UDC 004.056
DOI https://doi.org/10.52171/herald.412

Methods for Preventing Security Vulnerabilities in Software Systems

E.E. Abbasov

Azerbaijan State Oil and Industry University (Baku, Azerbaijan)

For correspondence:
Emil Abbasov / e-mail: emilabbas679@gmail.com

Abstract

This paper investigates methods for preventing security vulnerabilities in software systems and analyzes architectural and cryptographic mechanisms used to ensure information security. The rapid growth of digital services and information systems has significantly increased the importance of software security. The study proposes a multi-layered security approach aimed at reducing vulnerabilities in software applications. The proposed approach integrates secure programming practices, cryptographic protection mechanisms, and security monitoring techniques. Various data protection methods, including symmetric and asymmetric encryption algorithms as well as cryptographic hash functions, are examined. Mathematical models and risk assessment techniques are applied to evaluate potential security threats and vulnerabilities within software environments. In addition, statistical and analytical approaches are used to evaluate the effectiveness of implemented security mechanisms. The analysis demonstrates that the application of cryptographic methods and secure development practices significantly reduces the number of security vulnerabilities in software systems. The proposed framework contributes to improving system reliability, strengthening information protection, and enhancing the overall security level of modern information systems.

Keywords: software security, cryptography, security vulnerabilities, risk analysis, information systems.

Submitted *2 February 2026*
Published *30 March 2026*

For citation:
E.E. Abbasov
[Methods for Preventing Security Vulnerabilities in Software Systems]
Herald of the Azerbaijan Engineering Academy, *ONLINE*
ISSN (e): 2789-8245

Proqram təminatında təhlükəsizlik boşluqlarının qarşısının alınması metodları

E.E. Abbasov
Azərbaycan Dövlət Neft və Sənaye Universiteti (Bakı, Azərbaycan)

Xülasə

Məqalədə proqram təminatında təhlükəsizlik boşluqlarının qarşısının alınması üçün istifadə olunan memarlıq prinsipləri, kriptoqrafik müdafiə mexanizmləri və təhlükəsizlik modelləri tədqiq edilir. Müasir informasiya sistemlərinin geniş yayılması və rəqəmsal xidmətlərin sürətli inkişafı proqram təminatının təhlükəsizliyinə olan tələbləri əhəmiyyətli dərəcədə artırmışdır. Məqalədə proqram təminatında təhlükəsizlik risklərinin azaldılması üçün çoxsəviyyəli təhlükəsizlik yanaşması təklif olunur. Təklif olunan yanaşma təhlükəsiz proqramlaşdırma prinsiplərini, kriptoqrafik metodları və təhlükəsizlik monitorinqi mexanizmlərini özündə birləşdirir. Məlumatların qorunması üçün simmetrik və asimmetrik şifrələmə alqoritmləri, həmçinin hash funksiyalarının tətbiqi təhlil edilir. Təhlükəsizlik risklərinin qiymətləndirilməsi üçün riyazi modellər və risk analizi metodları istifadə olunur. Bundan əlavə, proqram təminatında təhlükəsizlik tədbirlərinin effektivliyi statistik və analitik yanaşmalar əsasında qiymətləndirilir. Aparılan təhlil göstərir ki, kriptoqrafik metodların və təhlükəsiz proqramlaşdırma prinsiplərinin tətbiqi proqram təminatında mövcud təhlükəsizlik boşluqlarının əhəmiyyətli dərəcədə azaldılmasına imkan verir. Təklif olunan yanaşma informasiya sistemlərinin təhlükəsizlik səviyyəsinin artırılmasına və proqram təminatının etibarlılığının yüksəldilməsinə kömək edir.

Açar sözlər: proqram təminatı təhlükəsizliyi, kriptoqrafiya, təhlükəsizlik boşluqları, risk analizi, informasiya sistemləri.

Методы предотвращения уязвимостей безопасности в программном обеспечении

Э.Э. Аббасов
Азербайджанский Государственный Университет Нефти и Промышленности (Баку, Азербайджан)

Аннотация

В статье исследуются методы предотвращения уязвимостей безопасности в программном обеспечении, а также анализируются архитектурные и криптографические механизмы обеспечения информационной безопасности. Быстрое развитие цифровых сервисов и информационных систем значительно повышает требования к безопасности программного обеспечения. В работе предлагается многоуровневая модель защиты, направленная на снижение количества уязвимостей в программных системах. Предложенный подход объединяет принципы безопасного программирования, криптографические механизмы защиты данных и методы мониторинга безопасности. Рассматриваются различные методы защиты данных, включая симметричное и асимметричное шифрование, а также криптографические хэш-функции. Для оценки рисков безопасности используются математические модели и методы анализа угроз. Кроме того, эффективность реализованных механизмов защиты оценивается с использованием статистических и аналитических методов. Полученные результаты показывают, что применение криптографических методов и принципов безопасной разработки существенно снижает количество уязвимостей в программных системах. Предложенный подход способствует повышению надежности информационных систем и улучшению уровня их безопасности.

