İnformasiya Təhlükəsizliyi üçün Açıq Kodlu Alətlər

Yadigar İmamverdiyev
AMEA İnformasiya Texnologiyaları İnstitutu, Bakı, Azərbaycan
yadigar@lan.ab.az

***Xülasə*— Hazırda açıq kodlu proqram təminatı informasiya texnologiyalarına böyük təsir göstərir, bir sıra yeni sahələrin meydana çıxmasına imkan verir. İnformasiya təhlükəsizliyinin bir çox istiqaməti üzrə kommersiya analoqları ilə rəqabət apara bilən yüksək keyfiyyətli açıq kodlu proqram sistemləri mövcuddur. Bu məqalədə azad proqram təminatının əsas konsepsiyalarına nəzər salınır, informasiya təhlükəsizliyi üzrə açıq kodlu alətlər analiz edilir və onların tətbiqi üzrə bir sıra tövsiyələr işlənir.**

Açar sözlər*— *informasiya təhlükəsizliyi, azad proqram təminatı, açıq mənbə, açıq kodlu proqram təminatı, GPL lisenziyası

I. GİRİŞ

Açıq kodlu proqram təminatı (AKPT) azad paylaşılan proqram kodundan və İnternetin kommunikasiya vasitələrindən istifadə etməklə əməkdaşlıq şəraitində işləyən proqramçılar tərəfindən yaradılan proqram təminatıdır. Belə proqram təminatı istifadəçilərə daha yüksək keyfiyyət, etibarlılıq, çeviklik və aşağı qiymət vəd edir. Bu xüsusiyyətlərinə görə hazırda AKPT geniş istifadə edilir. Müasir veb-serverlərin böyük hissəsi açıq kodlu komponentlərdən təşkil olunmuş LAMP (Linux, Apache, MySQL, PHP) stekinə əsaslanır. Dünyada şirkətlərin 78 %-i bu və ya digər dərəcədə AKPT-dən istifadə edir, şirkətlərin yalnız 3 %-i istifadə etmir və heç bir halda etməyi planlaşdırmır [1]. Bir sıra ölkələrdə dövlət təşkilatlarının açıq kodlu əməliyyat sistemlərindən istifadə etməsi məcburidir (məsələn, GosLinux).

2009-cu ildə ABŞ Müdafiə Nazirliyinin nəşr etdiyi açıq kodlu proqram təminatının istifadəsinə dair Memorandumda bəyan edilir ki, bu növ proqram təminatı nazirlik üçün daha məqbuldur, çünki o meydana çıxan yeni təhdidlər və daim dəyişən tələblər baxımından proqram təminatını daha çevik modifikasiya etməyə və uyğunlaşdırmağa imkan verir [2,3].

Hazırda açıq mənbəli və kommersiya proqram təminatları haqqında ayrılıqda danışmaq mümkün deyil. Açıq mənbəli və proprietar proqram təminatı bir-birinə zidd görünsə də, müasir proprietar tətbiqi proqramların əksəriyyəti digər istehsalçıların proqram təminatı komponentlərindən yığılır ki, onların da bir çoxu açıq kodlu komponentlərdir [4].

İnformasiya təhlükəsizliyi sahəsində də kommersiya məhsulları ilə rəqabət apara bilən kifayət qədər açıq kodlu məhsullar mövcuddur. Bu işdə informasiya təhlükəsizliyi üzrə açıq kodlu alətlər analiz edilir və onların tətbiqi üzrə bəzi tövsiyələr verilir.

