**AZƏRBAYCAN RESPUBLİKASI TƏHSİL NAZİRLİYİ**

**AZƏRBAYCAN DÖVLƏT İQTİSAD UNİVERSİTETİ (UNEC)**

**MAGİSTRATURA MƏRKƏZİ**

***Əlyazması hüququnda***

**VƏLİYEV SƏRXAN RAMİZ OĞLU**

# "BANK İNFORMASİYA SİSTEMLƏRİNDƏ İSTİFADƏÇİ HESABININ MÜHAFİZƏSİ MODELİNİN TƏDQİQİ"

**mövzusunda**

**MAGİSTR DİSSERTASİYASI**

**İxtisasın şifri və adı:** 060632 - "İnformasiya texnologiyaları və sistemləri mühəndisliyi"

**İxtisaslaşma:** "İnformasiya mühafizəsi və təhlükəsizliyi"

**Elmi rəhbər:** f.r.e.n., dos. T.Ə. ƏLİYEVA

**Magistr proqramının rəhbəri:** akad. Ə.M. ABBASOV

**Kafedra müdiri** akad. Ə.M. ABBASOV

**BAKI – 2020**

# MÜNDƏRİCAT

# G İ R İ Ş

**Tədqiqatın aktuallığı:** İnformasiya sistemlərinin (İS) tətbiq olunduğu sektorlardan biri də bank sektorudur. Bank sektorunda XX əsrin ən aktual problemlərindən biri yaradılan İS-nin mühafizəsinin təmin olunmasıdır, çünki informasiya texnologiyaları (İT) sahəsi inkişaf etdikcə kibercinayətkarlar tərəfindən iri maliyyə qurumlarının, xüsusilə də bankların İS-nə hücumlar edilir. Müasir dövrdə bütün banklar maksimum dərəcədə müştərilərin bank filialına gəlmədən əməliyyatlarını apara bilməsini təmin etmək niyyətindədir. Bunun üçün banklar öz proqramlarını yaxud məhsullarını hazırlayırlar. Əlbəttə ki, yaradılan bütün proqram və məhsulların təhlükəsizliyi ən mühüm məsələdir.

**Problemin qoyuluşu və öyrənilmə səviyyəsi:** Texnologiyanın inkişafı ilə birlikdə müştərilərin bankların yaratdığı proqram təminatı və məhsullarından istifadəsi gün keçdikcə artmaqdadır. Bu zaman bankların əsas problemlərindən biri yaradılan proqram təminatı və məhsullarının təhlükəsizliyini təmin etməkdir. Minlərlə insanın bank hesablarında saxladıqları pullar İS-nin təhlükəsizliyinin düzgün təmin edilməməsi ilə kibercinayətkarlar tərəfindən oğurlana bilər. Mövcud tətqiqat bu tip problemlərin aradan qaldırılması üçün yeni texnologiyaların, proqram təminatlarının və müasir informasiya şifrələmə alqoritmlərinin iş prinsipi, öyrənilməsi və real mühitdə tətbiqinə əsaslanır.

**Tətqiqat işinin məqsədi:** Son dövrlərdə bütün dünyada kibercinayətkarlar tərəfindən müştərilərin bank hesablarından pullar oğurlanmışdır. Bunun bir çox səbəbi ola bilər. Müştərilərin onlayn olaraq mənşəyi bilinməyən veb saytlardan alış-veriş etməsi ən çox yayılmış vasitədir. Digər bir səbəb də bankların yaratdıqları proqram təminatları yaxud veb saytlarının yüksək təhlükəsizlik tələblərinə cavab verməməsindən irəli gəlir. Aparılan tətqiqatın məqsədi bu tip problemlərin aradan qaldırılması üçün yeni texnologiyaların, proqram təminatlarının və müasir informasiya şifrələmə alqoritmlərinin iş prinsipi, onların öyrənilməsi və real mühitdə tətbiq edilməsi yollarının müəyyənləşdirilməsidir.

**Tətqiqatın predmeti və obyekti:** Tədqiqatın obyekti bank informasiya sistemləri və müştəri hesablarının mühafizə olunmasıdır. Tədqiqatın predmeti isə bank xidmətlərindən istifadə edən müştərilərin hesablarının təhlükəsizliyini təmin etmək üçün digər ölkələrdə tətbiq olunan təcrübə və həmin istiqamətlər üzrə mövcud olan nəzəri-metodoloji biliklərin öyrənilməsidir.

**Tətqiqatın informasiya bazası və metodları:** Elmi ədəbiyyatın öyrənilməsi, sintezi, müqayisəsi, elmi sintez üsulu, faktların seçilməsi və təhlil üsulları, informasiya təhlükəsizliyinin konkret inkişafı və onların real həyatda tətbiq edilməsi metodu. Bu dissertasiya işində çoxsaylı elmi məruzələrdən və internet resurlarından istifadə olunmuşdur. Azərbaycanda informasiya təhlükəsizliyinin hüquqi tənzimlənməsi mövzusunun təqdiqi zamanı isə əsasən ölkədə əsas qanunverici baza olan Azərbaycan Respublikası Konstitusiyasına əsaslanıb.

**Tətqiqata uyğun elmi yeniliklər:** Əvvəllər informasiya sistemlərinin təhlükəsizliyinin elmi cəhətdən araşdırılması, tədqiq edilməsi, öyrənilməsi dar çərçivədə yerinə yetirilirdi. Amma son dövrlərdə maliyyə qurumlarına, dövlət təşkilatlarına, özəl şirkətlərə, bank müştərilərinin hesablarına edilən kiberhücumların kəskin artması ilə bu sahənin elmi cəhətdən araşdırılmasına ehtiyac yaranmışdır. Bunun üçün bulud hesablama (cloud computing), rəqəmsal identifikator (Digital ID) kimi yeni texnologiyalar inkişaf etdirilmişdir. Bulud hesablama bank sektorunda məlumatları idarə etmə qabiliyyətini artırmaqla çoxsaylı üstünlüklər təqdim edir. Yəni resurslardan daha çevik və daha səmərəli istifadə edilə bilər. Rəqəmsal ID müştəri təhlükəsizliyinin təmin edilməsində və saxtakarlığın qarşısını almaqda mühüm rol oynayır. Bundan başqa vahid beynəlxalq təhlükəsizlik standartları yaradılmışdır. Bu standartlara görə qarşıya çıxan problemlərin aradan qaldırılması üçün yeni həll üsulları və konsepsiyalar irəli sürülmüşdür.

**Tədqiqat işinin strukturu və həcmi:** Dissertasiya işi giriş, 3 fəsil, 9 paraqraf, şəkil, cədvəl, nəticə və təkliflər, ədəbiyyat siyahısı və əlavələrdən ibarətdir.

Fəsil 1-də informasiya təhlükəsizliyi anlayışı, onun əsas elementləri, əhatə dairəsi kimi anlayışlar geniş şəkildə izah olunmuş, informasiya təhlükəsizliyi

siyasəti anlayışı, həmçinin informasiya sistemləri haqqında da ətraflı məlumat verilmişdir.

Fəsil 2-də bank sektorunda informasiya mühafizə vasitələrinin istifadəsindən bəhs edilmişdir. Bundan başqa mühafizə vasitələrinin ümumi xarakteriskaları, istifadəçilərin autentifikasiyası və identifikasiyası, kibercinayətkarların fəaliyyəti və onların növləri, banklara, dövlət orqanlarına edilən kiberhücumlar, kiber onların meydana gətirdikləri fəsadlar və bu fəsadların aradan qaldırılma yolları haqqında məlumat verilmişdir.

Fəsil 3-də banklarda istifadəçi hesabının mühafizəsi modelinin tədqiqi haqqında məlumat verilmişdir. Bank informasiya sistemlərində istifadəçilərin mühafizəsini təmin etmək üçün güclü vasitə hesab olunan parolların istifadəsi, düzgün və təhlükəsiz parolların seçilməsi, parolların hansı müddət ərzində dəyişdirilməsi kimi məsələlər qeyd edilmişdir. Həmçinin bank müştərilərinin istifadə etdiyi parolların təhlükəsizliyini təmin etmək üçün müasir şifrələmə alqoritmlər və onlara aid nümunələrdən istifadə olunmuşdur.

Dissertasiya işi 71 səhifədən ibarətdir. İş yerinə yetirilərkən çoxsaylı xarici mənbələrdən, internet resurslarından istifadə edilmişdir.

# I FƏSİL. BANK SEKTORUNDA İNFORMASİYA TEXNOLOGİYALARININ TƏTBİQİ

## 1.1. İnformasiya təhlükəsizliyi nədir?

İnformasiya təhlükəsizliyi, icazəsiz girişdən məlumat əldə etməklə bağlı deyil. İnformasiya təhlükəsizliyi, əsasən, informasiyanın pozulmasının, dəyişdirilməsinin, yoxlanılmasının, qeyd edilməsinin və ya məhv edilməsinin qarşısını almaqdan ibarətdir. İnformasiya fiziki və ya elektrik (siqnal) formada ola bilər. Beləliklə, informasiya təhlükəsizliyi kriptoqrafiya, mobil hesablama (Mobile Computing), Kiber Məhkəmə (Cyber Forensics), Onlayn Sosial Mediya və s. kimi tədqiqat sahələrini əhatə edir.

Birinci Dünya Müharibəsi dövründə məlumatların həssaslığını nəzərə alaraq çoxsəviyyəli təsnifat sistemi hazırlanmışdır. İkinci Dünya Müharibəsinin başlanması ilə təsnifat sisteminin rəsmi uyğunlaşdırılması edildi. Alan Turing almanlar tərəfindən müharibə məlumatlarını şifrələmək üçün istifadə olunan Enigma Machine-ni uğurla yarada bildi. İnformasiya təhlükəsizliyi proqramları ümumi olaraq - məxfilik, bütövlük, mövcudluq kimi tanınan 3 prinsip ətrafında qurulur. Bu 3 prinsip CIA (Confidentiality, Integrity, Availability) adlanır.

