UOT 004.387

İNFORMASİYANIN MÜHAFİZƏSİ SİSTEMİNDƏ SƏMƏRƏLİYİNİN QİYMƏTLƏNDİRİLMƏSİ METODİKASI

Rəsmiyyə İsrayıl qızı Əmiraslanova
Mingəçevir Dövlət Universiteti
Azərbaycan Dövlər Pedaqoji Universitetinin dissertantı
rasmiyya.amiraslanova@mdu.edu.az

Xülasə: *İnternet texnologiyalarının və e-ticarətin inkişafı ilə hər gün informasiya təhlükəsizliyinə daha çox təhlükə yaranır. Bu gün təşkilatlar idarəetmə qərarlarını asanlaşdırmaq və biznes aparmaq üçün biznes proseslərində informasiyadan getdikcə daha çox istifadə edirlər.*

Bir çox ticarət əməliyyatları internet vasitəsilə elektron şəkildə həyata keçirildiyi üçün biznes mühitində informasiyadan asılılıq son dərəcə yüksəkdir. Bu informasiya asılılığı informasiya sistemlərinin təhlükəsizliyi səviyyəsinin uğura, bəzən hətta bizneslə məşğul olmaq qabiliyyətinə təsirinin əhəmiyyətli dərəcədə artmasına səbəb olmuşdur. Ona görə də informasiya sistemlərinin təhlükəsizliyin səmərəli qiymətləndirilməsi metodikası informasiya təhlükəsizliyi sahəsində analitiklərin, mühəndislərin və digər mütəxəssislərin diqqətini cəlb edən ən mühüm məsələlərdən biridir. Təklif olunan elmi işdə, informasiya təhlükəsizliyinin qiymətləndirilməsi prosesinin əsas elementləri təyin olunmuşdur.

Açar sözlər: *informasiya təhlükəsizliyi, məxfilik, dürüstlük, əlçatanlıq, qiymətləndirmə metodikası*

Giriş

Müasir rəqəmsal texnologiyalar fərdin, cəmiyyətin və dövlətin bütün fəaliyyət sahələrinə daxil edildiyi üçün hesablama texnikası və avtomatlaşdırılmış sistemlərin informasiya təhlükəsizliyinin təmin edilməsi məsələsi getdikcə aktuallaşır. Buna görə də rəqəmsal texnologiyanın və ya avtomatlaşdırılmış sistemdə informasiya təhlükəsizliyi sistemlərinin inkişafına yönəlmiş üsul və metodların yaradılması və tətbiqi aktualdır. Bu tip sistemlərdə informasiya təhlükəsizliyi sisteminin yaradılmasında ən böyük çətinlik sistemdə istifadə olunan hər bir məxfi məlumat növünün, onun daşıyıcılarının və emal proseslərinin qorunması üçün tələblərin formalaşdırılması mexanizmidir. Təhlükəszilik problemi ilk növbədə hesablama qurğularında saxlanılan və emal edilən məlumatların məxfilik, bütövlüyü və əlçatanlığına dair tələblərin miqyasının müqayisəli qiymətləndirilməsi üçün formal modellərin olmaması ilə əlaqədardır. Bu problemin həllinə klassik yanaşma məlumatın yalnız bir təhlükəsizlik xüsusiyyətinin, onun məxfiliyinin nəzərə alınmasına əsaslanır [1].

İnformasiyanın bütövlüyünü və əlçatanlığını təmin etmək üçün tələblər, bir qayda olaraq, dolayısı ilə kompüter avadanlıqlarına və sistemlərinə ümumi tələblərdə özünü göstərir. Bu məqsədlə, lokal şəbəkələrdə informasiya hansı səviyyədə qorunması zəruri və vacibdir. Səviyyələr informasiya subyektlərinə dəyən mümkün zərərin miqyasına əsaslanaraq konkret olaraq dəqiqləşdirilir. Səviyyənin müəyyən edilməsi proseduru adətən aşağıdakı kimi təsvir olunur:

