Proqram sistemlərinin təhlükəsizliyi və etibarlılığının təmin edilməsində özünüidarə mexanizmləri

Tofiq Kazımov[1], Tamilla Bayramova[2]

AMEA İnformasiya Texnologiyaları İnstitutu
[1]tofig@mail.ru, [2]tamilla@iit.ab.az

***Xülasə*— Məqalədə proqram sistemlərinə olan haker hücumlarının sayının artması ilə əlaqədar olaraq yaranan təhlükələr təhlil edilir. Bu təhlükələrin qarşısını almaq məqsədilə onların avtomatik aşkar edilmə vasitələrinin, proqram təminatının ozünüidarə mexanizmlərinin işlənilməsi və yaradılan proqram məhsullarının sertifakatlaşdırılması məsələləri araşdırılır.**

Açar sözlər— proqram təminatının etibarlılğı; proqramların təhlükəsizliyi; malware; Self-Managment; Self-Configuring; Self-healing; Self-Adaptiveness; Self-protecting

I. GİRİŞ

İnformasiya texnologiyalarından (İT) istifadənin səmərəliliyi əsasən onun keyfiyyəti və istifadəçilərin proqramlara olan etibarından asılıdır. İT-nin tətbiq sahələrinin genişlənməsi bəzən proqram məhsullarının keyfiyyətinin lazımi səviyyədə olmaması və onlarda olan səhvlər nəticəsində dəyən ziyanın onların tətbiqindən əldə edilən gəlirdən xeyli artıq olmasına gətirdi.

İnformasiya təhlükəsizliyi istənilən şirkətin normal fəaliyyəti üçün əsas amillərdən biridir. Bu gün əksər şirkətlər öz biznes fəaliyyətlərinin əsas tərkib hissəsi kimi İnternetdən daha çox istifadə edirlər. Bunun nəticəsində şirkətin İT strukturundakı daxili proqramların təhlükəsiz fəaliyyəti və şirkətlərin, ümumilikdə təhlükəsizlik siyasəti üçün aparat və proqram vasitələrinin rolu daima artır. Bununla yanaşı əksər hallarda təhlükəsizlik vasitələrinin tətbiqinin iqtisadi səmərəliliyinin qiymətləndirilməsi, ofis proqramlarından istifadənin və müəssisəni idarə etmə sistemlərinin səmərəliliyinin qiymətləndirilməsinə nisbətən çətin olur.

Müəssisənin informasiya təhlükəsizliyini təmin edən vasitələri üç qrupa bölmək olar: antivirus mühafizə vasitələri, brandmauerlər və hücumların aşkar edilmə vasitələri. Birinci iki kateqoriyadan olan vasitələrdən kifayət qədər geniş istifadə edilir. Brandmauerlər sinfinə daxil olan bəzi məhsulların tərkibində hücumları aşkar etmək üçün vasitələrin olmasına baxmayaraq sonuncu qrup daha yenidir. Bu məqalədə bu hücumların daha çox yayılmış hallarını, onların qarşısının alınması üçün hansı tədbirlərin görülməsinin vacibliyini nəzərdən keçirilir və özünüidarə mexanizmləri analiz olunur.

II. PROQRAM SİSTEMLƏRİNDƏ OLAN BOŞLUQLARDAN İSTİFADƏ EDƏN HAKER HÜCUMLARI

Məlumdur ki, hücumlar korporativ resurslardan qanunsuz istifadə etmək və müəyyən prosesləri icra etmək üçün administrator hüquqları almağa yönəlib. Hücumlar həm xaricdən həm də daxildən ola bilər, lakin onun mənbəyindən asılı olmayaraq ilk addım administrator hüquqları almaq üçün proqram kodundakı zəif nöqtələri tapmaqdan ibarətdir. Təəssüf ki, belə zəif nöqtələr əksər proqram məhsullarında var. Proqram məhsulunun zəif nöqtələrindən istifadə edərək edilən hücumların siyahısı kifayət qədər genişdir, buraya parolların təyin edilməsi, Web-serverlərə hücumların edilməsi, Web-səhifələrə icra edilən kodlardan ibarət obyektlərin əlavə edilməsini aid etmək olar. Bunlardan ən çox yayılanları aşağıdakılardır:

- buferin dolması – qeydiyyatdan keçməmiş istifadəçilər hücum obyektinə çoxlu syda sorğular göndərir, bu hücumların nəticəsində proqram öz funksiyalarını icra etməyə qadir olmur. Bu hücum növünün çoxdan məlum olmasına baxmayaraq belə zəif nöqtələrə malik proqramlar yenə də yaradılır;
- standart parollardan istifadə edilməsi – bu hücumu edərkən ehtimal edirlər ki, şəbəkə və ya verilənlər bazası administratoru sənədləşmədə göstərilən parolu dəyişməyib bu parol isə onlara məlumdur;
- zərərli proqram təminatlarından (malicious software – *malware*) istifadə edilməsi – bu şəbəkənin icazəsiz monitorinqini aparmağa, zəif nöqtələrin aşkar edilməsinə və parolların təyin edilməsinə imkan verən xüsusi proqram təminatıdır. "Zərərli proqram təminatı" və ya "zərərli proqram kodu" anlayışlarına viruslar, troyan proqramları, fişinq, şəbəkə hücumları vasitələri, spamların göndərilməsi və digər arzuolunmaz fəaliyyətlər daxildir. [1];
- virusların göndərilməsi – viruslar verilənlərin dağıdılması, şəbəkənin işinin pozulması məqsədilə yazılmış xüsusi proqram təminatıdır və öz-özünə artma xüsusiyyətinə malikdirlər. Bəzi hallarda viruslardan şəbəkəyə nəzarəti ələ almaq və resurslara icazəsiz əlyetərlilik qazanmaq üçün də istifadə edirlər;
- xidmətdən imtina (Denial of Service, DoS - DDoS) – şəbəkə hücumlarının ən geniş yayılmış hallarından biridir. Belə hücumun özünü göstərməsinin ən sadə halı qanuni sorğuya cavabın verilməməsidir, çünki şəbəkənin bütün resursları (vəya fəaliyyət göstərən proqram təminatı) digər mənbələrdən daxil olan çoxlu sayda sorğulara xidmət etməklə məşğul olur. Qeyd edək ki, belə hücumlarda nəinki şəbəkəyə hücumlar edilir, həm də ondan digər şirkətlərin şəbəkələrinə də hücumlar zamanı istifadə edilir.

DDoS hücumların qarşısının alınması və veb-proqramların təhlükəsizliyinin təmin edilməsi üzrə ixtisaslaşmış Qrator Labs [2] və Wallarm [3] şirkətləri bu il üçün aktual olan kibertəhlükələr haqqında hesabat hazırlamışlar.

Qrator Labs şirkətinin direktoru Aleksandr Lyamin qeyd etmişdir ki, 2014-cü ildə hakerlər fenomenal aktivlik göstərmişlər, onlar DNS, NTP, SSDP, SNMP və digər serverlərin konfiqurasiyasında olan zəif nöqtələrdən istifadə edərək hücumların dəfələrlə gücləndirilmə metodlarını (Amplification Method) çox yaxşı öyrəniblər. Göndərilən paketlərə kütləvi şəkildə saxta IP-ünvanlar verərək minlərlə özgə serverləri məqsəd kimi götürülmüş serverə hücum etməyə məcbur edirlər. Wallarm şirkətinin direktoru İvan Novikov də öz növbəsində İnternet proqramları və veb layihələr üçün təhlükələrin gücləndiyindən danışdı. 2014-cü il bütün İnternetin təlükəsizliyinə təsir edən Heartbleed, ShellShock и Poodle hücumları ilə yadda qaldı.