II. AÇIQ KODLU PROQRAM TƏMİNATININ QISA TARİXİ

Açıq kodlu proqram təminatının tarixi 1950-ci illərdən başlayır. IBM 704 kütləvi istehsal olunmuş ilk kompüter kimi 1954-cü ildə bazara çıxarılmışdı. IBM bu kompüterləri açıq kodlu pulsuz proqram təminatı ilə təchiz edirdi. 1955-ci ildə proqram kodunu paylaşmaq üçün SHARE təşkilatı da yaradılmışdı (indiyədək mövcuddur). 1969-cu ildə Ədliyyə Nazirliyi İBM-ə qarşı kompüter bazarında inhisarçılıq iddiasını qaldırmışdı. Məhkəmə araşdırması 13 il sürsə də, onun təsiri dərhal hiss olundu − IBM proqram təminatının kompüterlərlə birgə verilməsini dayandırdı. UNIX əməliyyat sistemi 1960-cı illərdə Bell Labs-da (həmin vaxt AT&T-nin hissəsi idi) Multics kimi yaradılmağa başlamışdı və 1972-ci ildə assemlerdən C-yə keçirildikdən sonra böyük populyarlıq qazandı. UNIX universitetlərə və təhsil institutlarına pulsuz lisenziya ilə verilməyə başlandı, ilk BSD (Berkley Software Distribution) lisenziyası Berkli Universiteti tərəfindən 1984-cü ildə verilmişdi.

AT&T-yə hələ 1950-ci illərə gedən anti-inhisar işinə görə kompüter və proqram təminatı satmaq qadağan edilmişdi. 1984-cü ildə AT&T regional bölmələrə parçalandı və ona kompüter və proqram təminatı satmaq icazəsi verildi. AT&T UNIX distributivini yaymağa başladı və 1990-cı illərdə Berkli Universiteti ilə lisenziya çəkişmələrinə başladı.

1970-ci illərin sonlarına doğru fərdi kompüterlər meydana çıxdı, kompüterlər ucuzlaşdı, onların sayı çoxaldı və kompüter istehsalçıları proqram təminatına öz intellektual mülkiyyəti kimi baxmağa başladılar və onun istifadəsi imkanını məhdudlaşdırdılar. 1983-cü ildə Massaçusets Texnologiya İnstitutunda Riçard Stollman tərəfindən *free software* (azad proqram təminatı, burada *free* sözü ingiliscə *freedom* sözündəki mənada işlədilir) konsepsiyası yaradıldı. Azad proqram təminatı fəlsəfəsinin əsas tezislərini belə ifadə etmək olar – Yaradıcılığın zəruri şərti azadlıqdır. İdeyalar azad yaradıcılıqda doğulur. Azad proqram təminatı aşağıdakı dörd azadlığı təmin edir [5]:

1. Proqramı istənilən məqsədlə istifadə etmək azadlığı;
2. Proqramın iş prinsiplərini öyrənmək və öz ehtiyacları üçün proqramda dəyişiklik etmək azadlığı;
3. Proqramın nüsxələrini istədiyi şəxsə vermək azadlığı;
4. Proqramı təkmilləşdirmək və bütün cəmiyyətin rifahı naminə bunu hamıya əlyetər etmək azadlığı.

Beləliklə, azad proqram təminatının istifadəsinə, dəyişiklik edilməsinə və yayılmasına heç bir məhdudiyyət qoyulmur. Yeganə tələb ondan ibarətdir ki, bütün dəyişikliklər aydın qeyd

DOI: 10.25045/NCSoftEng.2017.08

olunsun, müəllifin adı və müəlliflik hüququ haqqında məlumatlar heç bir halda silinməsin və ya dəyişdirilməsin [6].

1984-cü ildə Stollman GNU (GNU is Not Unix – "GNU Unix deyil" rekursiv akronimdir) azad əməliyyat sistemi layihəsini elan etdi və 1985-ci ildə azad proqram təminatı fondunu (Free Software Foundation, FSF) yaratdı [6]. 1990-cı illərin əvvəlində GNU layihəsi ƏS nüvəsi istisna olmaqla reallaşdırıldı. 1991-ci ildə Linus Torvalds qeyri-kommersiya lisenziyası ilə Linux nüvəsini yazdı. Bu sistemi GNU/Linux adlandırmaq daha doğru olardı, lakin Linux adı daha geniş yayıldı.