- informasiya aktivlərinin növlərinin siyahısı tərtib edilir. Bunun üçün məlumatlar mövzuya, funksional təyinata, informasiya texnologiyalarının eyniliyinə və digər əlamətlərə görə təsnifləşdirilir;
- hər bir məlumat növü və informasiya təhlükəsizliyinin hər bir aktivləri üçün təşkilat səviyyəsində meyarlar müəyyənləşdirilir;
- informasiya aktivlərinin hər bir növü üçün subyektin əhəmiyyəti və onun vurduğu zərərin dərəcələri nəzərə alınmaqla, informasiya təhlükəsizliyi xassələrinin hər biri üçün zəruri təhlükəsizlik dərəcəsi müəyyən edilir [3].

Qeyd olunanları nəzərə alaraq, informasiyaın səmərəli qorunması mexanizmin yaradılması aktualdır.

Problemin qoyuluşu

İnformasiya Təhlükəsizliyi proqramları adətən MDƏ (CIA) kimi tanınan 3 məqsəd ətrafında qurulur – *Məxfilik, Dürüstlük, Əlçatanlıq* [7].

Məxfilik – məlumatın icazəsiz şəxslərə, qurumlara və prosesə açıqlanmaması deməkdir. Məsələn, istifadəçinin gmail hesabı üçün parolu var, bu parolu gmail hesabına daxil olarkən kimsə gördü. Bu halda mənim parolum oğurlanıb və məxfilik pozulub.

Dürüstlük – məlumatların dəqiqliyini və tamlığını qorumaq deməkdir. Bu o deməkdir ki, verilənlər icazəsiz şəkildə redaktə edilə bilməz. Məsələn, bir işçi təşkilatı tərk edərsə, bu halda hesablar kimi bütün departamentlərdə həmin işçi üçün məlumatlar statusu yenilənməlidir ki, məlumatlar tam və dəqiq olsun və buna əlavə olaraq yalnız səlahiyyətli şəxsə icazə verilməlidir.

Mövcudluq – məlumatın lazım olduqda mövcud olması deməkdir. Məsələn, işçinin məzuniyyətlərin sayını ötüb-keçmədiyini yoxlamaq üçün konkret işçinin məlumatlarına daxil olmaq lazımdırsa, bu halda şəbəkə əməliyyatları, inkişaf əməliyyatları, insidentlərə reaksiya və siyasət/dəyişikliklərin idarə edilməsi kimi müxtəlif təşkilati komandaların əməkdaşlığı tələb olunur.

Xidmətdən imtina hücumu məlumatın mövcudluğuna mane ola biləcək amillərdən biridir. Bundan başqa, informasiya təhlükəsizliyi proqramlarını tənzimləyən daha bir prinsip var. Bu, rədd edilməməsidir.

İmtina etməmək – bir tərəfin mesaj və ya əməliyyatı qəbul etməyi inkar edə bilməyəcəyi, digər tərəfin isə mesaj və ya əməliyyatın göndərilməsini inkar edə bilməyəcəyi deməkdir. Məsələn, kriptoqrafiyada mesajın göndərənin şəxsi açarı ilə imzalanmış rəqəmsal imzaya uyğun olduğunu göstərmək kifayətdir və həmin göndərənin göndərilmiş mesajı ola bilər və onu tranzit zamanı başqa heç kim dəyişdirə bilməz. Məlumatların bütövlüyü və həqiqiliyi rədd edilməməsi üçün ilkin şərtlərdir.

Həqiqilik – istifadəçilərin onların dedikləri şəxs olduğunu və təyinat yerinə gələn hər bir məlumatın etibarlı mənbədən olduğunu yoxlamaq deməkdir. Bu prinsipə əməl olunarsa, etibarlı ötürmə vasitəsilə etibarlı mənbədən alınan etibarlı və həqiqi mesajı təmin edir. Məsələn, yuxarıdakı nümunəni götürsək, göndərən mesajı mesajın hash dəyərindən və şəxsi açardan istifadə edərək yaradılan rəqəmsal imza ilə birlikdə göndərir. İndi qəbuledici tərəfdə bu rəqəmsal imza hash dəyəri yaradan açıq açardan istifadə etməklə deşifrə edilir və mesaj hash dəyərini yaratmaq üçün yenidən heşlənir. Əgər iki dəyər uyğun gəlirsə, o, həqiqi ilə etibarlı ötürmə kimi tanınır və ya alıcı tərəfdə orijinal mesajın alındığını deyirik.

