Addım 5: Təsdiqlənmiş mexanizmlərdən istifadə edin. SQLi müdafiəsini sıfırdan qurmağa çalışmayın. Müasir inkişaf texnologiyalarının əksəriyyəti sizə SQLi-dən qorunmaq üçün mexanizmlər təklif edə bilər. Təkəri yenidən ixtira etmək əvəzinə bu cür mexanizmlərdən istifadə edin. Məsələn, parametrləşdirilmiş sorğulardan və ya saxlanılan prosedurlardan istifadə edin.
Addım 6: Müntəzəm olaraq skan edin (Acunetix ilə). SQL inyeksiyaları tərtibatçılarınız tərəfindən və ya xarici kitabxanalar/modullar/proqram təminatı vasitəsilə təqdim oluna bilər. Siz Acunetix kimi veb zəiflik skaneri istifadə edərək müntəzəm olaraq veb proqramlarınızı skan etməlisiniz. Jenkins istifadə edirsinizsə, hər quruluşu avtomatik skan etmək üçün Acunetix plaginini quraşdırmalısınız.[11]

Nəticə

Bir çox veb sayt və proqramlar hazırda SQL İnyeksiya hücumlarına qarşı həssasdır. Bu cür hücumlar təhlükəsi olan platformalarda istifadəçilərin rahat işləməyi çətinləşir. Bununla belə, bu cür hücumları dayandırmaq üçün çoxsaylı məhdudiyyətlər və təhlükəsizlik tədbirləri mövcuddur.İstehlakçıları SQL İnyeksiya hücumlarından qorumaq üçün veb brauzerlər və sistemlər daha möhkəm təhlükəsizlik tədbirləri təmin etməlidir. Bu, mümkün SQL İnyeksiya mənbələrini daha uğurla müəyyən etməyə və dayandırmağa imkan verəcəkdir. İstifadəçi məlumatları daha güclü protokol şifrələməsi və daha geniş çeşidli autentifikasiya üsulları ilə daha yaxşı qorunacaq.

Ədəbiyyat

[1] Debarros, A. (2018), Practical SQL: A Beginner's Guide to Storytelling with Data, New York: No Starch Press, 392 s.
[2] Clarke-Salt, J. (2012), SQL Injection Attacks and Defense 2nd Edition, Oxford: Syngress, 576 s.
[3] Randolph, W., William A., Elizabeth N., Meagan L., Joseph D. A. (2023), SQL Server 2022 Administration Inside Out, United States: Pearson Education, 1593 s.
[4] Thirumalesh, (2022), The Complete Ethical Hacking Book, Hindistan: OrangeBooks Publication, 124 s.
[5] Richie M. (2022), Cybersecurity Design Principles: 2 Books In 1, Richie Miller, 210 s.
[6] Nathan C. , Steven F. (2022), Human Aspects of Information Security and Assurance, New York: Springer International Publishing, 329 s.
[7] https://www.invicti.com/blog/web-security/sql-injection-cheat-sheet/
[8] https://medium.com/@sevda_kh/sql-injection-4e959849f59d
[9] https://www.acunetix.com/websitesecurity/sql-injection2/
[10] https://www.knowledgehut.com/blog/security/sql-injection-and-prevention
[11] https://pentest-tools.com/blog/sql-injection-attacks

BAZAR MÜNASIBƏTLƏRI ŞƏRAITINDƏ INFORMASIYA TƏHLÜKƏSIZLIYININ BƏZI AKTUAL MƏSƏLƏLƏRI

Zamirə İbrahimli
Azərbaycan dövlət Neft və Sənaye Universiteti

Xülasə

Məqalədə müasir insan cəmiyyətinə yeni çağırışlar və təhdidlər kimi informasiya təhlükəsizliyindən bəhs edilir. İnformasiya təhlükəsizliyinin əsas pozucuları kimi hakerlərin elektron hücumları üsulları, spamlar, korporativ viruslar, korporativ şəbəkələr tərəfindən zərərli və təsadüfi hərəkətlər, təbii təhlükələr sadalanır. Müasir cəmiyyətdə informasiya təhlükəsizliyinin təmin edilməsi təcrübəsinin təkmilləşdirilməsində qanunvericilik bazasının gücləndirilməsi, İKT (informasiya-kommunikasiya texnologiyaları) sahəsində kadr hazırlığı sisteminin təkmilləşdirilməsi və bütün internet istifadəçilərinin

bacarıqlarının artırılması zərurətinə xüsusi diqqət yetirilir.Müvafiq məlumatların mühafizəsi sistemində kriptoqrafiya təcrübəsinin keyfiyyətcə təkmilləşdirilməsi probleminə xüsusi yer verilir.

Açar sözlər: informasiya, məlumat, bazar iqtisadiyyatı, informasiya təhlükəsizliyi, kriptoqrafiya, marketinq, rəqəmsallaşma, rəqəmsal texnologiyalar, transformasiya.

