AZƏRBAYCAN RESPUBLİKASI
DÖVLƏT TƏHLÜKƏSİZLİYİ XİDMƏTİNİN
HEYDƏR ƏLİYEV ADINA AKADEMİYASI

# “Dövlət Təhlükəsizliyi Xidmətinin Heydər Əliyev adına Akademiyası Ulu Öndər irsinin daşıyıcısıdır” adlı respublika elmi-praktik konfransının

# MATERİALLARI

01-02 dekabr 2023-cü il

**Tamilla BAYRAMOVA**
**İnformasiya Texnologiyaları İnstitutu**
***e-mail:*** *tamilla@iit.science.az*

# PROQRAM SISTEMLƏRININ TƏHLÜKƏSIZLIK PROBLEMLƏRI HAQQINDA

**Xülasə**

Məqalədə kibercinayətkarların hədəfləri və kiberhücumların növləri təhlil edilmiş və son illərdə ən çox ziyan vuran kibercinayətkar qruplar haqda məlumat verilmişdir. Proqram təminatının boşluqlarını klassifikasiya etmək və qiymətləndirmək üçün müxtəlif təşkilatlar tərəfindən yaradılmış sistemlər göstərilmişdir. Proqram təminatında olan xətaların və boşluqların aradan qaldırılması üçün proqram kodunu analiz metodları haqda məlumat verilmişdir.

***Açar sözlər:*** *kiberhücum, boşluqların klassifikasiyası, statik analiz, dinamik analiz, intellektual analiz.*

## 1. Giriş

Sənaye 4.0 konsepsiyasına daxil olan texnologiyaların (kiber-fiziki sistemlər, əşyaların İnterneti, bulud hesablamaları, böyük verilənlər, robototexnika və s.) həyatımızın bütün sahələrinə nüfuz etməsi kibertəhlükəsizliklə bağlı yeni problemlərin yaranmasına səbəb olmuşdur. Süni intellektin həyatımıza nüfuz etməsi informasiya təhlükəsizliyinə tələbləri artırmışdır. İntellektual sənaye sistemlərinin inkişafı yeni təhlükəsizlik çağırışları yaratmışdır. Əsas dövlət qurumlarının kritik infrastrukturunu pozmaq və ya tamamilə dağıtmaq məqsədi daşıyan gizli hücumların sayı durmadan artır. Proqram təminatının xətası nəticəsində dəyən ziyanın qiyməti milyonlarla dollarla deyil, milyonlarla insan həyatı ilə, ekoloji problemlərlə, cəmiyyətdə sosial partlayışlarla ölçülə bilir.

Proqram təminatının mürəkkəbliyi getdikcə artır, proqram kodunun uzunluğu milyon sətirlərlə ölçülür. Bu qiymət 5 milyon sətrə yaxınlaşdıqda, proqram təminatında olan xətaların sayı kəskin şəkildə artmağa başlayır [1]. Veb-cinayətkarlar kiberhücumları həyata keçirmək üçün proqram təminatında olan xətalardan istifadə edirlər. IEEE 610.12-1990 standartına görə ***boşluq (vulnerability)*** veb-cinayətkarlar tərəfindən istifadə edilən proqram xətalarıdır. Proqram təminatında olan bütün xətalar boşluq deyil (məsələn, hesablama səhvləri). Əgər proqram təminatında olan xətadan istifadə edərək məhsulun tamlığı, əlyetərliliyi və məxfiliyi pozula bilərsə belə xətalar proqram boşluqları adlanır. **Sıfırıncı gün boşluğu** proqram təminatına hücum etməyə imkan verən və əvvəllər məlum olmayan proqram boşluğudur. Bədniyyətlilər təhlükəsizlik boşluqlarını aşkar etmək üçün ciddi səy göstərirlər. Təhlükəsizlik vasitələri əvvəlcədən məlum olan eksploytlara qarşı işləndiyindən sıfırıncı gün eksploytlarını aşkar edə bilmir, belə hücumlar bədniyyətlilərə böyük fayda verir, uzun müddət aşkar olunmadan qala bilir və hücumun müvəffəqiyyəti eksploytun aşkar edilməsi ilə onun düzəldilməsi arasındakı vaxtdan asılıdır. ***Boşluqların idarə edilməsi*** son nöqtələrdə, işçi stansiyalarda və proqram sistemlərində boşluqların müəyyən edilməsi, qiymətləndirilməsi, hesabatın hazırlanması, idarə edilməsi və aradan qaldırılması üçün davamlı, müntəzəm prosesdir [2]. Proqram boşluqlarının idarə edilməsi təhlükəsizlik mütəxəssislərinin əsas vəzifələridir.