Heartbleed (qan daman ürək) zəif nöqtəsi hamı tərəfindən istifadə edilən OpenSSL kitabxanasında aşkar edildi (OpenSSL SSL və TLS kriptoqrafik protokollarını realizə edən funksiyalardan ibarətdir, verilənlərin təhlükəsiz ötürülməsi üçün müasir sistemlərin əksəriyyəti SSL protokolu əsasında qurulub). Heartbleed milyonlarla server və qurğunu təhlükə altında qoydu. Onun vasitəsilə uzaqlaşdırılmış serverlərin yaddaşından verilənləri oxumaq imkanı əldə edən hakerlər İnternet resurslara əlyetərlilik əldə edərək, oradan qeydiyyat yazıları, pul ödənişləri və digər məxfi informsiyalar haqqında məlumatları oğurladılar. Heartbleed zəif nöqtəsinin aşkar edilməsinə baxmayaraq İnternetdə yenə də bu hücumlar davam edir. Çünki bəzi qurğuların yenilənməsi çox mürəkkəb bir prosesdir və baha başa gəlir.

İkinci daha da təhlükəli zəif nöqtə ShellShock Linux və Unix sistemlərində geniş istifadə edilən Bash əmr üzlüyündə aşkar edildi. O Bash interpretatorunun daxilində dəyişənlər mühiti yaratmağa və sistemdə ziyanverici kodu işə salmağa imkan verir. ShellShock təkcə İnternet-serverlər və işçi stansiyalar deyil, həm də gündəlik həyatda daha çox istifadə edilən smartfonlar, planşetlər və noutbuklar üçün də təhlükə mənbəyidir.

Poodle (Padding Oracle On Downgraded Legacy Encryption) hücumları SSL protokolunda olan daha bir zəif nöqtəni də aşkar etdi.

2015-ci ilin əvvəlində iki daha təhlükəli zəif nöqtə Ghost və Freak aşkar edildi. Birincisi ShellShock qədər təhlükəli olmasa da bəzi hallarda o da kibercinayətkarlara Linux serverlərdə təhlükəli kodun icra edilməsinə imkan verir. İkincisi isə SSL kanalları üçün təhlükələr siahısına əlavə edildi. Bu təhlükələrin əksəriyyətinin qarşısını almaq üçün bir neçə patç (proqramın müəyyən bir hissəsini əvəz etmək üçün yazılmış kiçik proqram) buraxılmışdır. Təkcə Oracle son üç ayda öz proqramları üçün 128 patç buraxmışdır [4].

III. PROQRAM SİSTEMLƏRİNƏ OLAN HÜCUMLARIN İNKİŞAF PERSPEKTİVLƏRİ

Bu il kiber təhlükələrin sayı daha da arta bilər, proqnozlara görə 2015-ci ildə hücumlar daha aqressiv olacaq və bunlar təkcə gəlir əldə etmək üçün deyil, hücum edənlərin öz güclərini nümayiş etdirməsi üçün də yerinə yetiriləcək. Dövlətlər, təşkilatlar və ayrı-ayrı şəxslər arasındakı konfliktlər isə kibermühitə keçəcək. Şəbəkə avadanlıqlarına ShellShock və Heartbleed hücumları davam edəcək və SSL və NoSQL verilənlər bazası ilə əlaqəli yeni zəif nöqtələr aşkar ediləcək.

"Kasperski laboratoriyasının" ekspertlərinin proqnozlarına görə əgər belə hücumları dövlət maliyyələşdirərsə bu yenu "soyuq kibermüharibə" erasının başlanğıcı ola bilər. Onlar həm də qeyd edirlər ki, informasiya təhlükəsizliyi üçün effektiv sistem yaratmaq məqsədilə bu sahəyə bu gün istifadə edildiyindən 25% artıq investiisiya qoyulmalıdır [5].