Mövzunun məzmununu tam anlamaq üçün bir neçə tərifl ərə, mənalara və anlamlara aydınlıq gətirmək yerinə düşərdi. Beləliklə, informasiya dedikdə bir qayda olaraq müxtəlif mənbələrdən, müəyyən üsullarla (sorğu, müşahidə, nümunələrin götürülməsi, tədqiqatların aparılması və s.), eləcə də alət və metodlardan istifadə edərək əldə edilən məlumat və ya məlumat topluları başa düşülür. Demək, hər hansı bir məlumat və ya malumatlar kütləsi informasiyaların özəyini təşkil edir.

İnformasiya bizi əhatə edən ətraf mühit haqqında şüurlu qəbul etdiyimiz, saxlanma, çevrilmə, ötürülmə və istifadə obyekti olan məlumatlar toplusudur desək yanılmarıq. İnformasiya müxtəlif şəkildə paylanmış siqnallardan, mesajlardan, xəbərlərdən, bildirişlərdən və s. ifadə etdiyimiz məlumat dolu bilikdir. Məlumatlar müxtəlif informasiya daşıyıcılarında əksini tapa və toplana bilər.

Elmi-nəzəri terminlərə dair sonu görünməyən mübahisələr etmək olar. Lakin, onlarla əlaqədar heç olmazsa şərti olaraq, biri-birimizi anlamaq üçün müəyyən bir razılığa gəlmək düzgün olardı.

İnformasiya təhlükəsizliyi (İngiliscə ***Information Security***, və ya ***InfoSec***) məlumatın icazəsiz daxil olmasının, istifadəsinin, açıqlanmasının, təhrif edilməsinin, dəyişdirilməsinin, tədqiq edilməsinin, qeydə alınmasının və ya məhv edilməsinin qarşısının alınması təcrübəsidir. Bu universal anlayış məlumatların hansı formaya düşməsindən (məsələn, elektron və ya fiziki) asılı olmayaraq tətbiq edilir [6].

Əlavə olaraq bildirək ki, informasiya məlumat toplusu olmaqla müəyyən bir şey haqqında fikir və biliklərlərdən ibarət olur. Məlumat - mesaj informasiyanı özündə əks etdirən işarələr sistemləri vasitəsilə qeydə alınmış toplum kimi insanlar tərəfindən qəbul edilir.Digər tərifə görə informasiya təbiətdə, cəmiyyətdə, eləcə də insanlar tərəfindən yaradılan texnogen sistemlərdə dövr edən məlumatlar məcmusudur. İnformasiya resursları isə istehsalda, texnologiyada və sosial idarəetmədə istifadə olunan, kompüterdə xüsusi təşkil edilmiş və emal edilmiş verilənlər toplusudur.

Hər bir ictimai-iqtisadi sistemdə (ibtidai – icma, quldarlıq, feodalizm, kapitalizm və sosializm-kommunizm cəmiyyətlərində) insanlar müxtəlif məlumatlar və informasiyaları əldə etməyə çalışmışlar. Bütün bunlar isə çoxlu sayda müxtəlif təlim-təhsil sistemləri ilə yanaşı elmlərin də meydana gəlməsinə səbəb olmuşdur.

Əvvəllər daş, bürünc və dəmir dövrləri olmuşdursa, kapitalizmin (bazar iqtisadiyyatının) müasir mərhələsində, təxminən XX-ci əsrin ortalarından və ya 60-cı illərindən informasiya cəmiyyətinin formalaşması başlamışdır ki, bu da informasiya-kommunikasiya texnologiyalarının təkamülü və təkmilləşdirilməsi ilə əlaqələndirilir. Bazar münasibətləri şəraitində (kapitalizm kimi adlandırılan bir dövrdə) əmtəə ümumi xaraker daşımağa başlayır və hər bir şey alqı-satqı obyektinə çevrilir, hətta işçi qüvvəsi belə əmək bazarı vasitəsilə bazar məhsuluna çevrilir, informasiya isə adi məhsul kimi alınıb-satılır. Məşhur marketoloq-alim Filip Kotlerin fikrincə "Diqqəti özünə çəkmək, əldə etmək, istifadə etmək və ya istehlak etmək məqsədilə ehtiyacı və ya tələbatı ödəyə bilən və bazarda təklif edilən hər şey əmtəədir" *(Tərcümə müəllifindir)* [2].

Digər iqtisadçı-alim Aslan Məmmədov yazır: "Məhsul istehlakçının tələbatını ödəmək məqsədilə bazara təklif edilən hər hansı tələbatı ödəmək qabiliyyətinə malik olan təbiət tərəfindən hazır şəkildə verilən və (və ya) insan əməyi ilə yaradılan bütün predmetlərdir, şeylərdir, maddi nemətlərdir. Məhsul marketinq fəaliyyətinin, marketinq kompleksinin nüvəsini təşkil edir" [1]. Qeyd edək ki, hər bir yaradılmış məhsul ikili təyinatlı ola bilər: öz istehlakı (istismarı) üçün və ya bazar-satış təyinatlı. Həmin bazar paradiqması bütövlüklə informasiyalara da aiddir. Yəni, informasiyaları yaradan tərəf onlardan özü üçün istifadə etdikdə onlar (informasiyalar) məhsul kimi qiymətləndirilir, bazara çıxarılıb alıcılara təklif edildikdə isə informasiyalar əmtəə qismində çıxış etməyə başlayır.