## 2. Kibercinayətkarların hədəfləri və kiberhücumların növləri

*Kibercinayətkarlıq xərclərinə* məlumatların zədələnməsi və məhv edilməsi, oğurlanmış pul, məhsuldarlığın itirilməsi, əqli mülkiyyətin oğurlanması, şəxsi və maliyyə məlumatlarının oğurlanması, mənimsəmə, fırıldaqçılıq, hücumdan sonra biznes proseslərinin korlanması, məhkəmə araşdırmaları, sızdırılmış məlumatların bərpası və reputasiyaya vurulmuş ziyan daxildir [3]. Ekspertlər kibercinayətkarlığın qlobal dəyərinin 2025-ci ilə qədər 10,5 trilyon dollara çatacağını proqnozlaşdırırlar.

Kiberhücumlara ən həssas olan müəssisə və ya təşkilat növlərinə aşağıdakılar daxildir:

- ✓ **Banklar və maliyyə institutları:** kredit kartı məlumatlarını, bank hesabı məlumatlarını və müştəri və ya müştərinin şəxsi məlumatlarını ehtiva edir.

- ✓ **Səhiyyə:** Tibbi qeydlərin, klinik tədqiqat məlumatlarının və sosial təminat nömrələri, faktura məlumatları və sığorta iddiaları kimi xəstə qeydlərinin depoları.
- ✓ **Şirkətlər:** Məhsul anlayışları, əqli mülkiyyət, marketinq strategiyaları, müştəri və işçi verilənlər bazaları, müqavilə sövdələşmələri, müştəri təklifləri və s. kimi hərtərəfli məlumatları ehtiva edir.
- ✓ **Elmi müəssisələr:** Qeydiyyat məlumatları, akademik tədqiqatlar, maliyyə qeydləri və adlar, ünvanlar və faktura məlumatları kimi şəxsi məlumatlar haqqında məlumatı saxlayır.

Kiberhücumların aşağıdakı növləri məlumdur:

- **eCrime** - Maddi motivli cinayət müdaxiləsi;
- **Targeted** Kibercasusluq, hökumət əlaqələrini pozmaq üçün hücumlar və rejimi dəstəkləmək üçün hədəflənmiş dövlət tərəfindən dəstəklənən məqsədli hücumlar;
- **Hacktivist** bir səbəb və ya ideologiya üçün təcili görüntü yaratmaq və ya reklam qazanmaq üçün həyata keçirilən işğalçı fəaliyyətdir;
- **Unattributed** atributsuz.

Qabaqcıl Davamlı Təhdid *(Advanced Persistent Threat, APT)* yüksək səviyyəli biliyə və əhəmiyyətli resurslara malik olan, onları dəstəkləyən hökumətin məqsədlərinə çatmaq üçün çalışan konkret məqsədlərlə müəyyən əməliyyatlar aparan millətçi kibercinayətkar qruplardır.

Kibertəhlükəsizlik üzrə dünya liderlərindən olan CrowdStrike Holdings şirkətinin 2022-ci il üzrə hesabatında İT mühitində 2022-ci il üçün kibertəhlükəsizliyə olan əsas təhdidlərdən biri eCrime qrupundan olan *ransomware* hücumlarıdır. Ransomware hücumları verilənlərə əlyetərliliyi xüsusi şifrələmə nəticəsində bloklayır və həmin informasiyaya əlyetərliliyi bərpa etmək üçün bədniyyətlilələr müəyyən məbləğin ödənilməsini tələb edirlər. Kibercinayətkarlar informasiyanı bloklamaqla kifayətlənmirlər, həm də onu yayacaqları ilə təhdid edirlər [4].

