье были проанализированы некоторые стандарты и методы оценки безопасности компьютерных систем, такие, как общие критерии, индекс системной уязвимости, моделирование многоступенчатой атаки, обнаружение атаки, определены некоторые существующие проблемы.

Ключевые слова: компьютерные системы, оценка безопасности, метрика безопасности, методы оценки безопасности.

Ramiz H. Shikhaliyev¹, Tural E. Yunusov²

Institute of Information Technology of ANAS, Baku, Azerbaijan

¹ramiz@sciencez.az, ²turaly@mail.ru

Methods for assessing the security of computer systems

The article analyzed some of the standards and methods of security assessment of computer systems, such as the common criteria, the index of systemic vulnerability, modeling of multi-stage attacks, intrusion detection, and identified some problems.

Key words: computer systems, security assessment, security metrics, methods of security assessment.