Bazar münasibətləri şəraitində informasiyalar alqı və satqı obyektinə çevrildiyinə və kommersiya təyinatlı olduğuna görə marketinq elminin diqqətindən kənarda qalmır. Marketinq məlumatları

müəssisələrin, firmaların, şirkətlərin və bu kimi qurumların bazar fəaliyyətinin təhlili və proqnozlaşdırılması üçün zəruri olan rəqəmlər, faktlar, məlumatlar, şayiələr, proqnozlar və digər məlumatlardır.

Fakt ən sadə məlumat növüdür: birbaşa müşahidə oluna bilən hadisə və ya vəziyyətdir. İnformasiyanın özü təcrübədə sistemləşdirilmiş, ümumiləşdirilmiş formada təqdim edilən faktların bir növü kimi qəbul edilir. Şayiələr isə təsdiqlənməmiş, yoxlanılmamış faktlar və məlumatlardan ibarət biliklərdir desək səhv etmərik.İnformasiyalarda əksini tapmış məlumatların qiymətləndirilməsi nəticələrə, hesablamalara və statistik təhlillərə əsaslanan məlumatdır (qiymətləndirmə forması proqnozdur, yəni elmi bu və ya digər istiqamətlərə dəyişmə və inkişaf meyillərinin qabaqcadan təyin edilməsi cəhdidir).

İnformasiyalarda əksini tapmış rəqəmlər müəyyən kəmiyyət məlumatlarının göstərilməsi və xarakterlərinin açılması formasıdır.Burada bilavasitə məqsəd toplanmış məlumatları sistemləşdirmək və strukturlaşdırmaqdır ki, təhlil və proqnozlaşdırma üçün əlverişli olsun və təhlilçilərə düzgün nəticə və tövsiyələr verməyə əsaslar yaratsın.

Aralıq məqsəd, intuitiv nəticələr və dərhal marketinq qərarlarının ortaya çıxması üçün şirkət rəhbərliyi tərəfindən vizual baxış və qiymətləndirmə üçün mövcud olan toplanmış məlumatların xülasəsi və qruplaşdırılmasıdır. Marketinq məlumatlarına müəyyən edilən əsas tələblər aşağadakılardan ibarətdir:

- Aktuallıq - real məlumatın lazımi vaxtda təqdim edilməsi;
- Etibarlılıq - məlumatın toplanması və emalının elmi prinsiplərinə riayət etməklə təmin edilən məlumatın adekvatlığı;
- Məqsədyönümlülük (uyğun, uyğun) - verilən tapşırıqlara uyğun olan məlumatların əldə edilməsi;
- Tədqiq edilən obyektin bütöv (tam) açıqlanması– tədqiqat planının tərtib edilməsi, hadisənin mahiyyətinin, onun iyerarxik quruluşunun və əlaqələrinin müəyyənləşdirilməsi ilə təmin edilir;
- Məqsədyönlülük - məlumatın tədqiqatın ümumi məqsədinə uyğunluğu;
- Vahid informasiya sistemi və metodlarının seçilməsi - verilənlərin emalı metodologiyasının informatika nəzəriyyəsinin və müşahidələrin statistik nəzəriyyəsinin tələblərinə tabe olması.

Marketinq informasiya xidmətləri bazarının əsas iştirakçıları:

- informasiya istehsalçıları
- informasiya satıcıları - informasiya istehlakçıları (abunəçilər).
- informasiya xidmətləri bazarının istehlakçıları.

İstehlakçılar informasiya xidmətlərindən istifadə edərək həll etdikləri vəzifələrə görə fərqlənirlər. Tapşırıqların kommersiyalaşdırılması dərəcəsinə görə onları iki qrupa bölmək olar:

- alimlər, tədqiqatçılar, mühəndislər;
- biznes aləminin nümayəndələri;

İstehlakçılar informasiya-məlumat bazalarından istifadə baxımından iki kateqoriyaya bölünə bilərlər:

a) şirkətin marketinq problemlərini həll etmək üçün məlumatdan birbaşa istifadə edən istehlakçılar;

b) kommersiya informasiya xidmətlərini təşkil etmək üçün satın alınmış verilənlər bazasından istifadə edən istehlakçılar.

İnformasiya xidmətləri bazarının məhsul döndərənləri və təchizatçıları. İnformasiya xidmətləri bazarının əsas tədarükçüləri KİV (*kütləvi informasiya vasitələri*: qəzet və jurnallar, televiziya və radio), müəssisələrin verilənlər bazası generator mərkəzləri, verilənlər bazası əsasında məlumat paylama mərkəzləri, məlumatların ötürülməsi və telekommunikasiya xidmətləri, informasiya brokerləridir.

Marketinq məlumatlarının yaradılmasının son məqsədi bazar proseslərinin və hadisələrinin təsvirini vermək, bazarın inkişaf meyillərini və qanunauyğunluqlarını müəyyən etmək, şirkətin bazarda yerini qiymətləndirmək və digər idarəetmə problemlərini həll etməkdir.