Group-IB şirkətinin araşdırmalarına görə belə şifrələyici proqramların vurduğu ziyan ABŞ-da 1 mlrd. dolları keçmişdir. Bu hələ məlum olan ədəddir, real itkilər isə daha çoxdur, çünki bəzi şirkətlər kibercinayətkarlara pul ödədikdən sonra insident haqda heç yerə məlumat vermirlər [5].

Bu sahədə ən təhlükəli qruplar *Maze* (2020-ci ildən fəaliyyət göstərir) və *Revil* (müvəffəqiyyətli hücumların 50% bunların hesabındadır) hesab edilir. *Ryuk*, *NetWalker*, *DoppelPaymer* birləşmələri də ön sıralardadır. Bu qrupların son illərdə ən məşhur hücumları aşağıda verilmişdir:

- ✓ 2021-ci ildə REvil qruplaşması Apple şirkətinin yeni məhsulları haqda verilənləri oğurladığı haqda məlumat verdi və 50 milyon dollar tələb etdi.
- ✓ JBS ət emalı üzrə dünyada ən böyük şirkətdir. 2021-ci il 30 mayda ransomware hücumu ABŞ, Kanada və Avstraliyada bu şirkətin bütün zavodlarının işini dayandırdı. Nəticədə şirkət kibercinayətkarlara 11 milyon dollar ödədi.
- ✓ Robinhood ABŞ-da birja ticarət proqramıdır. 3 noyabr 2021-ci ildə kibercinayətkarlar 7 milyon istifadəçinin verilənlərini oğurladı və böyük məbləğdə pul tələb etdilər. Bu, 5 milyon istifadəçinin e-poçt ünvanlarının oğurlanması və daha 2 milyon istifadəçinin tam adının ifşa olunması ilə nəticələndi. 310 nəfərin isə əlavə şəxsi məlumatları oğurlandı. Robinhood pul ödəmədi, hücumun araşdırılması üçün kibertəhlükəsizlik üzrə şirkəti cəlb etdi.
- ✓ 16 sentyabr 2022-ci ildə Uber AWS şirkətinin bulud qeydiyyat verilənləri və Slack şirkətinin korporativ qeydiyyat verilənlərinə əlyetərlilik əldə etdilər. Cavab olaraq, Uber potensial təhlükə altında olan hesabları müəyyən etdi, onları blokladı, parolları sıfırladı. Onlar həmçinin daxili alətlərə girişi sıfırladılar və hər hansı yeni kod dəyişikliyinin qarşısını almaq üçün kod bazasını blokladılar. Hücumun vaxtında aşkar edilməsi nəticəsində müştəri kredit kartı detalları və bank hesabı məlumatları qorudular.
- ✓ 2022-ci il 4 avqustda Böyük Britaniya Milli Səhiyyə Xidmətinin (NHS) kibertəhlükəsizliyinin pozulması nəticəsində bir neçə xidmət dayandırıldı. Pasientlər haqda informasiya bloklandı, xəstəxanalar arasında elektron sənəd dövriyyəsi dayandırıldı. 22 avqustda problemlər aradan qaldırılmağa başlandı.

✓ *WannaCry* hücumunda Windows əməliyyat sistemində olan "EternalBlue" boşluğundan istifadə edilmişdi. "The Shadow Brokers" kimi tanınan haker qrupu hücumdan əvvəl problemi üzə çıxarmışdı. Microsoft, EternalBlue boşluğunu aradan qaldıran patç işlədi. Lakin xəbərdarlığa baxmadan bütün dünya üzrə müəssisələr və şəxslər kompüterlərinin təhlükədə olduğunu dərk etmədilər və sistemi yeniləmədilər. Nəticədə WannaCry dünya üzrə təxminən 4 milyard dollardan çox ziyan vurdu.

Dünya üzrə Ransomware proqramları tərəfindən 2021-ci ildə 623,3 milyon, 2022-ci ilin birinci yarısında 236,1 milyon hücum olmuşdur. Bu hücumların hamısı müvəffəqiyyətli olmasa da, bu ədədlər kiberhücumların geniş yayılmasını göstərir.