Bulud xidmətlərinin yayılması ilə yanaşı onlardan təhlükəli proqramların yadda saxlanılması və yayılması məqsədilə istifadə ediləcək, bu sahə kibercinayətkarlar üçün cəlbedici hədəfdir. Çünki, onların serverlərində böyük həcmdə məxfi verilənlər saxlanılır, müvəffəqiyyətli hücum nəticəsində onlar kibercinayətkarların əlinə keçə bilər. Lakin bulud infrastrukturu adətən təhlükələrdən kifayət qədər etibarlı və peşəkarcasına müdafiə edilir. Gartner şirkətinin (dünyada qabaqcıl İT-nin analizini aparır (ABŞ)) proqnozlarına görə burada baş verən təhlükəsizlik insidentlərinin 80%-i sistem administratorlarının xətalı fəaliyyətinə və bulud xidməti istifadəçilərinin xidmətdən istifadə edərkən yol verdikləri səhvlərə görə olacaq [6].

Buludlarda saxlanılan verilənlərə mobil qurğulardan da əlyetərlilik mümkündür, çünki, onlar şəbəkənin adi qovşaqları qədər etibarlı qorunmur. Eyni mobil qurğudan həm şəxsi məqsədlər, həm də biznes-məsələlərinin həlli üçün istifadə edildikdə risklər daha da artır.

Son illərdə ziyanverici mobil proqram təminatlarının sayı kəskin surətdə artmağa başlayıb. Bunlardan 90%-dən çoxu Android bazasında işləyən qurğulara yönəlib [7]. Statistikaya görə üç şirkətdən biri zərərli proqramlardan qorunma vasitələrindən tam şəkildə istifadə etmir.

IV. TƏHLÜKƏLƏRİN AŞKARLANMASI VASİTƏLƏRİ

Analitiklərin araşdırmaları göstərir ki, müəssisələrin 10%-i proqram təminatının tətbiq edilmə mərhələsində, 20%-i sənədləşmə mərhələsində təhlükəsizlik sistemini sınaqdan keçirir, 70%-i isə sistemin istismara verilməsini gözləyir [8]. Bu ondan irəli gəlir ki, proqramçılar proqramı hazırlayanda ümid edirlər ki, onlara hücum olmayacaq.

Təhlükələrin aşkar edilmə vasitələri hücum cəhdi kimi qiymətləndirilən hadisələri təyin edib IT administratoru xəbərdar etmək üçün nəzərdə tutulub. Bu vasitələri onların fəaliyyətindən asılı olaraq iki kateqoriyaya bölmək olar:

- bütün şəbəkənin trafikini təhlil edən vasitələr (bu halda şəbəkənin işçi stansiyalarında agent adlanan proqram təminatı qurulur);
- konkret kompüterin trafikini təhlil edən vasitələr (məsələn, korporativ Web-serverin trafikini).

Hücumların aşkar edilmə vasitələıri də brandmauerlər kimi həm proqram təminatı şəklində, həm də aparat-proqram kompleksi şəklində yaradıla bilər. Bu vasitələr o dərəcədə

dəqiq sazlanmalıdır ki, əsil hücum cəhdlərini aşkar etsin və yalançı siqnalların yaranma ehtimalını minimuma endirsinlər. Hücumların aşkar edilmə vasitələrinin yaradılmasında Cisco Systems, Internet Security Systems, Enterasys Networks və Symantec şirkətləri liderlik edir. Computer Associates və Entercept Security Technology şirkətlərini də bu sahədə liderlər sırasında hesab etmək olar.

Microsoft SDL Threat Modeling Tool 3.0 (Security Development Lifecycle (SDL) – təhlükəsiz proqram təminatının işlənilmə metodikasıdır və proqramların həyat dövrünün bütün mərhələlərində tətbiq edilə bilər) analitik vasitə olub, layihənin struktur təhlilini aparır və təhlükəsizliyin təmin edilməsi ilə əlaqədar potensial nöqsanları aşkar edir. Bu vasitədən Windows və ya digər platformalarda işləyən həm yeni, həm də mövcud proqramları yoxlamaq üçün istifadə edilə bilər. Proqram özü isə Windows mühitində işləyir.

Təhlükələrin modelləşdirilməsi proqram təminatının komponentlərinin işlənilməsi zamanı nəyə xüsusi diqqət yetirilməsinin vacib olduğunu müəyyən edir. Proqram təminatının hücumlara dözə biləcəyinə əmin olmaq üçün əvvəlcədən zəif nöqtələrin yerini təyin etmək lazımdır. Verilənlərin daxil edilməsi, autentfikasiya və məxfi məlumatların şifrələnməsi məsələlərinə xüsusi diqqət yetirilməlidir.