Azad proqram təminatı da lisenziya anlaşması ilə qorunur. Lisenziya – istifadəçi ilə proqram təminatını yayan tərəf arasında bağlanmış müqavilədir. Azad proqram təminatı üçün ilk lisenziya olan General Public License (GPL) 1988-ci ildə işlənmişdi. GPL lisenziyası ilə müəllif öz proqram təminatını ictimai mülkiyyətə verir. FSF fondu "copyright"-a analoji olaraq "copyleft" müəlliflik hüququ növü daxil etmişdi. Əsas məqsəd proqram kodunun dəyişdirilməsinə icazə verməyən müəlliflik hüququnun azad proqram təminatına tətbiqinin qarşısını almaqdır.

GNU layihəsi və İnternet azad proqram təminatı hərəkatının inkişafına şərait yaratdı. 1998-ci ildə Erik Reymond və Bryus Perens "açıq mənbə proqram təminatı" (ingiliscə *open source software*) terminini təklif etdilər. Onlar iddia edirdilər ki, *free software* termini ingilis dilində birmənalı deyil (free – *pulsuz* mənasını da verir) və kommersiya qurumlarını çəkindirə bilər. Onlar açıq kodlu layihələrə könüllülərin cəlb edilməsi prinsiplərini də işləyib hazırlamışdılar. 1998-ci ildə Microsoft Internet Explorer ilə rəqabət və mənfəətin azalması səbəbindən Netscape Communicator-un ilkin kodlarının nəşr olunması qərara alındı, AKPT layihələrinə dəstək üçün Open Source Initiative (OSI) təşkilatı yaradıldı.

Açıq mənbənin ilk 4 prinsipi – azad yenidən paylaşım, açıq kod, törəmə işlər, müəlliflərin açıq kodunun tamlığıdır. 5-10-cu prinsiplər isə ayrı-seçkiliyin olmaması və lisenziya məsələlərini əhatə edir.

"Açıq mənbə proqram təminatı" termininin tərifi "azad proqram təminatı"nın tərifi ilə üst-üstə düşmür, lakin mənaca yaxındırlar. Açıq kodlu proqramların böyük əksəriyyəti həm də azad proqram təminatıdır. Proqramlar, layihələr və lisenziyalar praktiki olaraq eynidir. Bir çox proqram təminatı layihəsi hər iki qrupla qarşılıqlı əlaqə saxlayır.

Açıq mənbə hərəkatı ilə və Microsoft-un qarşılıqlı münasibətlərinin tarixi olduqca maraqlıdır. 2000-ci illərin başlanğıcında onlar arasındakı rəqabət mübarizəsi açıq qarşıdurmaya keçmişdi. Microsoft idarəçiləri açıq mənbə hərəkatını "copyright xərçəngi", "kommunizm", "milli təhlükəsizliyə təhdid" adlandırırdılar. Lakin 2008-ci ildə birgə yaşayış mühiti bərqərar oldu [5], həmin vaxtdan Microsoft bir sıra məhsullarının kodlarını istifadəçilərə açmışdır.

Hazırda açıq mənbə termini təkcə proqram təminatı üçün işlədilmir, bir çox sahəyə tətbiq edilir. Hazırda azad proqram təminatı hərəkatına ictimai hərəkat, paradiqma, həyat tərzi kimi, açıq mənbə yanaşmasına isə – proqram təminatının yaradılması metodologiyası kimi baxılır.