Ключевые слова: безопасность программного обеспечения, криптография, уязвимости безопасности, анализ рисков, информационные системы.

Giriş

Müasir dövrdə informasiya texnologiyaları cəmiyyətin inkişafında mühüm rol oynayır. Rəqəmsal texnologiyaların sürətli inkişafı proqram təminatının müxtəlif sahələrdə geniş tətbiq olunmasına səbəb olmuşdur. Dövlət idarəçiliyində, biznes sektorunda, təhsildə və digər sahələrdə informasiya sistemlərindən aktiv şəkildə istifadə edilir. Bu sistemlər böyük həcmdə məlumatların toplanması, saxlanması və emalını təmin edir. Proqram təminatının geniş yayılması ilə yanaşı təhlükəsizlik məsələləri də daha aktual xarakter almağa başlamışdır.

Veb tətbiqlər və informasiya sistemləri istifadəçilərin şəxsi məlumatlarını, maliyyə məlumatlarını və digər həssas informasiyanı saxlayır. Bu səbəbdən proqram təminatının təhlükəsizliyi müasir dövrdə ən vacib məsələlərdən biri hesab olunur. Təhlükəsizlik boşluqları proqram təminatının zəif tərəflərini təşkil edir və bu boşluqlar müxtəlif kiber hücumlar üçün imkan yaradır. Hücum edən şəxslər bu zəifliklərdən istifadə edərək sistemlərə icazəsiz daxil ola və məlumatları ələ keçirə bilirlər.

Son illərdə dünyada kibercinayətkarlığın səviyyəsi əhəmiyyətli dərəcədə artmışdır. Bir çox təşkilatlar təhlükəsizlik boşluqları səbəbindən ciddi maliyyə və reputasiya itkiləri ilə üzləşmişdir. Bu problemlər proqram təminatının hazırlanması prosesində təhlükəsizlik məsələlərinin daha diqqətlə nəzərdən keçirilməsini zəruri edir. Müasir proqram təminatı yalnız funksional baxımdan deyil, həm də təhlükəsizlik baxımından etibarlı olmalıdır.

Proqram təminatında təhlükəsizlik boşluqları müxtəlif səbəblərdən yarana bilər. Bu səbəblərə proqramlaşdırma səhvləri, zəif autentifikasiya mexanizmləri və istifadəçi məlumatlarının düzgün yoxlanılmaması daxildir [1]. Xüsusilə veb tətbiqlərdə istifadəçi tərəfindən daxil edilən məlumatların düzgün filtrasiya edilməməsi ciddi təhlükəsizlik problemlərinə səbəb olur. Bu kimi zəifliklər SQL Injection, Cross-Site Scripting və digər hücumların yaranmasına şərait yaradır.

Müasir dövrdə proqram təminatının təhlükəsizliyinin təmin edilməsi üçün müxtəlif metod və texnologiyalar tətbiq olunur. Bu metodlar proqram təminatının hazırlanması prosesinin bütün mərhələlərini əhatə edir. Təhlükəsiz proqramlaşdırma prinsipləri, kod auditi və avtomatlaşdırılmış testlər bu istiqamətdə mühüm rol oynayır. Bundan əlavə, müasir autentifikasiya mexanizmləri proqram təminatının daha təhlükəsiz işləməsinə imkan yaradır.

Proqram təminatının təhlükəsizliyinin təmin edilməsi yalnız texniki məsələ deyil, həm də təşkilati və metodoloji yanaşmalar tələb edir. Bu sahədə proqramçılar, sistem administratorları və təhlükəsizlik mütəxəssisləri birgə fəaliyyət göstərməlidirlər. Təhlükəsizlik tədbirlərinin proqram təminatının hazırlanmasının ilkin mərhələlərindən tətbiq olunması daha effektiv nəticə verir.

Məqalədə, mövcud təhlükəsizlik problemləri, onların aradan qaldırılması üçün tətbiq olunan müasir yanaşmalar nəzərdən keçirilib. Bununla yanaşı, proqram təminatının təhlükəsizliyinin artırılması üçün istifadə olunan əsas metodlar və texnologiyalar da təqdim olunub.