İnformasiya bazarı bazar münasibətlərinin bir sahəsidir. Marketinq elmi isə bazar münasibətlərindən doğan problemlərin, o cümlədən risklərin idarə edilməsini tənzimləyən, cəmi bazar iqtisadiyyatına yeni nəfəs verən elmi-nəzəri və praktiki kompleksdən ibarətdir. Bazar problemlərinin bu qədər geniş əhatəli və dərin olması ilə əlaqədar marketinq elminin informasiya bazarı aşağıdakı əsas sektorlarla təmsil

olunur: iqtisadi və maliyyə informasiya bölmələri, birja məlumatları, kommersiya məlumatları, statistika xəbərləri, telekommunikasiya daxil olmaqla kütləvi informasiya şəbəkələri, müəssisə və təşkilatların xarici iqtisadi fəaliyyətinin informasiya təminatı, kütləvi məhsul və xidmətlərin istehlakı məlumatları və bazar-marketinq məlumatları.

İnformasiya təhlükəsizliyinin təmin edilməsində informasiyaların təsniləşdirilməsinə, yəni müəyyən əlamətlərə və prinsiplərə uyğun qruplaşdırılmasına xüsusi diqqət yetirilməsi olduqca vacibdir. Məhz təsnifləndirmə əsasında informasiyaların harada, kimlər tərəfindən, hansı məqsədlərlə, kimlər üçün yaradılmasına və digər aktual məsələlərə aydınlıq gətirmək olar. Belə ki, bir çox iqtisadçı – alimlər və təhlükəsizlik problemləri ilə məşğul olan praktiki işçilər amerikalı F.Kotler, rusiyalı A.M.Qodin və V.İ.Belyayev, azərbaycanlı E.N.Quliyev və T.İ.İmanov, M.M.Məmmədov və b. informasiyaları hansı zaman kəsiyində yaradılmasından asılı olaraq iki qrupa bölürlər: təkrar və ilkin informasiyalar.

Təkrar informasiyalara keçmiş dövrlərdən bəlli olan və qalan məlumat topluları, ilkin informasiyalara isə hazırda yaranmış hadisə və proseslərlə əlaqədar axtarılıb tapılan və tədqiqatlarda operativ istifadə edilən cəmi biliklər aid edilir. Adları qeyd edilən mütəxəssislər tövsiyyə edir ki, zamana və vəsaitlərə qənaət etmək məqsədilə ilk növbədə təkrar informasiyalardan istifadə edilməsi düzgün olardı. Sözsüz ki, həmin informasiyalar təzədən nəzarətdən keçirilməli, dəqiqləşdirilməli, və onlar kifayət etməzsə əlavə vaxt və resurs ayırıb, ilkin məlumatlar toplayıb strateji və taktiki tədqiqat prosesini davam etmək lazımdır.

Ümumiyyətlə informasiyaları mənşəyinə, təyinatlarına, əlçatanlıq səviyyələrinə, yayılma və əldə edilmə məqsədlərinə görə, eləcə də təhlükə amillərindən asılı olaraq və digər önəmli hesab edilən əlamətləri nəzərə alaraq qruplaşdırmaq və təsnifləşdirmək olar. İnformasiya təhlükəsizliyi dedikdə bir qayda olaraq məlumatların və onların yaradılmasında, qəbul edilməsində, saxlanılmasında, eləcədə işlənilməsində istifadə olunan infrastruktur obyektlərinə, onların sahiblərinə zərər vura biləcək hər hansı təsadüfi və ya ziyanlı təsirlərdən mühafizə səviyyəsi başa düşülür.

Müəyyən bir təşkilatın informasiya təhlükəsizliyi onun (təşkilatın) informasiya mühitinin formalaşması, istifadəsi və inkişafını təmin edən sistemin təhlükəsizliyinin real və ya hipotetik vəziyyətidir.

Müasir sosiallaşmış cəmiyyətdə informasiya sahəsi iki istiqamət kimi formalaşmaqdadır:

- informasiya və texniki (süni şəkildə insan tərəfindən yaradılmış texnika, texnologiya aləmi və s.);
- informasiya-psixoloji (o cümlədən, insanın özünün də daxil edildiyi canlı təbii mühit).

Müvafiq olaraq, ümumi halda cəmiyyətin (dövlətin) informasiya təhlükəsizliyi informasiya-texniki və informasiya-psixoloji (psixofiziki) təhlükəsizliyi komponentlərində təmsil oluna bilər. [3. 38].

Təcrübədə informasiya təhlükəsizliyi kimi əsasən üç əlaməti (parametri) özündə birləşdirən standart bir modeldən istifadə olunur:

- məxfilik, yəni məxtəlif informasiyanın məxfilik dərəcəsi nəzərə alınaraq yalnız ona hüququ olan məhdud istifadəçilər (subyektlər) üçün əlçatan olması;
- dürüstlük- məlumatın icazəsiz dəyişdirilməsinin icazə verilməməsi və bu kimi cəhdlərin qəti qarşısının alınması;
- əlçatanlıq – giriş hüquqlarını almış istifadəçilərdən məlumatların müvəqqəti və ya daimi gizlədilməsinin qarşısının alınması.