III. AÇIQ KODLU PROQRAM TƏMİNATI LAYİHƏLƏRİ VƏ LİSENZİYA NÖVLƏRİ

Uğurlu açıq kodlu proqram təminatı layihələri olduqca çoxdur, informasiya texnologiyalarının istənilən sahəsi üzrə belə layihələr vardır. Linux bazasında əməliyyat sistemləri, veb-server platforması (Apache), ofis proqramları paketi (OpenOffice), verilənləriin idarə edilməsi sistemləri (MySQL) açıq mənbə layihələri daha çox məşhurdur. Qeyd etmək lazımdır ki, Big Data alətləri açıq kodlu proqram təminatı layihələri kimi Apache Software Foundation çərçivəsində gerçəkləşdirilir. Açıq kodlu bulud platformasına OpenStack nümunə göstərilə bilər.

Açıq kodlu layihə repozitarilərindən GitHub, SourceForge, Apache Software Foundation (ASF) və CodePlex daha çox tanınır. Microsoft-un GitHub-dakı hesabına daxil olub onun paylaşdığı bir çox açıq proqram kodları barədə məlumat əldə etmək olar.

Google özünün bütün açıq mənbə layihələrini bir sayda toplamışdır (https://opensource.google.com/). Saytda Google tərəfindən dəstəklənən 2000-dən çox layihə barəsində ətraflı məlumat almaq olar.

Açıq mənbə əsasında biznes modelləri SaaS (Sofware as a Service), xidmət/dəstək, məxsusi tələblərə uyğunlaşdırılmış həllərdir [7].

Matthias Stürmer açıq kod icmalarının dörd təşkilati strukturunu müəyyən edir [8]:

1. Vahid kuratorlu layihələr (single-vendor projects);
2. Proqramçılar qrupu (development communities);
3. İstifadəçilər qrupu (user communities);
4. Qarşılıqlı əlaqə mərkəzi (open source competence centers).

Vahid kuratorlu layihələr konkret kommersiya təşkilatının maliyyə dəstəyi ilə xarakterizə olunur. Bu təşkilat layihənin inkişaf istiqamətinə nəzarət edir. Belə icmalara misal kimi Wordpress və Automattic; Hadoop və Cloudera; Elasticsearch və Elastic göstərilə bilər.

Açıq kod icmalarının yuxarıda sadalanmış digər üç təşkilati strukturu isə proqram təminatının paylanmış işlənməsi prosesi ilə əlaqədardır. Bəzi hallarda bu proses icmanın bazasında meydana çıxan qeyri-kommersiya təşkilatları tərəfindən koordinasiya edilir. Lakin bu tip icmalarda vahid maliyyələşdirmə mənbəyi yoxdur. Belə icmalara misal kimi Apache, Rails və Linux göstərilə bilər.

Açıq kodlu proqram təminatı o demək deyil ki, onda ümumiyyətlə heç bir məhdudiyyət yoxdur. Müəllif hüquqları ilə bağlı məhdudiyyətlər lisenziyalarda ifadə edilir.

Populyar lisenziya ailələri MIT, GPL, BSD, Apache və LGPL-dir. Apache, MIT və BSD akademik və ya icazəverici lisenziyalar qrupuna aid edilir. GPL və LGPL isə uyğun olaraq güclü və zəif copyleft lisenziyalar qrupuna aiddir [9].

GPL açıq kodlu komponentlərlə bağlı kitabxanaların qarışığına yol vermir, bu bəzi hallarda mürəkkəb proqram sistemlərinin və komplekslərinin GPL ilə yayılmasını

DOI: 10.25045/NCSoftEng.2017.08

mümkünsüz edir. Buna görə güzəşt kimi GNU Lesser General Public License (LGPL) təklif edilmişdir.

IV. İNFORMASİYA TƏHLÜKƏSİZLİYİ ÜÇÜN AÇIQ KODLU PROQRAM TƏMİNATI

İnformasiya təhlükəsizliyinin istənilən istiqaməti üzrə bir çox açıq kodlu alətlər mövcuddur [10]. Onlardan bəziləri haqqında məlumat cədvəl 1-də verilir.