1. Məxfilik - məlumatın icazəsiz şəxslərə, qurumlara və prosesə açıqlana biləməməyi deməkdir. Məsələn, gmail hesabına giriş üçün istifadəçi şifrəsi digər şəxs tərəfindən müşahidə nəticəsində ələ keçirilərsə, bu halda şifrə öz məxfilik xüsusiyyətini itirmiş olur.

2. Bütövlük - məlumatların dəqiqliyini və tamlığını qorumaqdır. Bu, məlumatların icazəsiz şəkildə redaktə edilə bilməyəcəyi deməkdir. Məsələn, işçi təşkilatdan ayrılırsa, bu halda həmin işçi üçün məlumatlar yenilənməlidir. Məlumatların tam və dəqiq olması üçün bu proses səlahiyyətli şəxs tərəfindən icra edilməlidir.

3. Mövcudluq - məlumat lazım olduqda onun mövcud olması deməkdir. Denial of service (DOS) informasiya əldə edilməsinə mane ola biləcək amillərdən biridir.

Bundan əlavə, informasiya təhlükəsizliyi proqramlarını tənzimləyən digər prinsiplər də var:

- Rədd etməmə (Non-repudiation) - bir tərəfin mesaj və ya əməliyyat almağı inkar edə bilməməsi və digər tərəfin mesaj və ya əməliyyat göndərilməsini inkar edə bilməməsi deməkdir. Məsələn, kriptoqrafiyada mesaj göndərənin şəxsi açarı ilə imzalanan rəqəmsal imza ilə uyğun olduğunu göstərmək kifayətdir. Məlumat bütövlüyü (Data Integrity) və doğruluq (Authenticity) rədd edilməmə üçün ilkin şərtdir.
- Doğruluq (Authenticity) - istifadəçilərin kimliyinin və təyinat yerinə gələn hər bir girişin etibarlı mənbədən olduğunun təsdiqlənməsi deməkdir. Bu prinsip təqib edildiyi təqdirdə etibarlı mənbədən etibarlı bir ötürmə yolu ilə alınan mesaja zəmanət verir. Məsələn, mesaj onun hash dəyəri və şəxsi açarı (private key) istifadə edərək yaradılan rəqəmsal imza ilə birlikdə göndərilir. İndi qəbuledici tərəfdə bu rəqəmsal imza hash dəyəri yaradan açıq açardan (public key) istifadə edərək deşifrələnir.
- Hesabatlılıq (Accountability) - bir təşkilatın hərəkətlərini bu təşkilata bənzərsiz olaraq izləməyin mümkün olması deməkdir. Məsələn, bütövlük bölməsində müzakirə etdiyimiz kimi, hər hansı bir işçinin digər işçilərin məlumatlarında dəyişiklik etməyə icazə verilməməlidir [3].

İnformasiya təhlükəsizliyinin əsasını informasiya təminatı (Information Assurance) təşkil edir ki, bu da məlumatların CIA-nin saxlanması, kritik problemlər yarandıqda məlumatın heç bir şəkildə pozulmamasını təmin edir. Bu məsələlər yalnız təbii fəlakətlər, kompüter / server nasazlığı və s. ilə məhdudlaşmır.

Beləliklə, son illər informasiya təhlükəsizliyi sahəsi xeyli inkişaf etmişdir. Şəbəkələrin və əlaqəli infrastrukturun qorunması, tətbiqetmələrin və məlumat bazalarının təminatı, təhlükəsizlik testi, məlumat sistemlərinin yoxlanılması, işin davamlılığının planlaşdırılması və s. o cümlədən bir çox ixtisas təklif edir.

İnformasiya sistemi (İS), açıqlanmayan zəifliklər vasitəsilə stimullaşdırılmış mövcud tədbirləri və ya nəzarətləri nəzərdən keçirmək və daha çox iş tələb olunan bir sahəni müəyyənləşdirmək deməkdir. İnformasiya təhlükəsizliyinin idarə edilməsinin məqsədi təhlükəsizlik hadisələrinin təsirinin qarşısını almaq və minimuma endirməklə işin davamlılığını təmin etmək və işgüzar zədənin miqyasını artırmaqdır.

Bu gün kiçik bir dükana sahib olan şəxsdən başlayaraq yüksək səviyyəli bir iş adamına qədər hər kəs üçün gündəlik həyatda informasiya mühüm rol oynayır. İnformasiya, smartfonları olmaqdan əməliyyat qəbzlərinə və satın alma modellərinə qədər fərqli şəkillərdə istehsal olunur. Bu, insanların informasiyaları oğurlamaları üçün geniş imkanlar təqdim edir. Buna görə informasiya təhlükəsizliyi zəruridir. İnformasiya təhlükəsizliyinin tarixinə və bu müddət ərzində necə inkişaf etdiyinə nəzər salaq.

- 1960-cı illər: Offlayn saytların təhlükəsizliyi. İnformasiya təhlükəsizliyi, kompüterlərin saxlandığı giriş nöqtələri ilə məhdudlaşmışdı, çünki onlar əvvəllər böyük idi və böyük bir sahə saxlanılmalı və işlədilməli idi. Parollar və digər təhlükəsizlik tədbirləri şəklində terminallar üzərində çoxlu təhlükəsizlik təbəqələri quraşdırılmışdı.
- 1970-ci illər: Fərdi kompüter və xakerlərin təkamülü. Bu zamanlarda qoşulmaq istəyən hər cihazı birləşdirən kütləvi bir qlobal şəbəkə yox idi. Yalnız böyük təşkilatlar, xüsusən hökumətlər, kompüterləri telefon xətləri ilə birləşdiməyə başlamışdılar. İnsanlar informasiyanı oğurlamaq üçün həmin telefon xətləri vasitəsilə axan dataları ələ keçirməyin müxtəlif yollarını axtarmağa başladılar və bu insanlar ilk xakerlər oldular.
- 1980-ci illər: Kibercinayətkarlığın təkamülü. Hacking və digər kibercinayətlərin bu on il ərzində artması insanların kompüter sistemlərinə daxil olmanın müxtəlif yollarını tapması və xakerlərə qarşı heç bir ciddi tənzimləmə olmamasından irəli gəlirdi. Bir çox hökumət və hərbi qrup bu cinayətlərin ABŞ banklarından milyonlarla dollar itkisi ilə nəticələnməsini gözləyirdi və buna cavab olaraq hökumət xakerləri təqib etməyə başlamışdı.

- 1990-cı illər: "Hacking" mütəşəkkil cinayətkarlığa çevrilir. 1989-cu ildə dünya miqyasında internet istifadəyə verildikdən sonra insanlar şəxsi informasiyalarını internetə qoymağa başlamışdılar. Xakerlər bunu potensial gəlir mənbəyi kimi görürdülər və internet vasitəsilə insanlardan, hökumətlərdən informasiya oğurlamağa başlamışdılar. Təhlükəsizlik divarı və antivirus proqramları bunun qarşısını almağa kömək etdi, lakin veb tərəfdə xakerlər hədəf cihazlara sızmağın müxtəlif yollarını tapmışdılar.
- 2000-ci illər: Kibercinayətkarlıq ciddi bir məsələyə çevrilir. Hacking 80-ci illərin sonlarında ciddi problem kimi qəbul edilməmişdi, lakin hacking təkamülü və təhlükələri ilə hökumətlər kibercinayətkarları təqib etməyə başladılar. Kibercinayətkarlar kibercinayətkarlıq fəaliyyətinə görə cəza kimi illərlə həbs edilmişdilər.
- 2010-cu illər: Bildiyimiz informasiya təhlükəsizliyi. Firewall və antivirus şəklində müxtəlif tədbirlər cihazları hücumlardan qorumaq üçün hazırlansa da, kifayət qədər səmərəli və bacarıqlı olan xakerlər hər halda sistemlərin işini poza bilirdilər. İnformasiyanın şəbəkə və digər ötürücü vasitələr üzərində qorunması üçün müxtəlif kriptoqrafik alqoritmlər və şifrələmə üsullarından istifadə olunur. Müxtəlif təşkilatlar informasinın fərqli yollarla pozulmasında insan səhvlərinin qarşısını almaq üçün təhlükəsizlik siyasəti həyata keçirirlər. Proqram və antivirus proqramları, onları kənar hücumlardan qorumaq üçün PC-də quraşdırılmışdır. Vaxt keçdikcə internet və ətrafdakı qurğular inkişaf etdikcə informasiya təhlükəsizliyinə olan təhdidlər və onların işini pozmağın bir çox yolu tapıldı. İnformasiya təhlükəsizliyi hər bir insanın və təşkilatın gündəlik həyatında böyük rol oynayır [4].

## 1.2. Banklarda informasiya təhlükəsizliyi sistemlərinin təşkilinin prinsipləri

Dünyanın son otuz ili informasiya texnologiyalarının (İT), xüsusən kompüterlərin, telekommunikasiya vasitələrinin və informasiya şəbəkələrinin heyrətləndirici və başgicəlləndirici inkişafının və yayılmasının şahidi oldu. Otuz il əvvəl çətin əldə edilən obyekt var ki, indiki dünyada artıq onlar adi obyektə çevrilmişdir. Bu gün yer üzündəki kompüterlərin sayı avtomobillərin sayını keçmişdir.