Təhlükəsizlik modelinin birqədər yumşaq formaları da mövcuddur:

-məlumatların müəlliflik mənbələrinin göstərilməsi;

-informasiyalarla tanış olan subyektlərin müəyyən edilməsi və onların hərəkətlərinin qeydə alınmasının təmin edilməsi;

- məlumatlarla əlaqədar nəzərdə tutulan davranışlara və ya qayda və qanunlara daima riayət edilməsi;
- subyektin və ya resursun elan edilmişlərlə eyniliyinə (dəyişdirilməməsinə) zəmanət verilməsi;

Müəssisə və təşkilatların informasiya təhlükəsizliyinə zərər verə biləcək hərəkətləri bir neçə kateqoriyaya bölmək olar [8]:

Hakerlər tərəfindən həyata keçirilən "elektron" təsir üsulları. Hakerlər kompüter cinayətləri ilə həm peşəkar (o cümlədən rəqabətin bir hissəsi kimi), həm də sadəcə maraq ucbatından məşğul olan insanlar kimi başa düşülür. Bu üsullara aşağıdakılar daxildir: kompüter şəbəkələrinə icazəsiz müdaxilə və DOS hücumları.

DOS (ing. Denial of Service - "xidmətin imtina edilməsi"). Belə xarakterli hücumlar sırasına informasiya təhlükəsizliyi və fayl, poçt serverləri kimi şəbəkə qovşaqlarının səmərəli işləməsinə cavabdeh olan müəssisələrə kənardan icazəsiz müdaxilələr aid edilir. Bu cür hücumların nəticəsində infomasiya bazalarına kütləvi şəkildə müxtəlif məlumatların göndərilməsi təşkil olunur və nəticədə həmin qurumlar bir müddət fəaliyyətlərini dayandırmaq məcburiyyətində qalırlar. Bu, adətən biznesdə pozulmalara, uzun müddət ərzində ağır zəhmətlə qazanılmış nüfuzların və müştərilərin itirilməsinə, eləcədə digər neqativ hallara səbəb olur.

Müəssisə və təşkilatların şəbəkəsinə xaricdən icazəsiz daxil olmanın məqsədi zərər vermək (məlumatların məhv edilməsi), məxfi məlumatları oğurlamaq və ondan qeyri-qanuni məqsədlər üçün istifadə etmək, üçüncü tərəf qovşaqlarına hücumların təşkili üçün şəbəkə infrastrukturundan istifadə etmək, hesablardan vəsait oğurlamaq ola bilər və s.

2. Kompüter virusları**.** Elektron təsir üsullarının ayrıca kateqoriyası kompüter virusları və digər zərərli proqramlardır. Onlar kompüter şəbəkələrindən, internetdən və elektron poçtdan geniş istifadə edən müasir müəssisələr üçün real təhlükə yaradır. Virusun korporativ şəbəkə qovşaqlarına daxil olması onların fəaliyyətinin pozulmasına, iş vaxtının və məlumatların itirilməsinə, məxfi məlumatların oğurlanmasına və hətta maliyyə resurslarının birbaşa oğurlanmasına səbəb ola bilər. Korporativ şəbəkəyə nüfuz etmiş virus proqramları vasitəsilə təcavüzkarlar şirkətin fəaliyyətinə qismən və ya tam nəzarət edə bilər.

Təcrübə göstərir ki, birçox hallarda İKT proqramlarını yaradanların özləri və müəyyən səbəblərlə əlaqədar işdən kənarlaşdırılmış mütəxəssisləri, eləcə də müxtəlif ölkələrin xüsusi xidmət orqanlarının əməkdaşları və s. müxtəlif motivlərlə həmçinin virus və antivirus proqramları da tərtib edirlər.

3. Spam. Cəmi bir neçə il ərzində spam kiçik problemdən ən ciddi təhlükəsizlik təhdidlərindən birinə çevrildi: e-poçt bu yaxınlarda zərərli proqramların yayılması üçün əsas kanala çevrildi; spam mesajlara baxmaq və sonradan silmək üçün çox vaxt tələb edir, işçilərdə psixoloji narahatlıq hissi yaradır; müəssisə və təşkilatlarda maliyyə vəsaitlərinin itirilməsinə, tərəflər arasında müqavilələrin pozulmasına və digər problemlərin yaranmasına yol açır.

Spam sonu görünməyən miqdarda müxtəlif formalarda göndərilən arzuolunmaz məlumatlardan ibarət olur. Çox vaxt spam geniş sayda ünvana göndərilən kommersiya e-poçtları şəklində, həmçinin ani mesajlar, mətn mesajları (SMS), sosial media və hətta səsli poçt vasitəsilə göndərilir.

4. Səlahiyyətli istifadəçilər tərəfindən həyata keçirilən hərəkətlər. Bu kateqoriyaya daxildir:

a) provayderlərin və s. iş yerlərində və ya serverdə məlumatların məqsədyönlü şəkildə oğurlanması və ya məhv edilməsi;

b) informasiya-kommunikasiya texnologiyaları (İKT) işçilərinin ehtiyatsız hərəkətləri nəticəsində istifadə ediləcək yararlı məlumatlara xələl gətirmələri.