CƏDVƏL I. AÇIQ KODLU ALƏTLƏR

İnformasiya təhlükəsizliyi vasitələri	**Açıq kodlu alətlər**
Antivirus	ClamAV, Immune
Antispam	ASSP, SpamAssassin, SpamBayes, MailScanner
Host IDS	OSSEC
Şəbəkə IDS	Snort, Bro, Suricata
Parolların idarə edilməsi	PasswordMaker, KeePassX, KeePass Password Safe
Şəbəkə monitorinqi	Wireshark, tcpdump, Security Onion
Şəbəkələrarası ekran	IOS Firewall, iptables, Endian, Untangle, ClearOS, NetCop, IPCop, Devil-Linux, Shorewall, Turtle Firewall, Vuurmuur
İnsidentlərin təhqiqatı	ODESSA, The Sleuth Kit/Autopsy Browser, Cuckoo Sandbox, GRR, Maltego
İnsidentlərin idarə edilməsi	MozDef
Təhlükəsizlik skanerləri	OpenVAS, Nessus, Nmap, Metasploit, Nikto, Brakeman
SIEM	OSSIM, OpenSOC
Şifrləmə	AxCrypt, TrueCrypt, Gnu Privacy Guard, NeoCrypt
Naqilsiz şəbəkələr	Kismet Wireless, Airsnort, and Netstumber.
Trekinq və verilənlərin analizi	Swatch, ACID, NCC
Sızma testləri	Kali Linux

İnformasiya təhlükəsizliyi sahəsində açıq kodlu həllərin əksəriyyətinin ümumi cəhəti ondadır ki, onların quraşdırılması, sazlanması və istifadəsi xüsusi səriştə tələb edir. Bunlar sadə istifadəçilər üçün deyil, səriştəli administratorlar və inteqratorlar üçün nəzərdə tutulmuş məhsullardır.

Bəzi hallarda açıq kodlu alətlər bazarın lideri mövqeyini tuturlar. Məsələn, Snort – şəbəkə müdaxilələrinin aşkarlanması sistemləri (Intrusion Detection System, IDS) sahəsində de-fakto standart hesab olunur. Snort-un hücum siqnaturalarının təsviri dili də de-fakto standartdır. Paket 1998-ci ildə Martin Raş tərəfindən yaradılmışdır, hazırda onun inkişafı ilə Sourcefire şirkəti məşğul olur. Snort IP-şəbəkələrdə trafiki real zaman rejimində analiz etməyə və arxivləşdirməyə, icazəsiz girişləri operativ aşkarlamağa imkan verir. Snort həm UNIX-, həm də Windows-sistemlərdə quraşdırıla bilər. Snort əsasında bir çox kommersiya sistemləri yaradılmışdır.

İnformasiya təhlükəsizliyi üzrə açıq kodlu həllərin daha bir cəhəti onların ikili təyinatlı alətlər olmasıdır. Onları həm də haker alətləri kimi istifadə etmək olar. Kali Linux – sızma testlərinin aparılması – veb-tətbiqlərin analizi, şəbəkələrin və servislərin sındırılması, sistemdə möhkəmlənmək üçün nəzərdə tutulmuş utilitlər toplusundan ibarət olan distributivdir. Bu distributiv əvvəllər Backtrack adı ilə tanınırdı.

Biznes üçün AKPT-nın üstünlüyü təkcə vəsaitə qənaətdə deyil, həm də inhisarçıdan – proprietar proqram təminatı istehsalçısından asılılığın aradan qaldırılmasındadır. AKPT sahəsində biznesin qarşılaşdığı əsas problem bu sahə üzrə mütəxəssislərin çatışmazlığıdır. Bu problemin həllərindən birini yeni informasiya texnologiyaları təklif edir – virtuallaşma, bulud texnologiyaları, proqram təminatı xidmətləri (SaaS). Onlar proqram təminatının dəstəklənməsini İT-departamentlərdən İT-xidmət provayderlərinə köçürməyə imkan verir. Lakin informasiya təhlükəsizliyi tələblərində informasiyanın yalnız müəssisənin İT mütəxəssisləri tərəfindən idarə edilməsi məhdudiyyəti ola bilər. Bu bizi yenidən AKPT sahəsində ixtisaslaşmış mütəxəssislərin hazırlanması məsələsinə qaytarır.