Fərdlərin əqli və fiziki təhlükəsizliyi son dərəcə vacib olduğu kimi, ailələrin fiziki, iqtisadi və psixi təhlükəsizliyi, həmçinin institusional strukturların fiziki, maliyyə və kiber təhlükəsizliyi, regional təhlükəsizlik, sosial təhlükəsizlik, milli təhlükəsizlik, iqtisadi təhlükəsizlik, sərhəd təhlükəsizliyi, ərzaq təhlükəsizliyi və nəticədə qlobal təhlükəsizlik, ekoloji təhlükəsizlik, nüvə təhlükəsizliyi və kiber təhlükəsizlik hər təbəqədə təmin edilməli və qorunmalı olan təhlükəsizlik növləridir.

İS hərbi və iqtisadi sahələrdə əhəmiyyət qazandığından, istər-istəməz həm hədəfə, həm də bir silah halına gəlmişdi. Bu cür vasitələrin və ya silahların istifadəsi yaxud hədəf alınmasına Amerika Hərbi Hava Qüvvələrinin bir terminologiyası olan Məlumat Müharibəsi (IW) adı verilib. Bu anlayışa düşmənin bu cür hərəkətlərindən özümüzü qorumaq, eyni zamanda düşmənin məlumatlarını təhrif etmək və ya məhv etmək kimi funksiyalar daxildir.

İKT tərəfindən verilən tərifə görə kibertəhlükəsizlik kibermühiti təşkil edən informasiya sistemlərini bu sistemlərə qarşı yönəldilə biləcək hücumlardan qoruyur. Bu mühitdə işlənən məlumatların məxfiliyini, tamlığını və əlçatanlığını təmin edir, kiber hücumları və kiber təhlükəsizlik hadisələrini vaxtında təyin edir.

İnsanlar tərəfindən yaradılan heç bir sistem digər insanlar tərəfindən nüfuz edilə bilməyəcək qədər etibarlı deyildir. Bu səbəblə banklar və digər maliyyə qurumları informasiya sistemlərinin təhlükəsizliyi üçün getdikcə artan miqdarda pul xərcləmək yerinə nə dərəcədə zərər gördüklərində hansı problemlərin yaranacağını nəzərə almalı və müvafiq tədbirlər görməlidirlər.

Hər hansı bir bank üçün informasiya təhlükəsizliyi siyasətinin məqsədi rəhbərliyə iş tələblərinə və müvafiq qanun və qaydalara (İSO 27002, 2013) uyğun olaraq informasiya təhlükəsizliyini təmin etməkdir. Rəhbərlik iş məqsədlərinə uyğun olaraq aydın siyasət istiqamətini təyin etməli və təşkilat daxilində təhlükəsizlik siyasətinin saxlanması yolu ilə informasiya təhlükəsizliyinə dəstək və sadiqliyini nümayiş etdirməlidir.

Nəzarətə sahib olmaq üçün informasiya təhlükəsizliyi siyasət sənədini idarəetmə orqanları təsdiqləməli, yayımlanmalı və bütün işçilərə və müvafiq xarici tərəflərə məlumat verilməlidir. Rəhbərlik aydın istiqamətləndirmə, nümayiş etdirilmiş öhdəlik, açıq tapşırıq və məlumat təhlükəsizliyi öhdəliklərinin (ISO 27002 2013) təsdiqlənməsi yolu ilə təşkilat daxilindəki təhlükəsizliyə fəal dəstək verməlidir. Siyasət bankı təmsil edən yüksək səviyyəli sənəddir. Effektiv olmaq üçün siyasətlər aydın və qısa olmalıdır (ISACA, 2012). Siyasət bank daxilində olan hər kəs üçün məlumat mənbəyi kimi qəbul edilməlidir. Yaxşı təhlükəsizlik siyasəti aşağıdakı primsipləri müəyyənləşdirməlidir:

• Həssas məlumatlara hansı şəkildə nəzarət edilməlidir;

• Bbir bank potensial təhlükəsizlik hadisəsinə necə cavab verməlidir.

İnformasiya təhlükəsizliyi siyasəti təşkilatda idarəetmə sisteminin vacib hissəsidir. Adətən, siyasətdə aşağıdakı aspektlərə dair qaydalar mövcuddur: şəbəkə, qurğular, məlumatlar, əməliyyat, sanksiyalar. Bank rəhbərliyi daxili və ya xarici peşəkar məlumat təhlükəsizliyi yardımına olan ehtiyacları tanımalı və tövsiyələrin nəticələrini təşkilat daxilində qiymətləndirməli və əlaqələndirməlidir (İSO 27002, 2013). Uitmana (2004) görə, effektiv təhlükəsizlik siyasəti xüsusi təşkilati vəzifələri nəzərdən keçirməli, sistemlərin və vasitələrin təsdiqlənmiş istifadəsini müəyyənləşdirməli, sistemə məlum və ya ehtimal olunan təhdidlər barədə məlumat verməli, pozuntular üçün nəzərdə tutulan nəticələri izah etməli və alətləri təqdim etməlidir. Bundan başqa hər il informasiya təhlükəsizliyi siyasətinə yenidən baxılmalıdır. İnformasiya təhlükəsizliyi siyasətinə yenidən baxma prosesində bank rəhbərliyinin qiymətləndirmələrinin nəticələri nəzərə alınmalıdır (İSO 27001, 2013).

Rəhbərliyin qiymətləndirilməsi zamanı aşağıdakılar nəzərə alınmalıdır:

• əlaqəli qurumların tövsiyələri;

• profilaktik və faydalı fəaliyyətlərin vəziyyəti;

• əvvəlcədən idarəetmə araşdırmalarının nəticələri;

• prosesin nəticələri və informasiya təhlükəsizliyi siyasətinə uyğunluq;

• informasiya təhlükəsizliyinə münasibətdə bankların metodunu poza biləcək dəyişikliklər, o cümlədən təşkilati vəziyyətə, iş şəraiti, tənzimləmə və hüquqi şərtlərə görə yayınmalar. Ümumiyyətlə, informasiya metodlarının təhlükəsizliyi mütəmadi olaraq yenidən nəzərdən keçirilməlidir.

İSO 27001 standartına əsasən, təşkilat daxilində təhlükəsizliyi təmin etmək və müştərilərə bankların əməliyyatlarına zəmanət vermək üçün təhlükəsizlik siyasəti və texnika kimi bir çox komponenti nəzərə alaraq həyata keçirilməlidir. Müasir dövrdə bir çox müəssisə, xüsusən maliyyə sektorundakı sahibkarlar, sənayedə müştəri məlumatlarının qorunması və məxfiliyinə dair bir neçə qayda və qaydalara riayət etməlidirlər. Banklar yerli qaydalara riayət etmək, risk azaltma üsullarını tətbiq etmək üçün informasiya təhlükəsizliyi siyasətlərini yaratmaqda səy göstərməlidirlər.

Mümkün olduqda, banklar tabeliyində olan xərclərin avtomatlaşdırılmış həllini axtarır, məhsuldarlığı artırır və təhlükəsizlik məlumatlarının monitorinqinin etibarlılığını bərpa edirlər. Təhlükəsizlik insanların, prosedurların, standartların, proseslərin və texnologiyanın qarışığı ilə tətbiq olunur. İnformasiya təhlükəsizliyinin avtomatlaşdırılması prosesi əsasən insan əməkdaşlığını əhatə edən təhlükəsizlik xüsusiyyətlərini sistemləşdirən müqavilələrdir. Avtomatlaşdırma bacarığı və ya xüsusiyyətləri əlavə edildikdə, banklar sıxlığın monitorinq prosesini artıra bilər. Bundan əlavə, resursların mövcudluğu azalırsa, banklar təhlükəsizliklə əlaqəli məlumatların düzgün araşdırıldığını təsdiqləmək üçün əlaqəli monitorinq sıxlığını tənzimləməyi nəzərdən keçirirlər.

İSO 27002 (2013) standartına əsasən, fiziki və ekoloji təhlükəsizliyin məqsədi biznes saytlarına təsdiqlənməmiş giriş, zərər və qarşıdurmaların qarşısını almaqdır. Ciddi və ya həssas biznes məlumatları emalı vasitələri qorunan ərazilərdə

saxlanılmalı, müvafiq təhlükəsizlik maneələri və giriş nəzarəti ilə dəqiq bir təhlükəsizlik həddi ilə təmin edilməlidir. Təmin edilmiş təhlükəsizlik qəbul edilmiş risklərə uyğun olmalıdır. Bu vəziyyətdə, fiziki təhlükəsizliyi qəbul etmək və təmin etmək üçün banklar əlavə proseduralar təyin etməlidirlər.

ISO 27001-ə əsaslanaraq, bu idarəetmənin məqsədi məlumat emalı vasitələrinin dəqiq və inamlı prosedurlarını təmin etməkdir. Bütün məlumat emalı qurğularının idarə edilməsi və istismarı üçün hesabatlılıq və tədbirlər müəyyənləşdirilməli və tanınmalıdır. Buraya müvafiq əməliyyat təlimatlarının genişləndirilməsi və hadisələrə cavab tədbirləri və ya proseslər daxil ola bilər.

Əsasən, ISO 27001 prinsiplərini və qaydalarını nəzərə alaraq, banklar informasiya təhlükəsizliyi siyasətinin idarə edilməsində və müəyyən edilməsində faydalana bilərlər. İnformasiya təhlükəsizliyi fasiləsizliyi təşkilatın iş davamlılığının idarə edilməsi sistemlərinə daxil edilməlidir. Bir şirkətin və ya bir bankın iş davamlılığının idarə edilməsi prosesi fövqəladə planlaşdırma, iş davamlılığı və bərpadan ibarət mürəkkəb bir prosesdir. Belə bir prosesi qurmaq və saxlamaq üçün səmərəli idarəetmə sistemi lazımdır.