Hesabatlılıq o deməkdir ki, müəssisənin hərəkətlərini yalnız həmin quruma aid etmək mümkün olmalıdır. Məsələn, dürüstlük bölməsində müzakirə etdiyimiz kimi, hər bir işçiyə digər işçilərin məlumatlarında dəyişiklik etməyə icazə verilməməlidir. Bunun üçün bir təşkilatda bu cür dəyişikliklərin edilməsinə cavabdeh olan ayrıca bir şöbə var və onlar dəyişiklik üçün müraciət aldıqda, həmin məktub yuxarı orqan tərəfindən imzalanmalıdır, məsələn, kollecin direktoru və həmin dəyişikliyi təyin edən şəxs edə bilər. Onun biometriklərini yoxladıqdan sonra dəyişdirilir, beləliklə istifadəçi ilə vaxt möhürü (dəyişikliklər edir) təfərrüatları qeyd olunur. Beləliklə, deyə bilərik ki, əgər dəyişiklik bu şəkildə baş verərsə, o zaman hərəkətləri yalnız bir varlığa görə izləmək mümkün olacaq.

İnformasiya Təhlükəsizliyinin əsasını İnformasiya Təminatı təşkil edir ki, bu da informasiyanın CIA-nın saxlanması, kritik məsələlər yarandıqda məlumatın heç bir şəkildə pozulmamasını təmin etmək deməkdir. Bu məsələlər təkcə təbii fəlakətlər, kompüter-server nasazlığı və s. ilə məhdudlaşmır. Beləliklə, informasiya təhlükəsizliyi sahəsi son illərdə əhəmiyyətli dərəcədə böyüyüb və inkişaf edib. Şəbəkələrin və müttəfiq infrastrukturun təhlükəsizliyinin təmin edilməsi, tətbiqlərin və verilənlər bazalarının təhlükəsizliyinin təmin edilməsi, təhlükəsizlik testi, informasiya sistemlərinin auditi, biznesin davamlılığının planlaşdırılması və s. o cümlədən ixtisaslaşma üçün bir çox sahələr təklif edir.

Qeyd olunanları nəzərə alsaq, idarəetmə sistemlərində təhlükəsizliyin səmərəliyinin qiymətləndirilməsi metodikası aşağıdakı problemlərin həllinə imkan verəcəkdir [4]:

− zərərli hücumların axınının intensivliyi;
− əks olunan hücumların axınının intensivliyi;
− hücumlar üçün istifadə olunan kanalların sayı;
− hücumların serverə təsiri qaydaları (xidmət intizamı);
− sındırma ehtimalı;
− rabitə kanalı üzərindən hücumların sayı;
− müşahidə vaxtı və s.

Problemin həlli

Yuxarıda qeyd olunan problemləri aradan qaldırmaq üçün təklif olunan qiymətləndirmə metodikası aşağıdakıları əhatə edir:

- subyektlərin əhəmiyyətinin müqayisəli qiymətləndirilməsi metodu, hər bir subyekt üzrə məlumatın məxfilik, bütövlüyü və mövcudluğu göstəricilərinin əhəmiyyəti;
- informasiya münasibətlərinin subyektlərinin məlumatın məxfiliyinə, bütövlüyünə və əlçatanlığına dair eyni tələblərlə siniflərə bölünməsi üsulu.

Konseptual olaraq, metod iyerarxiya təhlili sxeminə və klaster analizinə əsaslanır.