Təhlükəsiz proqramlaşdırma prinsiplərinin tətbiqinin əhəmiyyəti araşdırılır. Bu prinsiplərin proqram təminatının hazırlanmasında rolu müəyyən edilir.

Tədqiqat nəticəsində proqram təminatında təhlükəsizlik səviyyəsinin artırılması üçün tövsiyələr təqdim edilir. Bu tövsiyələr

proqram təminatının daha etibarlı hazırlanmasına kömək edə bilər. Aparılan araşdırma proqram təminatının təhlükəsizliyinin təmin edilməsinin vacibliyini göstərir. Bu sahədə tətbiq olunan metodların inkişaf etdirilməsi müasir informasiya sistemlərinin qorunmasında mühüm rol oynayır.

İşin məqsədi

Bu tədqiqat işinin əsas məqsədi veb tətbiqlərdə və proqram təminatında mövcud olan təhlükəsizlik boşluqlarını araşdırmaq və onların qarşısının alınması metodlarını təhlil etməkdir. Bu problemlərin yaranma səbəblərinin araşdırılması da işin əsas məqsədlərindən biridir. Bu istiqamətdə müxtəlif müdafiə mexanizmləri analiz olunur. Müxtəlif təhlükəsizlik yanaşmalarının effektivliyi müqayisə edilir. Eyni zamanda, proqram təminatının təhlükəsizliyinin artırılması yolları araşdırılır.

Məsələnin qoyuluşu

Müasir informasiya sistemlərində təhlükəsizlik məsələləri xüsusi əhəmiyyət kəsb edir. Proqram təminatının geniş istifadə olunması təhlükəsizlik risklərinin də artmasına səbəb olmuşdur. Bu səbəbdən proqram təminatında mövcud olan zəifliklərin müəyyən edilməsi mühüm vəzifələrdən biridir. Bununla yanaşı, bu boşluqların sistemin etibarlılığına təsiri də araşdırılmalıdır.

Məsələnin həlli

İnformasiya sistemlərində təhlükəsizlik zəifliklərı məlumat sızması, icazəsiz giriş və sistemlərin fəaliyyətinin pozulması kimi ciddi problemlərə səbəb ola bilər. Bu səbəbdən proqram təminatının hazırlanması prosesində təhlükəsizlik mexanizmlərinin sistemli şəkildə tətbiqi vacib hesab olunur.

Təhlükəsizlik boşluqlarının aradan qaldırılması üçün çoxsəviyyəli təhlükəsizlik modelinin tətbiqi təklif olunur. Bu model tətbiq səviyyəsində təhlükəsizlik tədbirlərini, kriptoqrafik müdafiə mexanizmlərini və sistem monitorinqi metodlarını özündə birləşdirir. Bu yanaşma proqram təminatının müxtəlif səviyyələrində yaranan təhlükəsizlik risklərinin minimuma endirilməsinə imkan verir.

Təklif olunan model üç əsas mərhələdən ibarətdir:

1. Təhlükəsizlik zəifliklərinin müəyyən edilməsi
2. Kriptoqrafik qoruma mexanizmlərinin tətbiqi
3. Təhlükəsizlik monitorinqi və risklərin qiymətləndirilməsi

İlk mərhələdə, sistemdə mövcud olan təhlükəsizlik zəifliklərinin müəyyən edilir. Bu məqsədlə təhlükəsizlik analizləri və zəiflik skanerləri istifadə olunur. Aşkar edilmiş zəifliklərin sistemə təsir səviyyəsi risk analizi vasitəsilə qiymətləndirilir.

Risk səviyyəsinin hesablanması üçün aşağıdakı riyazi modeldən istifadə edilə bilər [2]:

$$R = P \times I \quad (1)$$

R – təhlükəsizlik riski,

P – hücumun baş vermə ehtimalı,

I – hücumun sistemə təsir səviyyəsidir.

Risklərin daha dəqiq qiymətləndirilməsi üçün genişləndirilmiş model tətbiq edilə bilər:

$$R = (P \times I) + E \quad (2)$$

E – zəifliyin istismar olunma ehtimalını göstərən əmsaldır.

Bu model təhlükəsizlik zəifliklərinin prioritetləşdirilməsinə imkan yaradır və daha

yüksək riskə malik zəifliklərin aradan qaldırılmasını prioritet edir.

Təhlükəsizlik modelinin ikinci mərhələsində kriptoqrafik metodlardan istifadə edilir. Kriptoqrafiya məlumatların məxfiliyinin və bütövlüyünün qorunmasında əsas rol oynayır. Məlumatların qorunması üçün simmetrik və asimmetrik şifrələmə metodlarından istifadə olunur.