ISO 27001-ə görə, işin davamlılığı biznes fəaliyyətindəki pozulmalara cavab vermək və ciddi iş proseslərini əsas fəlakətlərin təsirindən qorumaqdır. Bu çərçivədə, fəlakətlər və təhlükəsizlik uğursuzluqları səbəbiylə sistemlərdə və ya gündəlik fəaliyyətlərdə fasilələrin azaldılması üçün iş davamlılığının idarə edilməsi prosesi tətbiq edilməlidir. Bundan əlavə, İT idarəetmə sistemləri kimi, informasiya təhlükəsizliyi menecmenti, bina menecmenti, keyfiyyət menecmenti və ya risk menecmenti ilə əlaqəli və ya üst-üstə düşən bütün sahələr müəyyənləşdirilməlidir. İş ardıcıllığının idarə edilməsi prosesi aşağıdakı mərhələlərdən ibarətdir: iş fasiləsizliyinin idarə edilməsi, fövqəladə halların planlaşdırılması və fövqəladə planlaşdırma konsepsiyasının həyata keçirilməsi, iş davamlılığına cavab, testlər və təlimlər, həmçinin işin davamlılığının idarə edilməsi prosesinin saxlanılması və davamlı təkmilləşdirilməsi. Təşkilat daxilində iş davamlılığını inkişaf etdirmək və yeniləmək üçün təsirli və idarə olunan proses olmalıdır. Ümumiyyətlə, bankların idarəetmə orqanları müəyyən edilmiş kritik proseslərin davamlılığını təmin etmək

üçün müvafiq çərçivənin yaradılması üçün cavabdeh olmalıdırlar. Planın hər bir komponentinin necə və nə vaxt sınaqdan keçirilməsini göstərmək üçün işin davamlılığı planı illik əsasda nəzərdən keçirilməlidir.

### 1.3. Banklarda istifadə olunan informasiya təhlükəsizliyi standartları

Daxili informasiya təhlükəsizliyinə nəzarət etmək üçün həmçinin, bütün informasiya təhlükəsizliyi hesabatlarının yaxşı müəyyənləşdirilib bölüşdürülməsi üçün ISO 27002 standartı tövsiyə olunur. Daxili siyasətlər, gözlənilən nəzarət səviyyələrini müəyyən edən və təsdiqləyənlərin idarəetmə tətbiq edənlərdən ayrıldığı və ya təşkilatın bir çox müxtəlif insanlara və ya funksiyalara tətbiq olunduğu vəziyyətlərdə daha böyük və daha mürəkkəb təşkilatlar üçün faydalıdır. İnformasiya təhlükəsizliyi siyasətləri vahid informasiya təhlükəsizliyi siyasəti sənədində fərdi yaxud əlaqəli sənədlər toplusu şəklində verilə bilər.

Təşkilatlar, banklar, bu beynəlxalq standartların minimumunu nəzərə almalıdırlar ki, onların əhatə dairəsinə uyğun olaraq düzgün şəkildə müəyyənləşdirilsin. Bu standartlar əhəmiyyət və nəzarət standartlarına görə banklar tərəfindən həyata keçirilə bilər. Bankların müəyyən etdiyi daxili siyasətlərin bu beynəlxalq standartlara uyğun olması tövsiyə olunur. Bu standartların tətbiqi mərhələsində bankların idarə heyətinin dəstəyi zəruridir. Ən yüksək səviyyədə təşkilatlar, banklar tərəfindən yenidən nəzərdən keçirilmiş və təsdiq edilmiş və bankların özünün informasiya təhlükəsizliyi məqsədləri ilə bağlı yanaşmasını müəyyənləşdirən informasiya təhlükəsizliyi siyasətini təyin etməlidirlər (İSO 27002, 2013).

İnformasiya təhlükəsizliyi siyasətləri aşağıdakı bəzi tələblərə cavab verilməlidir:

Biznes strategiyası;

• Əsasnamələr, qanunvericilik və müqavilələr;

• mövcud və proqnozlaşdırılan informasiya təhlükəsizliyinə təhdid mühiti;

**Beynəlxalq təhlükəsizlik standartları** **Cədvəl 1.1.**

| Standard | Təsviri |
|---|---|
| **ISO 27001 2013** | Bu standartın məqsədi İnformasiya Təhlükəsizliyi İdarəetmə Sisteminin yaradılması, tətbiqi, saxlanması və daim təkmilləşdirilməsi üçün tələbləri təmin etməkdir. |
| **ISO 27002 2013** | Bu standart təşkilat daxilində informasiya təhlükəsizliyi idarəetməsinin təşəbbüsü, tətbiqi, saxlanması və təkmilləşdirilməsi üçün ümumi qaydalar və prinsiplərdir. Standart, eyni zamanda, təşkilati təhlükəsizlik standartlarının və effektiv təhlükəsizlik idarəetmə təcrübələrinin inkişafı üçün bələdçi təqdim etmək və qurumlararası fəaliyyətə etimad yaratmağa kömək etmək məqsədi daşıyır. |
| **ISO 27003** | Bu inkişaf standartının məqsədi İnformasiya Təhlükəsizliyi İdarəetmə Sisteminin tətbiqində kömək və rəhbərlik göstərməkdir. |
| **ISO 27004** | Bu standard, təşkilata İnformasiya Təhlükəsizliyi İdarəetmə Sisteminin tətbiqi prosesinin effektivliyini yaratmağa kömək etmək məqsədi daşıyır. |
| **ISO 27006** | Onun rəsmi adı İnformasiya texnologiyası - Təhlükəsizlik texnikasıdır. İnformasiya təhlükəsizliyi idarəetmə sistemlərinin auditi və sertifikatlaşdırılmasını təmin edən orqanlara olan tələblər və 10 fəsil və dörd əlavədən ibarətdir. |
| **PCI/DSS Payment Card Industry** | Ödəniş Kartı Sənayesi Informasiya Təhlükəsizliyi Standartı - Bu standart, onlayn kart əməliyyat sənayesi ilə bağlı müştərilərin şəxsi məlumatlarının təhlükəsizliyi üçün istifadə olunur. |
| **ITIL or ISO/IEC 2000 series** | İnformasiya texnologiyaları İnfrastruktur Kitabxanası - İT-nin xidmət prosesləri üzərində dayanır və istifadəçinin mərkəzi rolunu nəzərdən keçirir. |
| **BS7799** | Britaniya Standartları İnstitutu - İngilis Standartlar İnstitutu tərəfindən yazılmış və saxlanılan standartdır və standart haqqında, habelə haradan əldə ediləcəyi barədə hərtərəfli məlumat verir. Əlavə olaraq, İnformasiya Təhlükəsizliyi Risklərinin İdarə Edilməsi qaydaları ISO 270010 (2013) standartını dəstəkləyir və risk qiymətləndirməsinin əsas aspektlərini əhatə edir. |
| **BSI IT** | Əsas Müdafiə Təlimatı - İT sistemləri və normal qorunma tələblərini ödəmək üçün cavabdeh olan məqbul bir təhlükəsizlik səviyyəsinə çatmağı hədəfləyir. |

• informasiya təhlükəsizliyinin məqsədi, informasiya təhlükəsizliyi ilə əlaqəli bütün fəaliyyətlərə rəhbərlik etmək məqsədi və prinsipləri;

• istisnalarla işləmə prosesləri.

Halbuki İSO 27001 (2013) əsasında rəhbərlik informasiya təhlükəsizliyi siyasətini qurmalıdır:

• bankın məqsədi üçün tətbiq edilir;

• informasiya təhlükəsizliyi məqsədlərindən ibarətdir (və ya informasiya təhlükəsizliyi məqsədlərini təyin etmək üçün əsas verir);

• informasiya təhlükəsizliyi ilə əlaqəli müraciətləri yerinə yetirmək üçün istifadə edilir;

• informasiya təhlükəsizliyi idarəetmə sisteminin davamlı genişlənməsinə və yenidən baxılmasına dair öhdəliyi özündə cəmləşdirir.

Daha aşağı səviyyədə, informasiya təhlükəsizliyi siyasəti, informasiya təhlükəsizliyi alətləri və idarəetmə vasitələrinin yerinə yetirilməsini tələb edən və adətən təşkilat daxilində müəyyən hədəf qruplarının ehtiyaclarını ödəmək və ya müəyyən mövzuları əhatə etmək üçün qurulmuş mövzuya aid siyasətlər tərəfindən dəstəklənməlidir. Bundan əlavə, bankın təhlükəsizliyini artırmaq üçün, işçilərin müxtəlif aspektlərini, vəzifələrini, sistemlərin daxilində bank qaynaqlarından ümumi istifadəni və həssas məlumatlara necə nəzarət edilməli olması barədə məlumat verərək ətraflı tətbiq olunan təhlükəsizlik siyasəti haqqında məlumat verilməlidir. Tədqiqatlar göstərmişdir ki, siyasətlərdə məqbul istifadənin məna aspektləri, həmçinin qadağan olunmuş fəaliyyət və ya hərəkətlər göstərilməklə təsvir ediləcəkdir. Əsasən, təhlükəsizlik siyasətinin yaradılması prosesinin əsas səbəbləri bankların informasiya təhlükəsizliyinin əsaslarını müəyyənləşdirmək, kadrlara informasiya aktivlərini qorumaq üçün məsul olduqları barədə izahatlar verməkdir.