Bulud texnologiyaları əsasında informasiya təhlükəsizliyi üzrə autsorsinq xidmətləri (Security-as-a-Service, SecaaS) bazarı da inkişaf edir. Məsələn, Splunk şirkəti loq-faylların analizi üçün bulud xidmətləri təklif edir (bu şirkəti "loq-fayllar üzrə Google" adlandırırlar) [11].

V. AÇIQ KODLU PROQRAM TƏMİNATININ TƏHLÜKƏSİZLİYİ

Açıq mənbənin üstünlüklərindən biri "çoxlu göz" prinsipi hesab olunur. Güman edilir ki, ilkin kod açıq olduğundan, onu çox sayda istifadəçi analiz edəcək [12].

Lakin ilkin kodun əlyetər olması onun analiz ediləcəyinə zəmanət vermir. Məsələn, açıq kodlu şəbəkə ekranı İnternetdə yerləşdirildikdən bir müddət sonra bu alətdən istifadə edən təxminən 2 000 sayt vardı, bununla belə, cəmisi 10 nəfər əlaqə saxlayaraq nöqsanlar və boşluqlar barədə fikir bildirmişdi [12]. Kodu analiz edən çox sayda "gözün" olması istifadəçilərdə yanlış təhlükəsizlik təsəvvürü yarada bilər. Eyni zamanda, çox "gözün" olması təhlükəsizlik boşluqlarının tapılıb aradan qaldırılmasına da zəmanət vermir [13]. Bunu çoxsaylı hadisələr sübut edir.

2014-cü ildə açıq kodlu layihələrdə bütün dünyada milyonlarla istifadəçini narahat edən bir neçə kritik boşluq açıqlanmışdı. Məsələn, OpenSSL kitabxanasında aşkarlanmış uzaqdan istismar edilə bilən Heartbleed, FREAK, POODLE və BEAST çox ciddi boşluqlar idi. Bu hadisələr istifadəçiləri AKPT-nin təhlükəsizliyi barədə daha ciddi düşünməyə vadar etdi [14]. Lakin Heartbleed açıq kodlu sistemlərdə aşkarlanmış ilk ciddi defekt deyildi. Məsələn, Apache Struts boşluğu ondan təxminən bir il əvvəl aşkarlanmışdı və ondan daha ciddi idi. Xatırlatmaq yerinə düşər ki, açıq kodlu proqram təminatında (sendmail və finger) olan boşluqlar 1988-ci ildə o vaxtkı İnternet-in işini bir neçə günlüyə iflic edən Morris soxulcanının yazılmasında istifadə edilmişdi.

Açıq kodlu mənbələrə əsaslanan texnologiya vendorları OpenSSL layihəsində nizam-intizam yaratmağa cəhd etdilər. Məlum olmuşdu ki, bu layihə könüllü ianələr şəklində daxil olan cəmi bir neçə min dollara natamam iş günü işləyən «iki Stiv» tərəfindən dəstəklənir. OpenSSL layihəsini dəstəkləmək üçün Amazon, Adobe, Cisco, Facebook və Google kimi nəhənglər tərəfindən xeyli maliyyə dəstəyi ayrıldı [15].

Linux-un kommersiya versiyalarını buraxan şirkətlər (Canonical, Red Hat) açıq kodlu proqram təminatının təhlükəsizliyinə xeyli vəsait yönəldirlər. Netflix və Facebook kimi şirkətlər AKPT-nın keyfiyyətini yüksəldən layihələrə xeyli resurslar yönəldirlər [15].