Simmetrik şifrələmə modelini aşağıdakı düsturla ifadə etmək mümkündür:

$$C = E(K, M) \quad (3)$$

M – ilkin məlumat,
K – şifrələmə açarı,
C – şifrələnmiş məlumatdır.

Məlumatın deşifrələnməsi isə aşağıdakı şəkildə həyata keçirilir:

$$M = D(K, C) \quad (4)$$

burada **D** deşifrələmə funksiyasını göstərir.

Simmetrik kriptoqrafiyada geniş istifadə olunan alqoritmlərdən biri AES (Advanced Encryption Standart) alqoritmidir [3]. AES alqoritmi yüksək təhlükəsizlik səviyyəsinə malikdir və böyük həcmli məlumatların qorunmasında effektiv nəticə verir.

Asimmetrik kriptoqrafiyada isə iki fərqli açardan istifadə edilir. Bu model aşağıdakı şəkildə ifadə olunur:

$$C = E\left(K_{pub}, M\right) \quad (5)$$

$$M = D(K_{priv}, C) \quad (6)$$

$\boldsymbol{K_{pub}}$ – açıq açar,
$\boldsymbol{K_{priv}}$ – gizli açardır.

Asimmetrik kriptoqrafiyanın ən geniş yayılmış alqoritmlərindən biri RSA (Rivest-Shamir-Adleman) alqoritmidir. RSA alqoritmi böyük sadə ədədlərin faktorizasiyasının mürəkkəbliyinə əsaslanır [4].

RSA modelində açarların yaradılması aşağıdakı düsturlar vasitəsilə həyata keçirilir:

$$\mathrm{n} = \mathrm{p} \times \mathrm{q} \quad (7)$$

$$\phi(\mathrm{n}) = (\mathrm{p} - 1)(\mathrm{q} - 1) \quad (8)$$

Şifrələmə prosesi aşağıdakı kimi həyata keçirilir:

$$\mathrm{C} = M^e mod\ n \quad (9)$$

Deşifrələmə isə aşağıdakı düsturla ifadə olunur:

$$\mathrm{M} = C^d mod\ n \quad (10)$$

Məlumatların bütövlüyünün qorunması üçün hash funksiyalarından istifadə edilir. Hash funksiyası məlumatı sabit uzunluqlu rəqəmsal xülasəyə çevirir [5].

Hash funksiyası aşağıdakı kimi göstərilə bilər:

$$\mathrm{H} = \mathrm{hash}(\mathrm{M}) \quad (11)$$

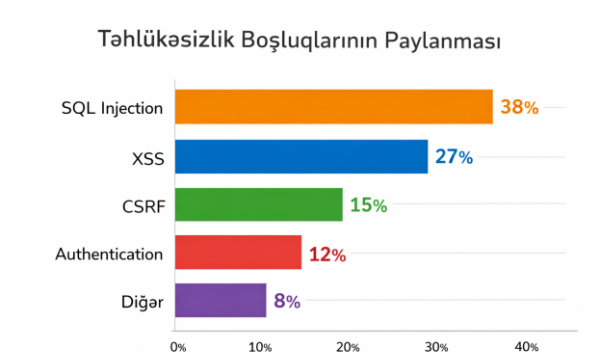
Hash funksiyaları məlumatın dəyişdirilib-dəyişdirilmədiyini müəyyən etməyə imkan verir. Bu metod autentifikasiya sistemlərində geniş istifadə olunur.

Təhlükəsizlik tədbirlərinin effektivliyini qiymətləndirmək üçün statistik analiz metodlarından istifadə edilir. Sistem daxilində aşkar edilən və aradan qaldırılan zəifliklərin sayı aşağıdakı göstərici ilə qiymətləndirilə bilər:

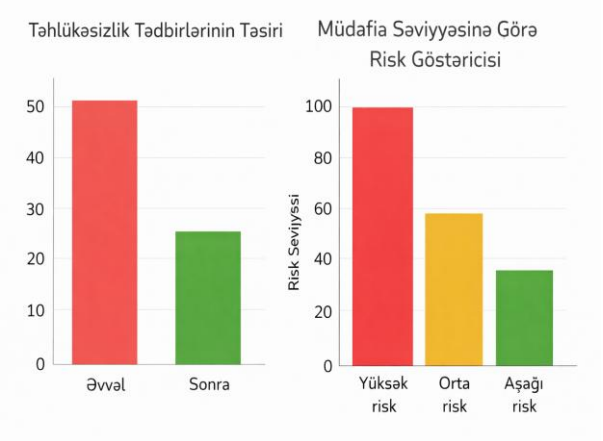
$$E = \frac{V_f}{V_t} \quad (12)$$

$\boldsymbol{V_f}$ – aradan qaldırılmış zəifliklərin sayı,
$\boldsymbol{V_t}$ – aşkar edilmiş ümumi zəifliklərin sayıdır.