5. "Təbii" təhlükələr. Müəssisə və təşkilatların informasiya təhlükəsizliyinə müxtəlif xarici amillər təsir edə bilər. Təcrübə göstərir ki, təhsil ocaqlarında, biznes qurumlarında, adi məişət şəraitində və bir çox digər hallarda informasiyaların itirilməsinin başlıca səbəbləri sırasına daxildir: məlumatların düzgün saxlanılmaması, kompüterlərin və informasiya daşıyıcılarının oğurlanması, fors-major hadisələri və digər ağıla-sığmaz hallar.

Beləliklə, qloballaşmaqda olan dünya iqtisadiyyatının müasir inkişaf mərhələsində inkişaf etmiş etibarlı informasiya təhlükəsizliyi sisteminin formalaşması istənilən ölkənin, biznes vahidinin və digər strukturların nəinki rəqabət qabiliyyətini, eləcədə ayaqda və həyatda qalmalarının ən vacib şərtlərdən birinə çevrilir. Müasir zamanda İnternet səbəkəsi ən son mütərəqqi kommunikasiya vasitələrindən istifadə edən ünsiyyət sisteminə çevrilməsi həqiqətdir. Dünya informasiya şəbəkəsi sürətlə inkişaf edir

və iştirakçılarının sayı durmadan artır. Bəzi məlumatlara görə, internetdə 1,7 milyarda yaxın səhifə qeydiyyatdan keçib. Həmin səhifələrin bir qismi cəmi 180 sutka ərzidə ömür sürür, bəziləri isə sahiblərinə uzun aylar və illər ərzində xidmət edərək gəlirli biznes obyektlərinə çevrilir. İnternetdə əks olunan informasiyalar cəmiyyətin bütün təbəqələrində və sadə insanların əksəriyyətində böyük maraqla qarşılanır. Buna baxmayaraq, son 20-30 il ərzində İKT sahəsində toplanmış təcrübə göstərir ki, internet resurslarının imkanlarından bir çox dövlət və biznes qurumları, eləcədə kriminal strukurlar və başqaları qanunsuz və sui-istifadə edərək sivil strukturlara və insanlara qarşı üzqaraldıcı hərəkətlər edirlər [9]. Müşahidələr göstərir ki, İnternet şəbəkələrinə daxil olanların xeyli qismi düşünmədən və məsuliyyətsiz hərəkət edərək, İKT sahəsində nakəm və heçbir hazırlığı olmadan kompüterdən istihadə etməyi dəb-moda kimi qəbul edirlər. Bu, təkcə adi istifadəçilər üçün deyil, həm də kompüter təhlükəsizliyi üzrə elə də dərin bilikləri olmayan və özlərini bu sahədə mütəxəssis kimi mövqeləşdirənlər üçün xarakterikdir. "Kaspersky Lab" şirkətinin məlumatına görə, kompüterə zərərli proqramların daxil olmalarının ümumi sayının təxminən 90%-i İnternet, e-poçt və İnternetə baxış zamanı həyata keçirilir. Bu cür proqramlar arasında xüsusi yeri informasiya şəbəkəsində sistemli şəkildə yayılan İnternet virusları tutur [10].

Elmin, texnikanın və texnologiyanın sürətli inkişafı tamamilə yeni bir sahənin-rəqəmsal texnologiya adlanan sahənin inkişafı üçün əsas olmuşdur. Məhz bu amillə əlaqədar müasir dövrün çoxları tərəfindən "rəqəmsal dövr" kimi təqdim və qəbul edilməsi təsadüf deyildir [4].Bu gün bütün bəşəriyyət minilliklər əvvəl Daş, Tunc və Dəmir dövrləri kimi tanınan çox əsrlərin ağrılı-acılı yollarından keçdiyini inkar etmir. Yəqin ki, bəşəriyyət nəhayət müasir "rəqəmsal dövrün" texniki səviyyəsinə yüksəlmək üçün öz izlərini qoymuş, unudulmuş sivilizasiyaların yıxılması və tərəqqi yolu ilə sonsuz dəhşətlərdən və çətinliklərdən keçərək çatmalıymış...

Təxminən 50 il ərzində bəşəriyyətin əldə etdiyi texniki və texnoloji nailiyyətlərdən istifadə bütün elmlər üçün çoxlu sayda geniş imkanlar açır. Xüsusilə, dünyanın qabaqcıl ölkələrinin aparıcı korporasiyalarının təcrübəsinin göstərdiyi kimi, onların yaradıcılıq strategiyalarında, istehsal və satış biznes fəaliyyətinin səmərəlilik səviyyəsinin yüksəldilməsinə yönəlmiş əməli addımlarda çox şey dəyişir [11]. Müasir informasiya əsrinin təcəssümü, şübhəsiz ki, internetdir. Hazırda ölkələr və mülkiyyət subyektləri arasında iqtisadi, siyasi, mədəni və digər əlaqələrin, habelə bazar subyektlərinin biznes fəaliyyətinin böyük bir hissəsi internet vasitəsilə həyata keçirilir. Bununla belə bir çoxları bilməyir ki, bunlarla korporasiyadaxili və korporasiyalararası informasiya şəbəkələri də mövcuddur [12].