ISO 27002, daxili sənəd olaraq, informasiya təhlükəsizliyi siyasətinə dair, idarə heyəti öhdəliyinin olacağını və bankların informasiya təhlükəsizliyi ilə əlaqəli metod və vasitələrini müəyyənləşdirdiyini bildirmişdi. Siyasət aşağıdakı məqamları əhatə edə bilər:

- ümumi məqsədləri və əhatə dairəsi;
- informasiya təhlükəsizliyi prinsiplərinə dəstəyi iş məqsədləri ilə müəyyənləşdirmək;
- nəzarət və məqsədləri nəzərə alan kontur;
- təhlükəsizlik siyasətinin, dəyərlərin, prinsiplərin və konkret mövqenin banka uyğunluq tələblərinin qısa şərhi;
- uyğunsuzluğa görə informasiya təhlükəsizliyi siyasətinin cərimələrinin təyin edilməsi;
- informasiya təhlükəsizliyinin idarə edilməsi üçün ümumi və detallı vəzifələrin təsnifatı;
- banklar, bank işçilərinin yerinə yetirməli olduğu xüsusi məlumat sistemləri və qaydaları üçün digər detallı təhlükəsizlik prosedurlarını və standartlarını müəyyənləşdirməlidirlər.

Siyasətin həyata keçirilməsini, siyasət qaydalarının bütün cəlb olunmuş şəxslər, banklardakı şöbələr tərəfindən effektiv düzgün tətbiq olunduğunu və işçilərin uyğunluğunu yoxlamaq üçün tez-tez yoxlanaraq nəzarət edilməsini təmin etməyi asanlaşdırır. Banklar insidentlərin idarə edilməsini və siyasətin pozulmasını özündə ehtiva edən əlavə metod, vasitə və təlimatlar təyin etməlidirlər. Bundan əlavə, informasiya təhlükəsizliyi siyasətinin yalnız işçilərin təhsili daxil olmaqla düzgün həyata keçirilməklə həyata keçirilə biləcəyini aydınlaşdırmalıdır.

İnformasiya təhlükəsizliyi siyasətinin məqsədi bank işçilərinin davranışlarını tətbiq etmək və dəyişdirməkdir. Digər bir perspektivdə, informasiya təhlükəsizliyi siyasətinin bankın informasiya aktivlərinin məxfiliyini, bütövlüyünü və mövcudluğunu qorumaq və tənzimləmə və əməliyyat daxili tələblərinin nəzərə alınmasına zəmanət verməkdir. Digər tərəfdən banklar informasiya təhlükəsizliyinin idarə edilməsi, məlumatların icazəsiz açıqlanması risklərini azaltmaq üçün təhlükəsizlik texnologiyaları ilə əlaqəli nəzarət və mexanizmlər yaratmağa çalışır. Bununla qarşılaşdıqda, banklarda məlumatların məxfiliyini, bütövlüyünü və əlçatanlığını qorumağa meylli effektiv siyasət, standartlar və tədbirlər sayəsində

səmərəli informasiya təhlükəsizliyi idarəçiliyinə nail olmaq mümkündür. Tədqiqatlar göstərdi ki, müvafiq təhlükəsizlik siyasətinə sahib olmaq üçün bu addımlar nəzərə alınmalıdır.

Təhlükəsizlik siyasətinin formalaşdırıldığı, nəzərdən keçirildiyi, yenidən qurulduğunu və idarə heyəti tərəfindən təsdiq edildiyi bir anda, icra prosesini də informasiya təhlükəsizliyi mütəxəssisləri izləməlidirlər. Bu, adətən siyasətin qurulmasından daha çətin bir hissədir. Bankların bu mərhələdə inamlı şəkildə işləməsi üçün işçilərə təlim keçməlidirlər. Tələb olunur ki, siyasətin təsdiq edilmiş versiyası bankın informasiya aktivlərinə çıxışı olan işçilərə təqdim olunsun. Siyasət istənilən vaxt əlçatan olmalıdır və bankın daxili intranetində yayımlanmalıdır. İnsanların özlərini qorumaları üçün daha məsuliyyətli yanaşma qəbul etmələri üçün, təhlükəsizlik siyasətinin alternativ variantlarını sadə tutaraq insan davranışlarının həqiqətlərini nəzərə almalarını təmin edən mexanizmlərin yaradılması vacibdir. Həm də sürətli texniki dəyişiklik nəzərə alınmaqla, siyasət həlləri də çevik və insanların hesablama vərdişlərindəki dəyişikliklərə uyğunlaşmalıdır. İnformasiya təhlükəsizliyi üçün siyasət sənədləşdirərkən nəzərə alınması lazım olan bəzi addımları təqdim edilməlidir. İdarəetmə prinsipi aşağıdakı hissələrdən ibarətdir:

• bütün informasiya resursları istifadəçilərini məlumatlandırmaq üçün hazırlanan siyasətlər və informasiya qaynaqlarının necə idarə olunacağı və bu mənbələrdən istifadə üçün icraedici rəhbərliyin hansı istiqamətlər təyin etməsi;

• informasiya mənbələri ilə işləyərkən riayət edilməli olan xüsusi məcburi qaydalar və konvensiyalar olan standartlar;

• informasiya mənbələrinin qorunması üçün tətbiq edilməli olan minimum qaydalar və konvensiyalar olan əsaslar;

• standartların necə həyata keçiriləcəyi ilə bağlı bəzi tövsiyələr verən təlimatlar;

• plan, addım və informasiya mənbələrinə necə baxılacağını dəqiqləşdirən prosedurlar.

Standartlar, strategiyalar və əlavə prosedurlar bankda tapılacaq müəyyən intizamın səviyyəsini və yetkinliyini müəyyənləşdirməlidir. Yuxarıda göstərilən təsnifatlardan ümumiləşdirə bilərik ki, banklar üçün informasiya təhlükəsizliyi

siyasətinin tərifi son istifadəçini başa düşməsinin asan olması üçün prosedurlar, standartlar, təlimatlar kimi əlavə sənədləri özündə birləşdirən quruluşdan ibarət olmalıdır.

İT İdarəetmə İnstitutu informasiya təhlükəsizliyi orqanının əhəmiyyətli üstünlüklər yaratdığını müəyyənləşdirmişdir:

• bankın dəyərini artırır;

• proqnozlaşdırılmanı artırır və iş əməliyyatlarının qeyri-müəyyənliyini azaldır;

• quruluş və kontur qeyri-kafi təhlükəsizlik mənbələrinin paylanmasını yaxşılaşdırır;

• effektiv informasiya təhlükəsizliyi siyasətinin və uyğunluğun təmin edir.

İnformasiya təhlükəsizliyi siyasəti məlumatların bütövlüyünə, mövcudluğuna və məxfiliyinə toxunur. Effektiv maneə törətmək üçün bunlar vacib şərtdir. Həmçinin işçilərin məlumat təhlükəsizliyinə diqqət yetirməli olduqlarını nümayiş etdirir. İnformasiya təhlükəsizliyinin həyata keçirilməsinin faydaları riskin təsirinin azaldılması ilə əlaqədardır. İnformasiya təhlükəsizliyi ümumiyyətlə bankın nüfuzunu artırır. İnformasiya təhlükəsizliyi siyasəti yenilənmiş yaxud təsirli sənəd olmalıdır və rəhbərliyi tərəfindən dəstəklənməlidir.

İS informasiyanın toplanması, saxlanması, emalı və ötürülməsi üçün ayrılmış bir komponentlər toplusudur.İnformasiya sistemlərinin 2 tipi var:

• Ümumi təyinatlı informasiya sistemi (General purpose information system):

İnformasiya sisteminin bəzi ümumi növləri var. Məsələn verilənlər bazasının idarəetmə sistemi (DBMS) məlumatların təşkili və təhlilini mümkün edən proqram və məlumatların birləşməsidir. Verilənlər bazası idarəetmə sisteminin proqram təminatı adətən müəyyən bir təşkilat və ya müəyyən bir analiz növü ilə işləmək üçün nəzərdə tutulmamışdır.

• Xüsusi təyinatlı informasiya sistemi (Specialized information system) :

Bunun əksinə olaraq bir təşkilat daxilində müəyyən prosesi dəstəkləmək və ya çox spesifik analiz tapşırığını yerinə yetirmək üçün xüsusi olaraq hazırlanmış bir sıra ixtisaslaşdırılmış informasiya sistemi mövcuddur. Misal: Müəssisə resurslarının

planlaşdırılması (ERP) (bütün təşkilat daxilində informasiya sisteminin idarə edilməsini birləşdirmək üçün istifadə olunur).

İnternet texnologiyası və desktop kompüter standartları ilə rəqabət təcrübəsi təklif edə bilən ağıllı telefon cihazlarının sayı sürətlə artır. Mobil cihazların təhlükəsizliyi və məxfiliyinə dair narahatlıq laptop üçün oxşar narahatlıqlardan kənara çıxır və ya mobil cihaz mahiyyətcə daha mobildir və bir təşkilat tərəfindən idarə olunma ehtimalı azdır. Təhlükəsizliyi təmin etmək üçün ən azı aşağıda göstərilən xidmətləri göstərmək lazımdır.

**1.** Avtorizasiya: Bir şəxsin (həqiqiliyini təsdiq edən) bir hərəkəti həyata keçirmək hüququnun olub olmadığını müəyyənləşdirmək üçün istifadə olunan vasitədir.

**2.** Audit**:** Nəyin səhv olduğunu və nəyin səhv getdiyini müəyyən etmək üçün istifadə edilə bilən fəaliyyət tarixini təmin edən bir audit xidmətidir.

**3.** Fiziki identifikasiya: Buna smart kart, barmaq izi, əlin həndəsi ölçüsü vasitəsilə girişi misal göstərə bilərik.

**4.** Məlumatların məxfiliyi: Keçid zamanı hər hansı bir informasiyanın açıqlanmasından qoruyur və informasiyanın şifrələnməsi ilə təmin olunur.