İT təhlükəsizliyinin qiymətləndirilməsi üzrə normativ sənədlər praktiki olaraq konkret metodları ehtiva etmir, bunun nəticəsində ümumi bəyannamələr və onların müddəalarının həyata keçirilməsi və nəzarəti üçün xüsusi alətlər arasındakı boşluğun ölçüsü qəbuledilməzdir. Məqsəddən asılı olaraq, metodoloji baza informasiya təhlükəsizliyi tələblərinin yerinə yetirilməsinin təmin edilməsi və yoxlanılmasının bütün mühüm aspektlərini əhatə etməlidir. İnformasiya təhlükəsizliyi sisteminin effektivliyinin qiymətləndirilməsinin obyektivliyi həyata keçirilən təhlükəsizlik mexanizmlərinin faktiki fəaliyyətini və onların tələblərə uyğunluğunu yoxlamaq, habelə statistik məlumatların təqdim edilməsi üçün nəzərdə tutulmuş funksional sınaqdır.

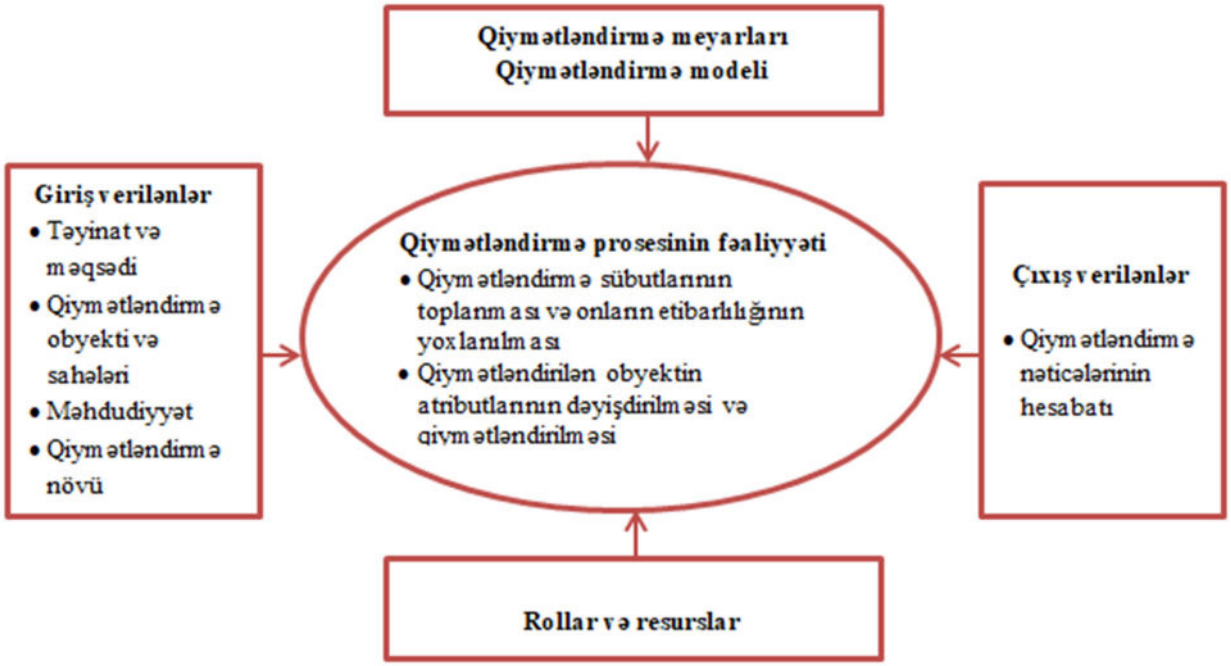
Təhlükəsizlik alətlərinin təhdidlərə qarşı məhdud imkanlara malik olması səbəbindən, sınaq zamanı təhlükəsizlik mexanizmləri yan keçməsə və ya bloklanmasa belə, həmişə təhlükəsizlik pozuntusu ehtimalı var. Bu ehtimalı qiymətləndirmək üçün əlavə tədqiqatlara ehtiyac var. Metodologiya baxımından, informasiya təhlükəsizliyi sisteminin effektivliyinin müəyyən edilməsi müvafiq göstəricilərin ölçülməsi əsasında personalın fəaliyyət metodunun uyğunluğu və ya texniki vasitələrin informasiyanın mühafizəsi məqsədinə çatmaq üçün uyğunluğu barədə mülahizələrin hazırlanmasından ibarət olmalıdır. Məsələn, funksional sınaq zamanı aşağıdakı problemləri həll etmək üçün səmərəlilik qiymətləndirilir:

- məqsədə çatmaq üçün müxtəlif amillərin töhfələrinin müəyyən edilməsi;
- informasiya sisteminin təhlükəsizliyinin səmərəliliyinin artırılması yollarının müəyyən edilməsi;
- alternativ sistemlərin müqayisəsi.

Belə ki, müasir metodoloji bazadan istifadə zamanı informasiya sisteminin təhlükəsizliyinin effektivliyinin qiymətləndirilməsi, əsasən, qeyri-səlis, subyektiv xarakter daşıyır. Mümkün təsadüfi və ya qəsdən təsirləri nəzərə alan standartlaşdırılmış kəmiyyət göstəriciləri, demək olar ki, yoxdur. Nəticədə, onun elementlərinə icazəsiz təsirlər olduqda bir məlumat sisteminin işləmə keyfiyyətini qiymətləndirmək və buna uyğun olaraq dizayn edilmiş sistemin bir versiyasının niyə daha yaxşı olduğunu müəyyən etmək olduqca çətindir və çox vaxt qeyri-mümkündür [2]. Görünür, informasiya təhlükəsizliyi sisteminin səmərəliliyinin hərtərəfli qiymətləndirilməsi probleminin həlli hətta layihələndirmə mərhələsində təhlükəsizlik səviyyəsinin kəmiyyətcə qiymətləndirilməsinə və risklərin idarə edilməsi mexanizminin yaradılmasına imkan verən sistemli yanaşmadan istifadə etməkdir [5].

İnformasiya təhlükəsizliyinin qiymətləndirilməsi prosesi aşağıdakı elementləri şək. 1-də təqdim edilmişdir.

Şək. 1-dən göründüyü kimi, struktur sxem aşağıdakı elementlərdən ibarətdir:
- giriş məlumatları;
- qiymətləndirmə meyarları;
-qiymətləndirmə modeli;
-qiymətləndirmə prosesinin fəaliyyəti;
-qiymətləndirmə nəticəsi.



Şək. 1. İnformasiya təhlükəsizliyinin qiymətləndirilməsi prosesinin əsas elementləri

Təşkilatın İS-nin qiymətləndirilməsi üsullarının xüsusiyyətlərini nəzərdən keçirməzdən əvvəl hər hansı bir İS qiymətləndirməsi üçün ümumi olan komponentləri təsvir etmək lazımdır: qiymətləndirmənin konteksti, qiymətləndirmə sübutlarının toplanması və onların etibarlılığının yoxlanılması, atributların ölçülməsi və qiymətləndirilməsi, müxtəlif növ qiymətləndirmələr (müstəqil qiymətləndirmə, özünüqiymətləndirmə) və qiymətləndirmənin nəticəsi [6].

Nəticə

İnformasiya təhlükəsizliyi sisteminin tələb olunan təhlükəsizlik səviyyəsininə dərəcədə təmin etdiyi sualına cavab vermək üçün informasiya təhlükəsizliyi sisteminin effektivliyini ehtimal xarakteri daşıyan göstəricilərlə qiymətləndirmək lazımdır. İnformasiya təhlükəsizliyi sahəsində normativ-hüquqi bazanın, metodiki təminatın təkmilləşdirilməsi, ilk növbədə, bu istiqamətdə baş verməlidir. İnformasiya təhlükəsizliyi sistemlərinin effektivliyinin qiymətləndirilməsində əhəmiyyətli nəticələr sistematik bir yanaşmanın olması mütləqdir.