Korporasiyadaxili informasiya şəbəkələri *(intranet)* bir şirkətin işçilərini həm öz aralarında, həm də bu şirkətin kompüter şəbəkəsini birləşdirən vahid şəbəkə sistemi kimi fəaliyyət göstərir.

Şirkətlərarası şəbəkələr *(ekstranetlər)* şirkəti öz təchizatçıları qismində çıxış edənlər-məhsul göndərənləri, distribyutorları və digər üçüncü tərəf tərəfdaşları ilə əlaqələndirən müasir informasiya-kommunikasiya sistemi təşkil edilir və fəaliyyət göstərir. Qeyd edilənləri və bunlarla bağlı olan digər məsələləri həll etmək üçün ayrı-ayrı dövlətlər və beynəlxalq səviyyələrdə kompleks tədbirlər görülməli, eləcədə qanunverici sənədlər hazırlanmalı, yerlərdə qəbul edilmiş qanun və qaydaların icraedici və nəzarətedici strukturların heyətləri arasında İKT sahəsində mütəxəssislər yetişdirilməli, bu sahənin maddi- texniki bazası möhkəmlədirilməli və digər təxirəsalınmaz işlər görülməlidir.

İKT sahəsində əksər mütəxəssislərinin bu fikri ilə tam razıyıq ki, hər bir ölkədə, dövlət və bələdiyyə qurumunda, biznes vahidində və s. strukturda informasiya təhlükəsizliyinin təmin edilməsi vəzifəsi sistemli şəkildə həll edilməlidir. Bu o deməkdir ki, müxtəlif mühafizə tədbirləri (texniki, proqram təminatı, fiziki, təşkilati və s.) eyni vaxtda və mərkəzləşdirilmiş nəzarət altında tətbiq edilməlidir. Eyni zamanda, sistem komponentləri bir-birinin varlığını "bilməli", qarşılıqlı əlaqədə olmalı və həm xarici, həm də daxili təhlükələrdən qorunmalıdır.

Texnika və texnologiyananın hazırkı inkişaf mərhələsində informasiya təhlükəsizliyinin təmin edilməsinin geniş elmi-metodiki bazası mövcuddur [5. 275]: təhlükəsizlik sədləri; özəl virtual şəbəkələr; məzmunların redaktə edilməsi, dürüst hala gətirilməsi filtrləmə vasitələrindən keçirilməsi; antivirus

mühafizə vasitələri; şəbəkə sistemlərinin texniki vəziyyətlərinin və kənardan müdaxilə olunmalarının yoxlanılması; istifadəçilərin dəqiqləşdirilməsi və təyin edilməsi vasitələri.
Sadalanan vasitələrin hər biri müstəqil və ya digərləri ilə inteqrasiyada istifadə edilə bilər. Bu, istifadə olunan platformalardan asılı olmayaraq istənilən mürəkkəblik və konfiqurasiyalı şəbəkələr üçün informasiya təhlükəsizliyi sistemlərini yaratmağa imkan verir. Həmin informasiya təhlükəsizliyi sistemlərindən biri də müəyyən alqoritimlər üzərində qurulmasından asılıdır (şəkil 1).

Şəkil 1. Müxtəlif strukturlarda informasiya təhlükəsizliyinin təmin edilməsinin sadələşdirilmiş alqoritmi

Şəkildə göstərildiyi kimi, bazar münasibətləri şəraitində müəssisə və təşkilatlarda, eləcədə cəmi idarəetmə strukturlarında informasiya təhlükəsizliyinin təmin edilməsi nəinki biri-birindən asılı olmayaraq fərdi qaydada, həmçinin sistemli şəkildə zəncirvari olaraq bütövlükdə informasiya yaradıcıları, informasiyaların yayım kanalları və informasiyaların istifadəçilərini əhatə edilməsi vasitəsilə təmin edilsə, bütövlüklə bazar subyektləri üçün sərfəli olmaqla, bu mütərəqqi İKT şəbəkəsinin etibarlığını artırmış olardı.İnformasiyaların qorunması yollarından biri də, kökləri uzaq tarixə gedən kriptoqrafiyadır. Kriptoqrafiya şifrələnmiş müxtəlif məlumat daşıyıcılarında alqoritmlərdən, xüsusi şifrləmə üsullarında, xeşlərdən və imzalardan istifadə etməklə məlumatın qorunması üsullarıdır. Kriptoqrafiya iki qədim yunan sözlərinin birəşməsindən (κρυπτός "gizli" + γράφω "yazıram") yaradılmış məxfiliyin, məlumatların bütövlüyünün, autentifikasiyanın və şifrələmənin təmin edilməsi üsulları haqqında elmdir [7]. Sözsüz ki, müasir dövrdədə informasiyaların daha mötəbər qorunmasını təmin etmək və bu sahədə durmadan artmaqda olan cinayətlərin qarşısını almaq üçün kriptoqrafiya elmini də inkişaf etdirməli və onun texniki-texnoloji bazasını durmadan gücləndirmək lazım olacaqdır.