İnformasiya Sisteminin Təhlükəsizliyi və ya INFOSEC, kompüterlərin, şəbəkələrin və data ilə əlaqəli olan hər şeyin qorunmasını təmin etmək üçündür. Texnologiyanın inkişafı ilə informasiyaların böyük şəbəkələrdə saxlanılması ondan sui-istifadə edə bilən kibercinayətkarlardan qorumaq bir o qədər vacibdir. Hər bir təşkilatın fəaliyyətinə dair məxfi informasiyaları özündə əks etdirən datalar yığını vardır.

İstifadəçilərin maraqlarını qorumaq və lazım olduqda onlara lazımi miqdarda informasiya vermək təşkilatın yeganə məqsədidir. Həm də eyni zamanda, heç kimin informasiya əldə edə bilməməsi üçün lazımi təhlükəsizliyi təmin etmək lazımdır. İnformasiya təhlükəsizliyi və əlçatanlığın mükəmməl tarazlığının qorunmasına ehtiyac ondan ibarətdir ki, informasiya təhlükəsizliyi heç vaxt mütləq ola bilməz.

İnformasiyaya pulsuz giriş təmin etmək zərərli ola bilər və əlçatanlığı məhdudlaşdırmaq çətin olacaq. Bu səbəbdən həm istifadəçilərin, həm də

təhlükəsizlik mütəxəssislərinin xoşbəxt olması üçün tələb olunan tarazlığı qorumaq lazımdır.

İS təhlükəsizliyini maksimum dərəcədə təmin etmək üçün müxtəlif təşkilatlar tərəfindən istifadə edilə bilən bir neçə vasitə var. Bununla birlikdə, bu vasitələr mütləq təhlükəsizliyə zəmanət vermir, lakin yuxarıda qeyd edildiyi kimi, məlumat əldə etmə və təhlükəsizlik arasında əhəmiyyətli bir balans yaratmağa kömək edir.

1. İdentifikasiya.Təhlükəsizliyin təmin edilməsinin vacib prosesinə başlamazdan əvvəl yadda saxlanması lazım olan ən vacib vasitədir.İdentifikasiya prosesi sistemin bir və ya birdən çox amili olan birini müəyyənləşdirməsidir. Bu amillər istifadəçilərin əksəriyyəti üçün unikal olmalıdır. Məsələn, şəxsiyyət vəsiqəsinin nömrəsi və şifrə kombinasiyaları, üz tanıma, barmaq izi və s. göstərə bilərik. Bu amillərə həmişə etibar etmək olmur çünki bunlar itirilə bilər yaxud hər hansı bir kənar şəxs tərəfindən əldə edilə bilər. Bu şərtlər üçün yuxarıda göstərilən amillərdən birini və ya daha çoxunu birləşdirərək eyni anda birdən çox amillərdən istifadə edə bilərsiniz.

2. Girişə Nəzarət (Access Control).Doğru şəxsin informasiya əldə etməsini təmin etdikdən sonra yalnız ona icazə verilən informasiyaları oxuya yaxud redaktə edə bilər. Girişə nəzarət alətindən istifadə edərək sistem hansı istifadəçinin müəyyən məlumatları oxumaq, yazmaq və ya dəyişdirmək imkanına malik olmasına qərar verir. Bunun üçün bütün istifadəçilərin siyahısını saxlayır. Siyahının iki növü var:

- Access Control List (ACL) – Girişə Nəzarət Siyahısı .Bu yalnız məlumat əldə etmək imkanı olan insanların siyahısıdır.
- Role - Based access Control List (RBAC) - bu siyahı səlahiyyətli işçilərin adlarından və onların hansı hüquqlara malik olduğunu göstərən siyahıdır.

3. Şifrələmə (Encryption).Bəzən məlumatlar internet üzərindən ötürülür, buna görə hər kəsin daxil olma riski artır.Bunun qarşısının alınması üçün güclü vasitələr olmalıdır. Bu ssenaridə, məlumatlar asanlıqla hər kəs tərəfindən əldə edilə və dəyişdirilə bilər. Bunun qarşısını almaq üçün yeni bir vasitə işə salınır. Bu şifrələmədir. Şifrələmədən istifadə edərək məxfi informasiyanı oxunmayan

simvolların yığımı vəziyyətinə salmaq olar və yalnız informasiyanı səlahiyyətli qəbuledicilər asanlıqla oxuya bilər [13].

# II FƏSİL. BANK SEKTORUNDA İNFORMASİYA MÜHAFİZƏ VASİTƏLƏRİNDƏN İSTİFADƏ

## 2.1. Banklarda kibermühafizənin rolu

Hər kəs kibertəhlükəsizliyin faydaları və bunun nə üçün hər bir internet istifadəçisi üçün vacib olduğunu bilməlidir. Kiber təhlükəsizlik və ya internet təhlükəsizliyi özünü kompüter cinayətlərindən qoruyur və istifadəçiyə şəxsi yaxud məxfi məlumatların verilməsində təhlükəsizlik pozuntularının riskini azaldır. Kiber cinayətin normal həyatımıza təsirini azaltmaq və bunun qarşısını almaq üçün mübarizə etməliyik. Dünyanın texnologiya dövrü ilə inkişaf etdiyi bir vaxtda internet istifadəçilərinin sayı kəskin şəkildə artır və bu istifadəçilərin əksəriyyəti uşaqlardır. Bu, son bir neçə ildə kiber təhlükəsizliyin pozulmasının səbəblərindən biridir.

Artıq bu mövzu ilə əlaqəli bir neçə cinayəti misal göstərə bilərik:

- Phishing;
- Internet Scams;
- Malware

Yuxarıda göstərilən 3 təhdid, kiber təhlükəsizliyin tələb və əhəmiyyətini bilmək üçün bəzi səbəblərdəndir. Mavi balina oyunu və davam edərkən yaratdığı təhdidlər barədə eşitmisinizmi? Bu oyun sosial media, sürətli mesajlaşma saytları , tətbiqləri və kompüterlərdə yaxud dizüstü kompüterlərdə veb kameralar istifadəsi yolu ilə həyata keçirildi. İstifadəçilər naməlum bir mənbəyə istinadən bir keçid açdıqdan sonra hack olunurlar. Sonra istifadəçilərə sərt təlimatlara əməl etmələri bildirilir əgər etməsələr pis nəticələrin olması ilə hədələyirdilər. Bunu etməklə kiber cinayətkar istifadəçinin sahib olduğu hər şeyi əldə edə bilər. Bu bir insana həm zehni, həm də fiziki cəhətdən ciddi zərər verə bilər. Kibertəhlükəsizlik internetdən istifadə edən hər kəs üçün vacib bir tələbdir. Son bir neçə ildə kibercinayətlə əlaqəli bir çox

hadisə olmuşdur. Bu işlər ümumiyyətlə AHTCC (Avstraliya Yüksək Texnologiyalar Cinayət Mərkəzi), Childnet və s. kimi təşkilatlar tərəfindən həll edilir.

Kiber sistem təhlükəsizliyi adı etibarı ilə sistemi kiber hücumlardan, zərərli hücumlardan qorumağı təklif edir. Sistemin təhlükəsizliyini inkişaf etdirmək üçün sistemə kiber cinayətkarın icazəsiz girişinin qarşısı alınmalıdır. Bugünkü dünyada, kiber cinayətkar hər hansı bir sistemin təhlükəsizliyini pozmaq üçün daha inkişaf etmiş olduğu üçün, təhlükəsizliyi inkişaf etdirmək istifadəçinin məsuliyyətindədir çünki kiber cinayətkarın istifadəçiyə problem yaradan məlumatları istismar edə bilər.

Məsələn, Hindistanda 200-dən çox veb sayta , o cümlədən Sərhəd Təhlükəsizliyi Qüvvələrinin veb saytına Banqladeşli bir qrup tərəfindən hücum edilmişdir. Başqa bir misal, Nyu Yorkdakı su elektrik stansiyasına , İrandakı elektrik şəbəkəsinə edilən hücumlardır. Bu hücumlar çox böyük və bütün dünya üçün təhlükə idi. Bu hücumlar böyük ölçüdə ölkənin təhlükəsizliyini ciddi dərəcədə təhdid edirdi.

Kompüter təhlükəsizliyinin təhlükəsizliyi məxfilik, bütövlük, mövcudluq kimi üç hədəfdən asılıdır. Bu hədəflər əsasən kiber cinayətkar tərəfindən təhdid olunur. Anti-casus proqramı, antivirus və firewall kimi məlumatları qorumaq üçün müxtəlif proqramlar mövcuddur. Sistemdə Intrusion Detection Sistemi, kriptoqrafiya, rəqəmsal imza kimi hücumlardan qorumağa kömək edəcək digər təhlükəsizlik sistemləri mövcuddur.

Kibertəhlükəsizlik və informasiya təhlükəsizliyi terminləri çox vaxt bir-birini əvəz edir. Hər ikisi bir-birilə çox sıx bağlıdır, çünki təhlükəsizlik və kompüter sistemini təhdidlərdən və məlumat pozuntularından qorumaq üçün məsuliyyət daşıyırlar.Çox vaxt kibertəhlükəsizlik və informasiya təhlükəsizliyini sinonim hesab edirlər. Data təhlükəsizliyi dedikdə datanın pis niyyətli istifadəçilərdən və təhdidlərdən qorunması başa düşülür. İndi başqa bir sual budur ki, data və informasiya arasındakı fərq nədir? Beləliklə, bir vacib məqam ondan ibarətdir ki, “hər data informasiya ola bilməz”. Məsələn, "100798" datadır və əgər bir insanın doğum tarixi olduğunu bilsək, o zaman bu informasiyadır çünki bunun müəyyən bir mənası var. Belə ki, informasiya müəyyən mənaya malik olmalıdır.