### 3. Proqram boşluqlarının klassifikasiyası

Proqram təminatında boşluqlar aşkar edilən kimi proqram təminatını işləyənlər onları aradan qaldırmaq üçün tədbirlər hazırlayır. Boşluqların kritikliyindən asılı olaraq, sistem administratoru hansı səhvləri ilk olaraq və nə qədər tez aradan qaldıracağına qərar verir. Buna görə də, proqram təminatının boşluqlarını klassifikasiya etmək və qiymətləndirmək üçün müxtəlif sistemlər hazırlanmışdır.

1) **CVE** *(Common Vulnerabilities and Exposures)* - proqram təminatında aşkar edilmiş səhvləri və boşluqları qeyd edən verilənlər bazasıdır. Burada əsas məqsəd bütün məlum səhvlərin və çatışmazlıqların identifikasiyasını standartlaşdırmaqdır. CVE formatı aşağıdakı kimidir [6]:

   **CVE- [il 4 simvol] - [növbəti identfikator]**

   Məsələn, CVE-2020-0168, 2020-ci ildə aşkar edilmiş 168-ci xəta deməkdir.
2) **CWE** *(Common Weakness Enumeration)* - bu, bədniyyətli hücumlar zamanı istifadə edilə bilən proqram təminatı boşluqlarının verilənlər bazasıdır [7].
3) **NDV** *(National Vulnerability Database)* – ABŞ hökumətinin SCAP protokolundan istifadə edərək təqdim edilmiş standart boşluqların idarə edilməsi üzrə məlumatları birləşdirən repozitaridir [8].
4) **CVSS** *(Common Vulnerability Scoring System)* - proqram təminatı boşluqlarının təhlükəsizlik reytinqini qiymətləndirmək üçün verilənlər bazasıdır. CVSS üç qrup göstəricidən ibarətdir: baza, müvəqqəti və ətraf mühitin qiymətləndirilməsi [9].
5) **CAPEC** *(Common Attack Pattern Enumeration and Classification)* – ən məşhur hücumların kataloqudur [10].
6) **MITER ATT & CK Matrix** *(Adversarial Tactics, Techniques & Common Knowledge)* - kiberhücumların həyata keçirilməsi üçün istifadə olunan taktika və texnologiyaların rəsmi təsvirini verən verilənlər bazasıdır [11].

Bu verilənlər bazalarına açıq girişin olmasına baxmayaraq, informasiya təhlükəsizliyi üzrə mütəxəssislər böyük həcmdə məlumatlarla işləyirlər. Məlumatların təhlili vaxt və peşəkar bacarıq tələb edir. Buna görə də, bu verilənlər bazalarında boşluqları müəyyən etmək üçün mətnlərin intellektual analizi metodlarının tətbiqinə maraq artır. Bu, mütəxəssislərə axtarışı avtomatlaşdırmağa və onlara lazım olan məlumatları təhlil etməyə kömək edə bilər.

### 4. Proqram təminatında olan xətaların və boşluqların aşkar edilməsi üçün təhlükəsizlik alətləri

*Analizatorlar* (skanerlər) müxtəlif məqsədlər üçün bədniyyətlilər tərəfindən istifadə edilə bilən boşluqları və səhvləri aşkar etmək üçün nəzərdə tutulmuş xüsusi proqramlardır. Boşluğun qiymətləndirilməsi alətləri obyektin həyat dövründə iki mərhələdə tətbiq edildikdə daha faydalı nəticə verir:

- Proqram təminatı tətbiq edilməzdən əvvəl;
- Tətbiq edildikdən sonra təkrarən.

Boşluqları aşkar etmək üçün müxtəlif analiz metodları mövcuddur [12, 13]:

✓ Statik analiz;
✓ Dinamik analiz;
✓ Ekspert analizi;
✓ İntellektual analiz.