Nəticə

İnternet, bütün dünyaya səpələnmiş müxtəlif növ istifadəçiləri bir-biri ilə əlaqələndirən və öz həcminə görə inanılmaz dərəcədə böyük olan məlumat bazası ilə birləşdirən çoxlu sayda kompüter şəbəkələrindən ibarət ictimaiyyət üçün daima əlçatan olan açıq informasiya-məlumat şəbəkəsidir.
Hazırda yaşadığmız cəmiyyətdə İKT sistemləri kimi İnternet, intranet və ekstranetlərin məqsədli şəkildə müəyyən kommunikasiya və biznes planlarını həyata keçirmək və ya nəticədə dəyər (gəlir) əldə etmək üçün məqsədyönümlü işlər görüb və müəyyən dəyərlər yaratmaqdır. Müasir rəqəmsallaşma əsrində inkişaf etmək (və ya ən azı sağ qalmaq) üçün şirkətlər inkişaf strategiyalarını yenidən düşünməli və onları dəyişən mühitə uyğunlaşdırmalıdırlar. İnternet qlobal informasiya cəmiyyətinin formalaşmasına və inkişafına çox güclü təsir göstərib və göstərməkdə davam edir. Sosial fenomen kimi internet ərazi və milli sərhədlər olmadan mətn, qrafik, audio və video məlumatların mübadiləsini və onlayn xidmətlərə çıxışı təmin edən qlobal ünsiyyət vasitəsidir. Formalaşmaqda olan müasir informasiya cəmiyyətində İKT sahəsində yaradılmış internet, intranet və ekstranet şəbəkələri dövlətlərin və xalqların iqtisadi və sosial inkişaflarına yeni imkanlar açmaqla yanaşı yeni çağırışlar və təhdidlər də yaradır. Bu və digər problemləri davamlı olaraq həll etmək və aradan qaldırılması üçün informasiyaların yaradılması, ötürürülməsi, saxlanılması və işlənilməsi üzərində icra və nəzarət edici sistemləri təkmilləşdirmək, bu sahənin təlim və təhsil, eləcədə qanuvericilik bazasını möhkəmləndirmək dövrün tələbi kimi qalmaqdadır.

Ədəbiyyat

[1] Məmmədov A.T.. Marketinqin əsaslari. Dərs vəsaiti. Bakı: "İqtisadiyyan universitetinin nəşriyyatı" 2007.- 337 səh.
[2] Котлер Ф. Основы маркетинга. Краткий курс. : Пер. с англ.- М.:ООО «И.Д. Вильямс», 2012.- 496 с.
[3] Галатенко, В. А. Основы информационной безопасности : учебное пособие / В. А. Галатенко. — 2-е изд. — Москва : ИНТУИТ, 2016. — 266 с.
[4] Грибанов Ю.И., Шатров А.А. Сущность, содержание и роль цифровой трансформации в развитии экономических систем // Вестник Алтайской академии экономики и права. – 2019. – № 3-1. – с. 44-48.
[5] Щербаков, А.Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты. − М.: Книжный мир, 2009. – 352 с.
[6] https://mail.ru/search?search_source=mailru_desktop_safe&msid=1&src=suggest_B&encoded_text=AACxjx4VAxFWS_UtAWJZi7olDXjBh3G-mgV_3bBsDdVZqyIrvrJsxg94sGpST7asc8JOwlG0PewGoxrfb6GbAXRS1oeHDftH6L45Dy4UehAtMD86jhXwMlWszJQOG9zXikXEsBxDw04sWdWOSHeByZCrFr7Vwsc%2C&serp_path=%2Fsearch%2F&type=web
[7] https://www.google.com/search?client=opera&q=что+такое+криптография+9+букв&sourceid=opera&ie=UTF-8&oe=UTF-8
[8] https://www.smart-soft.ru/blog/osnovnye_metody_obespechenija_informatsionnoj_bezopasnosti/
[9] https://cyberleninka.ru/article/n/tsifrovaya-transformatsiya-osnovnye-tendentsii-i-vliyanie-na-sistemu-upravleniya-personalom-predpriyatiya
[10] https://www.litres.ru/book/aleksandr-prohorov-174/cifrovaya-transformaciya-analiz-trendy-mirovoy-opyt-39143851/chitat-onlayn/
[11] https://vaael.ru/ru/article/view?id=349
[12] https://framelink.ru/po-stopam-ccna-10-ponyatiya-internet-intranet-i-ekstranet/

CONSTRUCTİON OF CANSAT (MODEL SATELLİTE). INTEGRATİON WİTH SUBSYSTEMS, DATA ACQUİSİTİON AND PREPARATİON AS A PROTOTYPE

Huseynova Aygun
Askarov Ramid
Azerbaijan State Oil and Industry University

Abstract
One kind of satellite that can fit inside the capacity of a typical soda can is called a CanSat. It is usually used to give students practical experience in planning, constructing, and managing a small satellite system in educational environments like colleges and high schools. CanSats are typically outfitted with an array of sensors and communication systems to carry out particular functions, like atmospheric condition measurement, environmental parameter monitoring, or scientific experimentation. Using balloons or rockets, they are propelled into the atmosphere and return to Earth, generally with a parachute for safety. Students can easily learn about engineering principles and space technology with CanSats.
Keywords: Data Bus, Power Bus, ADCS, OBC, EPS, Payload**.**

CanSat Subsystems and components