Kompüter sisteminin təhlükəsizliyi vacib məsələdir. Kiber sistem təhlükəsizlik adlı sistem sistemi kiberhücumlardan və zərərli hücumlardan qorumağı təklif edir. Sistemin təhlükəsizliyini inkişaf etdirmək üçün sistemi cinayətkarın icazəsiz girişindən qorumaq lazımdır.Bunun üçün təhlükəsizlik tətbirlərindən istifadə etmək lazımdır.

Fiziki **.** Kompüter sistemləri olan saytlar silahlı və zərərli müdaxilələrə qarşı fiziki olaraq qorunmalıdır. Xüsusilə də iş stansiyaları diqqətlə qorunmalıdır.

İnsan**.** Sistemə daxil olmaq üçün yalnız müvafiq istifadəçilərin icazəsi olmalıdır.

Əməliyyat sistemi. Sistem özünü təsadüfi və ya məqsədyönlü təhlükəsizlik pozuntularından qorumalıdır.

Şəbəkə sistemi**.** Demək olar ki, bütün informasiyalar şəbəkə vasitəsilə müxtəlif sistemlər arasında paylanır. Bu informasiyaları tutmaq, kompüterə girmək qədər zərərli ola bilər. Ümumiyyətlə, şəbəkə bu cür hücumlara qarşı düzgün şəkildə qorunmalıdır.

Virus qanuni proqrama daxil edilmiş bir kod parçasıdır. Virus özünü çoxaldır və digər proqramları yoluxdurmaq üçün hazırlanmışdır. Sistem qəzalarına və proqram çatışmazlığına səbəb olan faylları dəyişdirmək və ya məhv etməklə sistemə zərər verə bilərlər. Hədəf maşına çatdıqda virus damcısı (ümumiyyətlə trojan atı) virusu sistemə təqdim edir.

Müxtəlif virus növləri:

1. Fayl Virusu: Bu tip virus, sistemin özünü faylın sonuna əlavə edərək yoluxdurur. Proqramın başlanğıcını dəyişdirir, beləliklə nəzarət kodu daxil olur. Kodun icrasından sonra nəzarət əsas proqrama qayıdır. Hətta onun icrası da nəzərə çarpmır. Hər hansı bir sənədin təsirsiz qalmadığı üçün parazitar virus adlanır.

2. Makro Virus**:** Aşağı səviyyəli dildə (məsələn, C və ya yığma dili) yazılmış virusların əksəriyyətindən fərqli olaraq, Visual Basic kimi yüksək səviyyəli dildə yazılmışdır. Bu viruslar makros işlədə biləcək proqram işlədildikdə işə düşür. Məsələn, makro virus elektron tablo sənədlərində tapıla bilər.

**Kibertəhlükəsizlik və informasiya təhlükəsizliyi arasındakı fərqlər** **Cədvəl 2.1.**

| **Kiber təhlükəsizlik** | **İnformasiya təhlükəsizliyi** |
|---|---|
| • Məlumatların internetdəki mənbədən kənarda qorunması praktikasıdır. | • Bu, məlumatların icazəsiz istifadəçi girişindən və informasiyanın dəyişdirilməsindən,məxfiliyindən, bütövlüyündən və mövcudluğundan qorunması ilə bağlıdır. |
| • Söhbət kiber hücumlardan kiber sahənin istifadəsinin qorumaq bacarığından gedir. | • Datanın hər hansı bir təhlükə formasından qorunması ilə məşğul olur. |
| • Kiber aləmdə hər şeyi qorumaq üçün kiber təhlükəsizlik lazımdır. | • İnformasiya təhlükəsizliyi ətraf aləmdən asılı olmayan informasiya üçündür. |
| • Kiber təhlükəsizlik kiber sahəyə qarşı gələn təhlükə ilə əlaqəlidir. | • İnformasiya təhlükəsizliyi dataların hər hansı bir təhlükə formasından qorunması ilə məşğul olur. |
| • Kiber təhlükəsizlik kiber cinayətlərə, kiber fırıldaqçılara qarşı yönəlir. | • İnformasiya təhlükəsizliyi icazəsiz giriş, açıqlamanın dəyişdirilməsinə və pozulmasına qarşı yönəlir. |
| • Digər tərəfdən kiber təhlükəsizlik mütəxəssisləri qabaqcıl davamlı təhdidlə məşğul olurlar. | • İnformasiya təhlükəsizliyi üzrə mütəxəssislər, təhdidləri həll etməzdən əvvəl mənbələrə üstünlük verən data təhlükəsizliyi və təhlükəsizlik üzrə mütəxəssislərdir. |
| • Sosial media hesabını qorumaq, şəxsi məlumatları və s. kimi kiber aləmdə ola biləcək və ya olmaya biləcək təhdidlərdən bəhs edir. | |

3. Mənbə kodlu virus: Mənbə kodu axtarır və onu virusun tərkibində saxlamağı və yayılmasını təmin etmək üçün əvəz edir.

4. Polimorf Virus**:** Virus imzası bir virusu (virus kodunu təşkil edən bir sıra baytlar) müəyyən edə biləcək nümunədir. Buna görə antivirus tərəfindən aşkarlanmaması üçün bir polimorf virus hər dəfə quraşdırıldıqda dəyişir. Virusun funksionallığı eyni qalır, lakin imzası dəyişir.

5. Şifrələnmiş virus: Bu cür viruslar antivirus proqramı tərəfindən aşkarlanmaması üçün şifrəli formada olur. Özü ilə deşifrələmə alqoritmi daşıyır. Beləliklə, virus əvvəlcə şifrəni açır və sonra həyata keçirir.

6. Gizli virus: Çox çətin bir virusdur çünki aşkar etmək üçün istifadə edilə bilən kodu dəyişdirir. Buna görə virusun aşkarlanması çox çətin olur. Məsələn, oxu sistemi zəng dəyişdirə bilər ki, istifadəçi virus dəyişdirilmiş kodu oxumağı istədikdə yoluxmuş kodun əvəzinə orijinal kod formatı göstərilir.

7. Tunel virusu: Bu virus özünü kəsici işləmə zəncirinə yükləyir və antivirus skaner tərəfindən aşkarlanmağı kənara qoymağa çalışır.Əməliyyat sistemi fonunda saxlanılan və tutulan virus tunel virusu zamanı yarasız olur.

8. Boot sektoru virusu: Sistem açıldıqda və əməliyyat sistemi yüklənmədən əvvəl sistemin açılış sektoruna yoluxan zaman yerinə yetirilir. Ayrıca disketlər kimi digər önyüklenebilir medianı da yoluxdurur. Bunlar yaddaş sisteminə aiddir, çünki fayl sisteminə yoluxmur.

9. Çoxtərəfli virus: Bu tip virus sistemin çox hissəsini, o cümlədən boot sektorunu, yaddaşı və faylları yoluxdura bilər. Bu, aşkarlanmağı və tutmağı çətinləşdirir.

10. Zirehli virus**:** Antivirusun açılmasını və başa düşülməsini çətinləşdirmək üçün zirehli bir virus kodlaşdırılır. Antivirusun başqa bir yerdə olduğuna inanmaq və ya kodunu çətinləşdirmək üçün sıxılma istifadə etmək kimi müxtəlif üsullardan istifadə edir [14].

## 2.2. Mühafizə vasitələrinin ümumi xarakteriskaları

İnformasiya təhlükəsizliyi internetin bank sektorlarında tətbiqi zamanı daha vacibdir.Bank və maliyyə xidmətlərində yüksək təhlükəsizlik tələbi həm problemlər, həm də yeni iş imkanları yaradır.İnformasiya təhlükəsizliyi təşkilatın fəaliyyət göstərməsi üçün vacib olan məlumatları emal edən və saxlayan, sistemlərini, media vasitələrini qoruduğu və təmin etdiyi bir prosesdir.Maliyyə qurumları və banklar, məlumatların risklərini müəyyənləşdirən, riskləri idarə etmək üçün strategiya hazırlayan, strategiyanı tətbiq edən, testləri həyata keçirən və riskləri idarə etmək üçün mühiti izləyən təhlükəsizlik prosesi quraraq məlumatlarını qoruyurlar.

Maliyyə qurumları və banklarda informasiya təhlükəsizliyi mövcudluq, bütövlük, məxfilik, hesabatlılıq və təminat kimi müəyyən məqsədlərə çatmaqla artırıla bilər. Təhlükəsizlik məqsədlərinə təhlükəsizlik risklərinin qiymətləndirilməsi, strategiya, nəzarətlərin tətbiqi, monitorinq və proseslərin monitorinqi yaxud yenilənməsi ilə nail olmaq olar.

Mobil telekommunikasiya texnologiyasının iş dünyasına geniş yayılması ilə mobil bankçılıq son zamanlarda bank sektorunda populyar və perspektivli bir bank üsulu halına gəlib. Mobil bankçılıq müştərilərə daha keyfiyyətli və daha qənaətli xidmətlər təqdim edə bilər. Bu, mobil telekommunikasiya qurğularının köməyi ilə bank və maliyyə xidmətlərinin göstərilməsinə və istifadəsinə aiddir. Təqdim olunan xidmətlərin əhatə dairəsinə bank və investisiya bazarlarında əməliyyatların aparılması, hesabların idarə edilməsi və xüsusi məlumatların əldə edilməsi imkanları daxil ola bilər.