DOI: 10.25045/NCSoftEng.2017.08

Analizlər göstərir ki, dünyada şirkətlərin 67 %-i açıq kodlu proqram təminatında boşluqları analiz etmir [1]. Bundan başqa, açıq kodlu komponentlərdə olan məlum boşluqların yalnız 41 %-i aradan qaldırılır və onların aradan qaldırılması müddəti təxminən 390 gündür.

Beləliklə, AKPT-nin təhlükəsizliyinə daha ciddi, sistematik yanaşma tələb edilir. Proqram təminatı istehsalında da digər istehsal sahələrində istifadə edilən yüksək keyfiyyət və məsuliyyət təmin edən təchizat zənciri sistemini yaratmaq lazımdır. Bu zəncirdə istehsalçı son məhsula daxil olan hər bir hissənin mənşəyini bilir, problemlərin kökünü konkret təchizatçıya, avadanlığa və hətta istehsal proseslərinə kimi izləmək imkanına malikdir.

Lakin müasir proqram təminatı istehsalçılarında oxşar sistem yoxdur. Demək olar ki, hər bir kommersiya proqram təminatı AKPT və patentli komponentlərdən istifadə etməyə imkan verir, lakin proqram təminatı istehsalçıları bu kodların keyfiyyəti və mənşəyi haqqında səthi məlumatlara malik ola bilərlər. Çox zaman boşluğun mövcudluğu və təsir miqyası yalnız bu problemlər meydana çıxdıqdan sonra məlum olur.

Açıq kodlu proqram təminatından istifadə edilməsi zamanı aşağıdakıların nəzərə alınması tövsiyə olunur.

Təşkilatda açıq kodlu proqram təminatından istifadə siyasətinin, belə proqramların seçilməsi və qiymətləndirilməsi siyasətinin işlənməsi vacibdir. Daha az kritik olan funksiyalardan başlamaq tövsiyə olunur. Qiymətləndirmə, yükləmə, tətbiq və yeniləmə üçün kimin məsuliyyət daşıması müəyyən edilməlidir. Həmçinin seçilmiş proqram təminatının istifadəsi üzrə statistik məlumatların əldə edilməsi də vacibdir.

Açıq kodlu proqram təminatının etibarlı İnternet mənbələrindən yüklənməsi siyasəti işlənməlidir. Əgər binar fayllar yüklənirsə, onların nəzarət cəmləri yoxlanmalıdır. Nəzərə almaq lazımdır ki, proqram təminatının paylaşılması ilə məşğul olan serverlərə dəfələrlə hücumlar olub və bu zaman ilkin kodlar deyil, nəzarət cəmləri dəyişdirilib.

Yenilənmələr – AKPT-nın yüklənməsi ilə bağlı yuxarıda qeyd olunanlar burada da təkrarlanır. HTTP serverlər altında bədniyyətli mənbələr də gizlənə bilər. Hər bir yenilənmədən əvvəl və sonra təhlükəsizlik qiymətləndirməsi yerinə yetirilməlidir.

AKPT-nin auditi periodik aparılmalıdır. İlkin kod əlyetər olduğundan bədniyyətlilər boşluqları daha asan tapa bilərlər.

Boşluqların istismarı – bir çox AKPT layihələrində kodda olan səhvləri izləyən ayrı-ayrı şəxslər və hətta qruplar vardır, bu bədniyyətlilərin diqqətini köhnəlmiş boşluqlara cəlb edə bilər. Potensial boşluqlar barədə açıqlanan məlumatlar boşluqları istismar edən proqramların (eksploytların) yaradılmasını da xeyli asanlaşdıra bilər.

Açıq kodun lisenziya şəffaflığı – AKPT lisenziya hüquqlarının pozulmadığına əmin olmaq lazımdır [9].