V. TƏHLÜKƏLƏRƏ QARŞI MÜASİR MÜDAFİƏ TEXNOLOGİYALARI

Təhlükələrə qarşı müasir müdafiə texnologiyalarına tələbat obyektiv və subyektiv səbəblərdən yaranır. Obyektiv səbəblərə təhlükələrin böyük sürətlə dəyişməsini göstərmək olar. Odur ki, yaradılacaq proqram vasitəsinin yeni tip təhlükələrə qarşı çevik və effektiv olması və qiymətinin də geniş istifadəçi kütləsi üçün uyğun olması vacibdir. Subyektiv tələblərə gəldikdə isə hər hansı bir məxfi informasiyanın əlyetərlilik səviyyəsinə nəzarət imkanının olması əhəmiyyətli şərtlərdəndir.

Müasir və həcminə görə böyük proqram kodunun daxili mürəkkəbliyi və dinamik şəkildə dəyişməsi bir çox çətinliklər yaradır. Hələ 2001-ci ildə IBM şirkətinin vitse-prezidenti yazırdı ki, İT-nin inkişafında əsas maneə proqram təminatının mürəkkəbliyi olacaq [9]. Proqram təminatının mürəkkəbliyi artdıqca onda olan zəif nöqtələrin də sayı arta bilər. Proqram təminatının sınağından sonra da milyonlarla sətir koddan ibarət olan sistemdə bütün problemləri aşkar etmək mümkün deyil. Bu problemlə yanaşı kiberhücumlar da qaçılmazdır. Proqram təminatının tamlığını və əlyetərliyini qorumaq üçün möbcud olan metodlar artıq kifayət etmir.

Qoyulan tələbləri təhlil edərək (adaptiv, sərbəstlik, yeni təhlükələrə sürətli reaksiya və s.) demək olar ki, bu məsələlərin həllində süni intellekt texnologiyalarına əsaslanan, sərbəst işləyə bilən və yeni şərtlərə tez uyğunlaşan sistemlərin yaradılmasına ehtiyac duyulur. Məhz belə sistemlər dəyişən şərtlərdə fasiləsiz olaraq uyğunlaşa və biliklərini artıra bilərlər və daha vacib olan odur ki, onlar bunu sərbəst şəkildə insanın iştirakı olmadan həyata keçirir [10]. Beləliklə, proqram təminatının özünü idarəetmə (Self-Managment) anlayışı yarandı. Buraya özüuyğunlaşan, özüqorunan, özünümüalicə və s. kimi funksiyalar daxildir.

Özünü idarəetmə dedikdə sistemin administratorun müdaxiləsi olmadan avtomatik və dinamik şəkildə öz fəaliyyətini və funksional imkanlarını və sistemin etibarlılıq səviyyəsini yaxşılaşdırmaq məqsədilə öz xarakteristikalarını dəyişmək qabiliyyəti başa düşülür. Proqram təminatlarının özünüidarə mexanizmlərini təyinatından (adaptasiya, nəzarət fəaliyyət rejimlərinə tələblərin dəstəklənməsi) asılı olaraq aşağıdakı kimi klassifikasiya etmək olar:

- ümumilikdə sistemin strukturunu dəyişən (özünü sazlama - Self-configuring) və onun ayrı-ayrı komponentlərinə təsir edən (özünü təşkil etmə - Self organizing) mexanizmlər;
- sistemin daxili (özünümüalicə - Self-healing) və xarici (özüuyğunlaşan - Self-adaptiveness) dəyişikliklərinə (ətraf mühitin dəyişməsi) nəzarət mexanizmləri;
- proqram sistemlərinin təhlükəsizlik tələbləblərini dəstəkləyən (özünümüdafiə - Self-protecting) və onun işinin keyfiyyət (özüoptimallaşan - Self-optimizing) mexanizmləri.