*4.1. Statik analiz metodları*

Statik analiz təhlil edilən proqramın ilkin kodu üzərində onu icra etmədən həyata keçirilir. Bu metodlara daxildir:

- ***HP Fortify Static Code Analyzer (SCA)*** – statistik kod analizi üçün alətdir. Xətanın səbəbini tapır, nəticəni emal edir və koddakı xətanı aradan qaldırmaq üçün yolu göstərir.
- ***AppChecker*** – C/C++, C#, Java, PHP dillərində işlənmiş proqramların ilkin kodunda qüsurları və proqram xətalarını axtarmaq üçün nəzərdə tutulmuş statik kod analizatorudur. 100-dən çox kodlaşdırma qüsurunu axtarır, CWE təsnifatını dəstəkləyir.
- ***Checkmarx CxSAST*** – ilk növbədə adi proqram təminatının təhlili üçün nəzərdə tutulub, lakin PHP, Python, JavaScript, Perl və Ruby proqramlaşdırma dillərini dəstəklədiyinə görə veb-proqramların təhlili üçün də yaxşı vasitədir. Checkmarx CxSAST, xüsusi spesifikliyə malik olmayan universal analizatordur və buna görə də proqram məhsulunun həyat dövrünün istənilən mərhələsində - işlənmədən tətbiqə qədər istifadə üçün uyğundur, CWE bazasını dəstəkləyir.
- ***ITS4*** – potensial boşluqları aşkar etmək üçün ilkin kodun statik olaraq skan edən alətdir.
- ***RATS*** – Potensial təhlükəli funksiya çağırışlarını aşkar etmək üçün ilkin kodu skan edir.
- ***Pscan*** – Potensial olaraq düzgün istifadə edilməyən funksiyaları axtarmaq üçün C dilində yazılmış ilkin mətni skan edir və format sətirlərində boşluqları tapır.
- ***Сканер Nessus*** – informasiya sistemlərinin qorunması üçün məlum boşluqların avtomatik axtarışı üçün nəzərdə tutulmuşdur.
- ***Metasploit framework*** - şəbəkə və veb tətbiqlərdə boşluqları axtaran ən məşhur vasitələrdən biridir.
- ***Gamascan*** – veb tətbiqlər üçün skanerdir, proqramları və serverləri kiberhücumlardan qoruyur. Avtomatik olaraq veb tətbiqlərdə boşluqları axtarır və verilənlər bazasının təhlükəsizliyinin pozulmasını yoxlayır.
- ***Wapiti Wapiti*** – qara qutu skaneridir, ilkin kodu deyil veb-səhifəni skan edir. Əsas məqsədi veb tətbiqlərdə naməlum boşluqların axtarılmasıdır.

Digər statik analizatorlar: ***HP Fortify Static Code Analyzer***, ***IBM Security AppScan Source, Solar inCode, PT Application Inspector, InfoWatch Appercut, Digital Security ERPScan.***

*4.2. Dinamik analiz metodları:*

*Proqram kodunun dinamik analizi* icra üçün araşdırılan məhsulun mənbə koduna və işə salınma mühitinə əlyetərlilik olmadan proqramın təhlükəsizliyinin analizini aparır. Dinamik təhlilin üstünlüyü proqramın icrası zamanı yoxlanılması ilə bağlı heç bir fərziyyənin olmamasıdır [14].

- ***Valgrind*** – İcra edilən proqram kodunun dinamik analizi üçün nəzərdə tutulmuş pulsuz alətlər dəstidir.
- ***BOON*** –ilkin mətnin dərin semantik analizini aparır və buferin daşmasına səbəb ola biləcək boşluqların axtarılması prosesini avtomatlaşdırır.
- ***MOPS*** – Proqramın statik modelə uyğun olmasını təmin etmək üçün dinamik tənzimləmə üçün nəzərdə tutulmuşdur. Proqramın təhlükəsiz proqram təminatı yaratmaq üçün müəyyən edilmiş qaydalar toplusuna uyğun olub-olmadığını aydınlaşdırmaq üçün proqram yoxlama modelindən istifadə edir.
- ***Viva64*** – mütəxəssisə 32 bitlik sistemlərdən 64 bitlik sistemlərə keçidlə əlaqəli proqramların mənbə kodundakı potensial təhlükəli fraqmentləri izləməyə kömək edir. Analizator 64-bit sistemlər üçün düzgün və optimallaşdırılmış kodu yazmağa kömək edir.
- ***EXE*** – səhvlərin baş verdiyi giriş məlumatlarını avtomatik olaraq yaradan proqramlarda səhvləri tapmaq üçün alət.
- ***Flayer*** – proqramın binar kodunun dinamik təhlili üçün nəzərdə tutulmuşdur.
- ***IBM AppScan Standard*** – İşləyən proqram təminatında boşluqları tapmaqda ixtisaslaşmış mexanizmdir.
- ***Java ThreadSanitizer*** – ThreadSanitizer layihəsi tərəfindən yaradılmış, Java bayt kodunu dinamik şəkildə ölçmək üçün ASM freymvorkundan istifadə edir.