Şəkil 1 təhlükəsizlik tədbirlərinin effektivliyini müəyyən etməyə imkan verir. Şəkil 2 təhlükəsizlik tədbirləri tətbiq olunmuş və olunmamış proqram təminatları arasındakı fərqləri göstərir.



Şəkil 1 – Veb tətbiqlərdə ən geniş yayılmış təhlükəsizlik boşluqlarının paylanması
Figure 1 – Distribution of the most common security vulnerabilities in web applications



Şəkil 2 – Təhlükəsizlik tədbirlərinin tətbiqindən əvvəl və sonra sistemdə aşkar edilən zəifliklərin sayı və risk səviyyəsinin müqayisəsi
Figure 2 – Comparison of the number of detected vulnerabilities and risk levels before and after the implementation of security mechanisms

Beləliklə, proqram təminatında təhlükəsizlik boşluqlarının aradan qaldırılması kompleks yanaşma tələb edir [6]. Təhlükəsiz proqramlaşdırma prinsiplərinin tətbiqi, kriptoqrafik metodlardan istifadə və mütəmadi təhlükəsizlik analizlərinin aparılması informasiya sistemlərinin təhlükəsizlik səviyyəsinin artırılmasına imkan verir. Bu metodların tətbiqi nəticəsində proqram təminatının etibarlılığı və davamlılığı əhəmiyyətli dərəcədə yüksəlir.

Nəticə

Aparılan tədqiqat nəticəsində proqram təminatında təhlükəsizlik boşluqlarının informasiya sistemləri üçün ciddi risklər yaratdığı müəyyən edilmişdir. Müasir veb tətbiqlərdə məlumatların qorunması üçün kompleks təhlükəsizlik yanaşmasının tətbiqi vacib hesab olunur. Təhlükəsizlik zəifliklərinin müəyyən edilməsi və risklərin qiymətləndirilməsi proqram təminatının təhlükəsizlik səviyyəsinin artırılmasında mühüm rol oynayır. Tədqiqat zamanı təhlükəsiz proqramlaşdırma prinsiplərinin tətbiqinin təhlükəsizlik boşluqlarının azalmasına müsbət təsir göstərdiyi müəyyən edilmişdir.

Kriptoqrafik metodların tətbiqi məlumatların məxfiliyinin və bütövlüyünün qorunmasında mühüm əhəmiyyətə malikdir. Simmetrik və asimmetrik şifrələmə metodları informasiya sistemlərində təhlükəsiz məlumat mübadiləsini təmin edir. Hash funksiyalarının istifadəsi məlumatların dəyişdirilib-dəyişdirilmədiyini müəyyən etməyə imkan verir. Təhlükəsizlik mexanizmlərinin tətbiqi nəticəsində sistemdə mövcud olan zəifliklərin sayı əhəmiyyətli dərəcədə azaldıla bilər.

Beləliklə, proqram təminatında təhlükəsizlik boşluqlarının aradan qaldırılması üçün çoxsəviyyəli müdafiə strategiyasının tətbiqi zəruridir. Təhlükəsiz proqramlaşdırma prinsipləri və kriptoqrafik metodların birgə tətbiqi informasiya sistemlərinin daha etibarlı və təhlükəsiz fəaliyyət göstərməsinə imkan yaradır.

Maraqlar münaqişəsi

Müəllif bu məqalədə araşdırılması tələb olunan maraqlar münaqişəsinin olmadığını qeyd edir.

REFERENCES

1. **OWASP Foundation,** Secure Coding Practices Quick Reference Guide, 2020, pp. 3–8.
2. **NIST,** Guide for Conducting Risk Assessments, NIST Special Publication 800-30, 2012, pp. 10–15.
3. **NIST,** Advanced Encryption Standard (AES), FIPS 197, 2001, pp. 1–10.
4. **Schneier, B.,** Applied Cryptography: Protocols, Algorithms and Source Code in C, Wiley, 1996, pp. 466–472.
5. **Stallings, W.,** Cryptography and Network Security: Principles and Practice, Pearson, 2017, pp. 350–360.
6. **Sadigov Ulfat.** Development and Preparation of Information Security Methods, Herald of the Azerbaijan Engineering Academy, 2026, ONLINE, pp. 1–13, https://doi.org/10.52171/herald.347