Özünümüalicənin həyata keçirilməsinə dair aşağıdakıları misal göstərmək olar:

- Massaçuset Texnoloji Universitetində (ABŞ) proqramların nasazlıqlara və hücumlara qarşı dayanıqlığını artırmaq məqsədilə Clear View adlı sistem işlənilmişdir. Mühəndis – proqramçı proqram təminatında zəif nöqtəni aşkar etdikdə onu aradan qaldırmaq üçün patç hazırlayır bu da bir ayadək vaxt tələb edir. Proqram insan müdaxiləsi olmadan işləyir, ona proqram təminatının düzgün işləməsi haqda təlimatlar daxil edilir. Sistem hücumu aşkar edən kimi onun hansı istismar parametrlərini dəyişdirdiyini təyin edir və proqram təminatının bərpası üçün patç hazırlayır, sonra edilən düzəlişlərin problemi aradan qaldırıb qaldırmadığını yoxlayır.
- Hewlett-Packard (HP) firmasında hücumlardan qorunmaq üçün qurğunun özü üçün “smart BIOS” proqramı hazırlanıb. Yuxarıda qeyd etdiyimiz kimi haker hücumlarının əksəriyyəti əməliyyat sistemlərinə edilir və BIOS-da dəyişikliklər edərək administrator hüququ alırlar. Yeni proqramda BIOS-un bir nüsxəsi avadanlığa quraşdırılır və həmişə yüklənən proqramla müqayisə edilir. Fərq aşkar edildikdə kompüter BIOS-un ilkin versiyasını yenidən yükləyir.

NƏTİCƏ

Hazırda proqram təminatlarının təhlükəsizliyinin və etibarlılığının təmin edilməsilə bağlı müxtəlif layihələr işlənib hazırlanır. ABŞ milli Kəşfiyyat İdarəsinin qabaqcıl tədqiqat layihələri şöbəsi Machine Intelligence from Cortical Networks (MICrONS) proqram layihəsi üzrə mütəxəssislərin yeni təkliflərini qəbul edir. Bu layihənin məqsədi insan beyninin mikrostrukturuna bənzər modelə əsaslanan, mürəkkəb məsələləri insan kimi həll etməyə imkan verən yeni nəsil adaptiv alqoritmlərin yaradılmasıdır [11]. Bu alqoritmlər

beyinə məxsus olan təhsil alma qaydalarına əsaslanaraq qəbul edilən verilənləri dəyişdirmək və yeniləmək qabiliyyətinə malik olmalıdır. Mürəkkəb informasiya sistemlərinin arxitektur, texniki və proqram-informasiya uyğunluğuna proqram və texniki vasitələrin beynəlxalq standartlara müvafiq olaraq standartlaşdırılması hesabına nail olmaq olar. Bunun üçün istifadə edilən vasitələrin, proseslərin və xidmətlərin sertifikatlaşdırılması lazımdır.

İT-nin tətbiq sahəsindən və proqram vasitələrinin və verilənlər bazasının təyinatından asılı olaraq sertifikatlaşdırma məcburi (sərt) və fakultativ (yumşaq) ola bilər. Məcburi sertifikatlaşdırma xüsusi əhəmiyyətli funksiyaları yerinə yetirən informasiya sistemləri üçün vacibdir. Burada keyfiyyətin aşağı olması, səhvlər və imtinalar böyük ziyan vura bilər və ya insanların həyatı və sağlamlığı üçün təhlükə yarada bilər. Belə sistemlərdə informasiya texnologiyalarının sertifikatlaşdırılması onların tətbiqindən yaranan risklərin azaldılmasına və fəaliyyətinin təhlükəsizliyini lazımi səviyyəyədək artırmağa imkan verir.