İstifadə edilmiş ədəbiyyat

1. Воробьев Е.Г., Петренко С.А., Ковалева И.В., Абросимов И.К. Организация доверенных расчетов в ответственных объектах информатизации в условиях неопределенности. В материалах 20-й Международной конференции IEEE по программным вычислениям и измерениям (24-26 мая 2017 г., Санкт-Петербург, Россия). СКМ 2017, 2017, с. 299 - 300. DOI: 10.1109/SCM.2017.7970566

2. Сахно В. В., Маршаков Д. В., Айдинян А. Р. Применение методов нечеткой логики для решения задачи обеспечения информационной безопасности. Молодой исследователь Дона / № 4 (13), Ростов-на-Дону: Издательский центр ДГТУ, 2018, с. 26-34. URL: http://mid-journal.ru

3. Долженко А.И. Модель анализа риска потребительского качества проектов экономических информационных систем // Вестник Северо-Кавказского государственного технического университета, 2009, № 1 (18), с.129-134

4. Лукинова О.В. Семантическое описание факторов безопасности информационных систем при проектировании системы защиты, Системы высоко! доступности, 2013, № 3, с.149-156

5. Мустафаева А.М. Анализ рисков информационной безопасности. Инновационные научные исследования. Электронное издание, Научный журнал. № 1-1(15), 2022, с.56-62

6. Minyaev A., Krasov V., Saharov V. The method and methodology of efficiency assessment of protection system of distributed information systems // 2020 12th International Congress on Ultra Modern Telecommunications and Control Systems and Workshops (ICUMT) / Brno, Czech Republic. 2020

7. The CIA Triad Of Information Security. 2022. URL: https://uniserveit.com/blog/the-cia-triad-of-information-security

METHODOLOGY FOR ASSESSING THE EFFECTIVENESS OF THE INFORMATION SECURITY SYSTEM

R.Amiraslanova
Mingachevir State University
candidate for PhD degree of Azerbaijan State Pedagogical University

Abstract: *With the development of Internet technologies and e-commerce, more and more threats to information security arise every day. Organizations today increasingly use information in their business processes to facilitate management decisions and conduct business.*

Since many commercial transactions are carried out electronically through the Internet, the dependence on information in the business environment is extremely high. This dependence on information has led to a significant increase in the impact of the security level of information systems on the success, sometimes even on the ability to do business. Therefore, the method of effective evaluation of the security of information systems is one of the most important issues that attract the attention of analysts, engineers and other specialists in the field of information security. In the proposed scientific work, the main elements of the information security assessment process are determined.

Keywords: *information security, confidentiality, integrity, accessibility, assessment methodology*

МЕТОДИКА ОЦЕНКИ ЭФФЕКТИВНОСТИ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ

Р.И.Амирасланова
Мингячевирский государственный университет
диссертант Азербайджанского государственногопедагогического университета

Резюме: *С развитием интернет-технологий и электронной коммерции с каждым днем возникает все больше угроз информационной безопасности. Сегодня организации все чаще используют информацию в своих бизнес-процессах для облегчения принятия управленческих решений и ведения бизнеса.*

Поскольку многие коммерческие операции осуществляются в электронном виде через Интернет, зависимость от информации в бизнес-среде чрезвычайно высока, что привело к значительному увеличению влияния уровня безопасности информационных систем на успех, иногда даже на умение вести дела. Поэтому метод эффективной оценки защищенности информационных систем является одним из важнейших вопросов, привлекающих внимание

аналитиков, инженеров и других специалистов в области информационной безопасности. В предлагаемой научной работе определены основные элементы процесса оценки информационной безопасности.

Ключевые слова: *информационная безопасность, конфиденциальность, целостность, доступность, методология оценки*

Elmi redaktor: tex.f.d., dos. E.İsrafilova
Çapa təqdim edən redaktor: tex.f.d., dos. A.Əliyeva
Daxil olub: 01.02.2023
Çapa qəbul edilib: 08.02.2023