*4.3. Proqram kodunun ekspert analizi:*

Bu analiz metodları insan-ekspertlərin işinə əsaslanır. Onlar:

- Tədqiq olunan obyektin arxitekturunda potensial təhlükəli funksionallıq və boşluqların müəyyən etməyə yönəlmiş arxitekturun təhlilini aparırlar;
- Statik və dinamik analizin nəticələri əsasında qərar qəbul edirlər;
- Test nəticələrinə əsasən potensial boşluqları təsdiq edirlər.

*4.4. Proqram boşluqlarının intellektual analizi*

Yalnız insan-ekspertlərə əsaslanan boşluq şablonları vaxt aparır və səhvlərə meyillidir, bu da boşluqları aşkar etmək üçün intellektual metodların tətbiqini zəruri edir.

Maşın təlimi metodları proqram təminatında olan anomaliyaları təhlil edərək müxtəlif hücumları erkən mərhələdə aşkar etmək üçün istifadə edilə bilər. Proqram təminatında olan qüsurların və boşluqların proqnozlaşdırılması üçün neyron şəbəkələr, Support Vector Machine, Naïve Bayes, K-Nearest Neighbor, Random Forest, genetik alqoritmlər və s. metodlar tətbiq edilir. Hər bir metod müxtəlif proqnozlaşdırma və qiymətləndirmə qabiliyyətinə malikdir [15, 16].

Süni intellekt texnologiyalarının istifadəçilərin autentifikasiyası, davamlı olaraq şəbəkənin vəziyyəti haqda məlumatların alınması, təhlükəli hərəkətlərin monitorinqi və anomal trafikin identfikasiyası məsələlərində tətbiqi hücumların vaxtında aşkar edilməsinə kömək edir. Lakin bununla yanaşı, kibercinayətkarlar da həmin texnologiyalardan istifadə edərək müdafiə sistemlərindən qorunmağı bacaran "ağıllı" hücumlar təşkil edirlər.

İntellektual analiz alətləri: ***Fazzinq, DeepCode, Infer, Sapienz, SapFix, Embold, Source{d}, Clever-Commit, Commit Assistant, CodeGuru.***

Proqram kodunun düzgün analizini apardıqdan sonra hər bir qüsur haqqında hesabat hazırlanmalıdır. Hesabatda aşağıdakılar göstərilməlidir:

- Verilən qüsurun istifadə edilməsi nəticəsində bədniyyətlilərin yarada biləcəyi təhlükə haqqında tam məlumat verilməlidir
- Bu qüsurdan bədniyyətlilərin necə istifadə edə biləcəkləri barədə misal göstərməli və onların hansı peşəkarlığa malik olmaları təsvir edilməlidir;
- Verilən problemin həlli yolları və lazım olacaq xərclər haqqında məlumat verməlidirlər;
- Bu hesabat nəticəsində şirkət həmin proqram kodunun tətbiq edilməsi barədə qərar qəbul edilir;

**Nəticə**

Əgər boşluqların idarə edilməsi üzrə vasitələr boşluğu vaxtında aşkar etmirsə, bu vasitələr faydalı deyil. Şəbəkə skanerləri bu baxımdan öz aktuallığını itirmişdir. Təhdidlərə qarşı tədbirlərə aiddir:

- Şəbəkədə olan və olmayan bütün işçi stansiyalarda proqram boşluqlarının analizinin avtomatlaşdırılması;
- Boşluqlara və kibertəhdidlərə real zaman rejimində nəzarət etməklə aşkarlama müddətinin minimallaşdırılması;
- Eksploytların və təhdidlərin davamlı şəkildə analizi;
- Kritik proqram boşluqlarının təcili şəkildə aradan qaldırılması.