Fakultativ sertifikatlaşdırma İT-nin rəqabətə davamlılığını artırmaq məqsədilə onun keyfiyyətinə zəmanət vermək, tətbiq sahəsini genişləndirmək və bazarda əlavə iqtisadi üstünlüklər əldə etmək üçün tətbiq edilir. Belə sertifikatlaşdırma sınaqlarına əməliyyat sistemlərinin komponentləri və tətbiqi proqram paketləri məruz qalır. İT-nin sertifikatlaşdırılmasına çəkilən xərclər onların qiymətinin artması, istifadəçilərin iradlarının azalması, satış tirajlarının artması və s. hesabına özünü doğruldur [12].

$(ISC)^2$ şirkəti (International Information Systems Security Certification Consortium – informasiya sistemlərinin təhlükəsizliyini sertifikatlaşdıran beynəlxalq konsorsium) kompyuter təhlükəsizliyi sahəsində mütəxəssislərin sertifikatlaşdırılasını həyata keçirir. Bu ildən daha iki sertifikatın verilməsi nəzərdə tutulur [13]. Bunlardan biri proqramların təhlükəsizliyini təmin edən metodların işlənilməsi və tətbiqində proqramçıların kvalifikasiyasını müəyyən etmək üçün nəzərdə tutulub. CSSLP (Certified Secure Software Lifecycle Professional təhlükəsiz proqramların həyat dövrü üzrə sertifikatlaşdırılmış mütəxəssis) sertifikatı almaq üçün mütəxəssis proqramların həyat dövrü, zəif nöqtələri, risklər və informasiya təhlükəsizliyinin əsasları üzrə imtahan verir. Digəri isə $(ISC)^2$ və Cloud Security Alliance (CSA) şirkətlərinin birgə verəcəyi CCSP (Certified Cloud Security Professional - bulud texnologiyalarının təhlükəsizliyi üzrə mütəxəssis) sertifikatıdır.

Haker hücumlarından qorunmaq və proqramların etibarlılığını artırmaq üçün proqram təminatının özünüidarə metodlarından bir neçəsi təhlil olundu. Bu metodların təcrübədə tətbiqi proqram təminatının interaktivliyini, çevikliyini və dayanıqlığını artıracaq. Bu həm də tam avtonom sistemin yaradılması məsələsinin həlli ola bilər. Bu səbəbdən də proqramların təhlükəsizliyini və etibarlılığını təmin etmək məqsədilə özünü avtomatik olaraq bərpa edən proqram təminatlarının işlənilməsi İT sənayesinin əsas məqsədlərindən biridir. Bu sahədə artıq ilk işlərin görülməsinə baxmayaraq məsələ öz aktuallığını qoruyub saxlayır.

ƏDƏBİYYAT

[1] Julian Evans. “Mobile Malware – the new cyber threat” / HAKIN9, 2010, Vol. 5, No. 8, P. 46-49.

[2] www.qrator.net/ru/company/news/qrator-labs-i-wallarm-proanalizirovali-rynok-kiberugroz-v-runete

[3] www.wallarm.com

[4] www.pcworld.com/article/2034729/oracle-shipping-128-patches-for-apps-database-and-middleware.html

[5] www.blog.kaspersky.ru/ksb2014-predictions/6381/ www.osp.ru/lan/2013/01/13033558/

[6] www.baselinemag.com/c/a/Mobile-and-Wireless/10-Best-Practices-for-Mobile-Device-Security (Access date: 26.02.2009).

[7] www.osp.ru/news/articles/2008/37/5439424/

[8] Horn P. “Autonomic computing: IBM’s perspective on the state of information technology”, IBM, October 2001.

[9] Bailey C., Montrieux L., De Lemos R., Yu Y., Wermelinger M. “Run-Time Generation, Transformation, and Verification of Access Control Models for Self-Protection” / Proc. of 9th International Symposium on Software Engineering for Adaptive and Self – Managing Systems. Hyderabad, India. 2-3 June 2014, p135-144.

[10] www.iarpa.gov/research-proqrams/microus/

[11] Методические документы ИСО/МЭК по сертификации продукции, оценке систем обеспечения качества продукции и аккредитации испытательных лабораторий, пер. с англ. М.: Изд-во стандартов, 1988.

[1] www/isc2/org