AKPT-nın təhlükəsizlik səviyyəsini bəzən dolayı əlamətlərlə də müəyyənləşdirmək olar. Məsələn, seçilmiş AKPT-nı dəstəkləmə qrupunun, forumların, saytların mövcudluğu, onların yenilənməsi periodikliyi, gələcək inkişaf planları və s. informasiya təhlükəsizliyinin səviyyəsi barədə müəyyən informasiya verə bilər.

Yuxarıda deyilənlərlə yanaşı, mütləq qeyd etmək lazımdır ki, AKPT-nin proprietar proqram təminatından daha təhlükəsiz olduğunu və ya bunun əksini iddia etmək üçün heç bir obyektiv əsas yoxdur.

NƏTİCƏ

Açıq kodlu proqram təminatını tətbiq edərkən onunla bağlı riskləri diqqətlə qiymətləndirmək lazımdır. Korporativ mühitdə AKPT-nin tətbiqi bir sıra problemlərlə müşaiyət edilir. Bəzən AKPT-nin müşaiyət səviyyəsi, funksional imkanları kommersiya analoqları ilə rəqabət apara bilmir. Arxitekturanın dəyişilməsi xərcləri, dəstək qrupunun kvalifikasiyası olduqca yüksəkdir. AKPT istehsalçıları adətən, pulsuz dəstək və əməkdaşların təlimi xidmətlərini təklif etmirlər.

ƏDƏBİYYAT

[1] Black Duck Software, and North Bridge, The Ninth Annual Future of Open Source Survey. 2015. https://www.blackducksoftware.com/futureof-open-source

[2] D. M. Wennergren, Clarifying guidance regarding open source software (OSS). Department of Defense Chief Information Officer. 2009. 6 p.

[3] M. Metheny, “A case for open source,” in Federal Cloud Computing, Elsevier, 2017. pp. 59-77.

[4] A. van Loon, D. Toshkov, Adopting open source software in public administration: The importance of boundary spanners and political commitment,” Government Information Quarterly, Vol. 32, Issue 2, pp. 207-215, April 2015

[5] J. Söderberg, Hacking capitalism: The free and open source software movement (Vol. 9). Routledge. 2015.

[6] İ. Calallı, İnformatika terminlərinin izahlı lüğəti (ingiliscə-rusca-türkcə-azərbaycanca). Bakı: İnformasiya texnologiyaları. 2017. – 995 s.

[7] I. Hann, J. Roberts, S. Slaughter, “Why developers participate in Open Source software projects: An Empirical investigation,” Proc. of the 25th International Conference on Information Systems, 2004, pp. 821-830.

[8] Stürmer M. “Four types of open source communities.” 2013. https://opensource.com/business/13/6/four-types-organizational-structures-within-open-source-communities

[9] G. M. Kapitsaki, N. D. Tselikas, I. E.Foukarakis, “An insight into license tools for open source software systems,” Journal of Systems and Software, Vol. 102, pp. 72-87, April 2015.

[10] T. Howlett, Open Source security tools: Practical guide to security applications. Prentice Hall. 2004. 608 p.

[11] Gartner: "Market Trends: Cloud-Based Security Services Market, Worldwide, 2014." http://www.gartner.com/resId=2607617.

[12] A. Boulanger, “Open-source versus proprietary software: Is one more reliable and secure than the other?,” IBM Systems Journal, vol. 44, no. 2, pp. 239-248, 2005.

[13] S. Mansfield-Devine, “Open source software: determining the real risk posed by vulnerabilities,” Network Security, Volume 2017, Issue 1, pp. 7-12, January 2017.

[14] Editorial: “‘Heartbleed’ flaw leaves millions of websites, email servers and other services vulnerable to attack,” Network Security, Vol. 2014, No. 4, pp. 1-2, April 2014.

[15] P.F. Roberts, The state of open source security. InfoWorld, 2015. http://www.infoworld.com/article/2901893/security/the-state-of-open-source-security.html.

DOI: 10.25045/NCSoftEng.2017.08