Proqram təminatındakı boşluqları aşkar edərək qaldıra bilən vahid metod və ya alət yoxdur. Bu sahədə süni intellekt texnologiyalarının tətbiqi ilə yeni metod və vasitələrin işlənməsi aktual problem olaraq qalır.

**İstifadə edilmiş ədəbiyyat**


1. Li G., Pattabiraman K., Hari S. K. S., Sullivan M., Tsai T., "Modeling Soft-Error Propagation in Programs," 2018 48th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), 2018, pp. 27-38, doi: 10.1109/DSN.2018.00016.
2. 610.12-1990 - IEEE Standard Glossary of Software Engineering Terminology. https://ieeexplore.ieee.org/document/159342
3. R. Sabillon, V. Cavaller, J. Cano and J. Serra-Ruiz, "Cybercriminals, cyberattacks and cybercrime," *2016 IEEE International Conference on Cybercrime and Computer Forensic (ICCCF)*, Vancouver, BC, Canada, 2016, pp. 1-9, doi: 10.1109/ICCCF.2016.7740434.
4. CrowdStrike 2023 Global Threat Report. https://www.crowdstrike.com/global-threat-report/

5. Group-IB. https://www.group-ib.com/blog/golddigger-fraud-matrix/
6. https://cve.mitre.org/
7. https://cwe.mitre.org/
8. https://nvd.nist.gov/
9. https://www.first.org/cvss/
10. https://capec.mitre.org/
11. https://bdu.fstec.ru/threat
12. Amankwah, Richard et al. "Evaluation of Software Vulnerability Detection Methods and Tools: A Review. International Journal of Computer Applications, 169, 2017, pp. 22-27.
13. Vieira M., Antunes N., Madeira H. Using web security scanners to detect vulnerabilities in web services, Dependable Systems & Networks, DSN'09. IEEE/IFIP International Conference on, 2009, pp. 566-571.
14. Вартанов С.П., Герасимов А.Ю. Динамический анализ программ с целью поиска ошибок и уязвимостей при помощи целенаправленной генерации входных данных. Труды Института системного программирования РАН. 2014;26(1):375-394. https://doi.org/10.15514/ISPRAS-2014-26(1)-15
15. Lin G., Wen S., Han Q. -L., Zhang J., Xiang Y., Software Vulnerability Detection Using Deep Neural Networks: A Survey, in Proceedings of the IEEE, vol. 108, no. 10, 2020, pp. 1825-1848.
16. Munea T. L., Lim H., Shon T. Network protocol fuzz testing for information systems and applications: a survey and taxonomy, Multimedia Tools and Applications, vol. 75,, 2016, pp. 14745-14757.

**Тамилла БАЙРАМОВА**

## О ПРОБЛЕМАХ БЕЗОПАСНОСТИ ПРОГРАММНЫХ СИСТЕМ

**Резюме**

В статье анализируются цели киберпреступников и виды кибератак, а также приводятся сведения о группах киберпреступников, нанесших наибольший ущерб за последние годы. Приведен обзор систем, разработанных различными организациями для классификации и оценки уязвимостей программного обеспечения. Дана информация о методах анализа программного кода для устранения уязвимостей в программном обеспечении.

***Ключевые слова:*** *кибератака, классификация уязвимостей, статический анализ, динамический анализ, интеллектуальный анализ.*

**Tamilla BAYRAMOVA**

## ABOUT SECURITY PROBLEMS OF SOFTWARE SYSTEMS

**Summary**

The article analyzes the goals of cybercriminals and types of cyberattacks, and also provides information about the groups of cybercriminals that have caused the greatest damage in recent years. An overview of systems developed by various organizations for classifying and assessing software vulnerabilities is provided. Information is provided on methods for analyzing program code to eliminate vulnerabilities in software.

***Keywords:*** *cyber attack, vulnerability classification, static analysis, dynamic analysis, intellectual analysis.*