Mobil bank tədqiqatçılarının əksəriyyəti mobil bankçılığın üç hissədən ibarət olduğunu qəbul etdilər: mobil mühasibat, mobil broker və mobil maliyyə məlumat xidmətləri. Müştəri xidmətləri sektoruna daxildir: balans yoxlanılması, hesab əməliyyatı, ödəniş və s. şərti bank xidmətləri. Getdikcə, bank müştəriləri, dünyanın harasında olursa olsun, həftədə yeddi gün, 24 saat real vaxt məlumat əldə edəcəklər. Elektron hesabın idarə edilməsi, mobil broker və maliyyə məlumatları və siqnallar kimi xidmətlər banklara və şəbəkə operatorlarına bankın rəqabət qabiliyyətini artırmağa və gücləndirməyə imkan verir.

Mobil bank sistemi mobil bank vahidi və bank əməliyyatlarının emalı və məlumatların saxlanması üçün cavabdeh olan əsas bank kompüteri ola bilən məlumat emalı mərkəzini əhatə edir. Mobil bankçılığa bankomatlar, depozit maşınları və multimedia sorğu stansiyaları kimi bir və ya bir neçə bank terminalı daxildir. Mobil bank sistemi, bir sıra simsiz rabitə kanallarını özündə cəmləşdirən, fərqli texnologiyaların mahiyyətlərini özündə cəmləşdirən, fərdi, müştəri yönümlü, yeni maliyyə xidmətlərinin təqdim edilməsi üçün yaxşı bir zəmin yaratdı.

Ən vacib texnologiyalara aşağıdakılar daxildir: Kriptoqrafiya, Steganografiya, PKI (açıq açar infrastrukturu), elektron imza, elektron sertifikat, təhlükəsizlik

protokolları, doğrulanma protokolları, firewall, giriş idarəetmə modelləri, şifrələr, rəqəmsal zərf, bioloji təhlükəsizlik texnologiyaları, filtrləmə, giriş təsbit sistemləri.

Ümumiyyətlə, böyük beynəlxalq bank qrupları Risk Landşaftını və mövcud təhlükəsizlik sxemlərini yaxşı başa düşdüklərini nümayiş etdirdilər. Bir çox şirkət İnformasiya Təhlükəsizliyi İdarəetmə Sistemini (İSMS) izləyir və təhlükəsizlik idarəetməsinin bir hissəsi olaraq standartlar və idarəetmə çərçivələrini qəbul edir. Təhlükəsizliklə bağlı reseptlər əsasən milli qaydalarda bildirilir və ya sektor daxili strategiyaları ilə müəyyən edilir. Bəzi üzv dövlətlərdə sənayenin maraqlı tərəfləri yüksək səviyyəli təhlükəsizlik və uyğunluq strategiyaları dərc edir və mərkəzi bankının planlaşdırdığı təlimlərdə iştirak edirlər. Orta ölçülü maraqlı tərəflər yüksək səviyyəli idarəetməyə cəlb olunmağı, mövcud beynəlxalq standartlara uyğun sertifikatlaşdırılmaq üçün məhdud imkanları və təhlükəsizlik investisiyalarının prioritetləşdirilməsini nümayiş etdirir. Vəziyyətin bu cür fərqi yeni deyil, eyni zamanda maliyyə sektoruna da aid deyil. Məqsəd, bu cür perspektivlərin ümumilikdə maliyyə dayanıqlığına zərər verə biləcəyini anlamaqdır.

Maliyyə sektorunun quruluşu ümumilikdə mürəkkəbdir. Təhdidlər və potensial zəif cəhətlər iş növü və qəbul olunan təhlükəsizlik modelinə görə dəyişir: məsələn, İnvestisiya bankları və ya yüksək tezlikli ticarət (HFT) fəaliyyətlərində informasiya təhlükəsizliyinin davamlı və balanslı təmin edilməsini təmin etməkdə çətinliklə üzləşə bilərlər. Müştəri ilə əlaqəli operatorlar sürətlə inkişaf edən texnoloji mühitlə əlaqəli risklərə daha çox məruz qala bilərlər. Digər tərəfdən, texnoloji mühit sürətlə dəyişərkən biznes və maliyyə xidmətləri mənzərəsi də sürətlə inkişaf edir (məs: yeni rəqiblər, inkişaf etməkdə olan bazar modelləri və s.). Bu meyllərin birləşməsi mürəkkəblik dərəcəsinə təsir göstərir.

Maliyyə təşkilatlarının əsas missiyası müştəriləri sevindirmək və asan pul əməliyyatlarında kömək etməkdir. Bunlara aşağıdakılar aiddir:

- Maliyyə sisteminə inamı qorumaq və onu təmin etmək;
- Maliyyə sistemi haqqında məlumatlılığın və ictimaiyyətin anlaşılmasının təşviqi;
- İstehlakçıları qorumaq üçün müdafiəni lazımi səviyyədə təmin etmək;

- Maliyyə cinayətlərinin və bank kabuslarının azaldılması
- İnternet bankçılığın bir çox faydası var. Ən vaciblərindən ikisi sürət və rahatlıqdır. İnternet bankçılıqda iştirak edən insanlar hesablarına daxil ola, hesabatlarına baxa, əməliyyatlar edə, ödəmələr edə bilər və s. Məhz bu üstünlüklərə görə ABŞ-ın təxminən 70 faizi internet bankçılıqda iştirak edir. Bununla birlikdə, internet bankçılığın üstünlüklərinə baxmayaraq, internet bank sektorunda bir sıra fərqli problemlər də mövcuddur. Bunlar həm internet bankçılıq təklif edən banklar üçün, həm də bankların səmərəli fəaliyyət göstərməsindən asılı olan müştərilər üçün olduqca əhəmiyyətlidir.
- İnternet bank marketoloqları bu çətinlikləri bilməlidirlər ki, onları səmərəli idarə edə bilsinlər. Marketoloqların bilməli olduğu internet bank sektorundakı ən vacib problemlər bunlardır:
- Ənənəvi bank vərdişləri. İnternet bankçılığın faydalarına baxmayaraq, amerikalı yetkinlərin 30 faizi ümumiyyətlə iştirak etmir. Bu, ənənəvi bankçılıq bir çox insanın alışdıqları və vərdişlərini pozması üçün vaxt tələb edə biləcəyi səbəbindən baş verir. Beləliklə, onlayn bank marketinqçiləri ənənəvi bank istifadəçilərini onlayn bank xidmətlərindən istifadə etməyə başlamağa inandırmaq yollarına diqqət yetirməlidirlər. Bu marketinq səyləri, internet bankçılığın çoxsaylı faydalarını xüsusilə vurğulamalıdır. İnternet bankçılığın ənənəvi bank problemlərini daha səmərəli şəkildə necə həll edə biləcəyini insanlara göstərməlidirlər.
- Təhlükəsizlik. Təhlükəsizlik onlayn bank marketoloqlar üçün ən vacib problemlərdən biridir. Keçmişdə soyğunçunun bank əmanətlərini oğurlaması üçün, fiziki olaraq banka girməli və ordan qaçmalı idi. Bu, olduqca çətin perspektiv idi və bir çox təhlükə və risk tələb edirdi. İnternet bankçılıqda isə kibercinayətkarlar sadəcə şəxsin hesabına girmək və pullarını oğurlamaq üçün müəyyən şəxsi məlumatları müəyyənləşdirməlidirlər. Bu anonim olaraq edilə bilər və əvvəlkindən daha az fiziki təhlükə ehtiva edir. Əslində 2015-ci ildə ABŞ-da, fırıldaqçılıq yolu ilə internet bank hesablarından təxminən 130 milyon ingilis funtu oğurlanmışdı. Beləliklə, təhlükəsizlik hələ də internet banklar və onların müştəriləri üçün əsas məsələdir. Onlayn bank sektorundakı marketinq mütəxəssisləri bu çətinliyi aradan qaldırmaq

üçün onlayn bankların təhlükəsizliyini nümayiş etdirməyə və izah etməyə diqqət yetirməlidirlər [18].

- Əməliyyat çətinliyi. İnternet bankına pul yatırmaq və ya pul götürmək xeyli çətin və uzun vaxt tələb edə bilər. Nəinki onlayn banklarda ənənəvi banklara nisbətən daha az ATM var, həm də əmanətlərin işlənib bank hesabına qoyulması üçün daha uzun vaxt tələb olunur. Məsələn, ən böyük onlayn banklardan biri olan PayPal hesablarında əmanətlərin göstərilməsi təxminən 3-5 gün çəkir.
- Texniki məsələlər. Banklar öz onlayn platformalarına etibar etməlidirlər çünki, əks halda sistemləri çökdükdə və ya kodlarında səhvlər olduqda ciddi itki verə bilərlər. Bir gündə bankın aşağı düşməsinə səbəb olan texniki problem, banka milyonlarla itki verə bilər. Saytın nasaz olduğu müddətdə ödənişlər edə və ya əməliyyat keçirə bilməyən bank müştəriləri üçün problem yarana bilər. İndi istehlakçıların 54 faizi mobil bankçılıq tətbiqindən istifadə edir. Beləliklə, bankların yalnız onlayn platformalarının rahat işləməsi deyil, həm də mobil tətbiqetmələrinin olması vacibdir. Qəza səbəbiylə vəsait və ya məlumat itkisi, bank müştərilərinin çox narahat olacaqları bir şeydir. Beləliklə, marketoloqlar texniki problemlər yaranarsa hesabdakı vəsaitin necə itiriləcəyini izah edərək bu narahatlığı azaltmağı üstün tutmalıdırlar.

Kibercinayət və ya kompüter yönümlü cinayət, kompüter və şəbəkəni əhatə edən bir cinayətdir. Kompüter cinayətin icrasında istifadə edilmiş ola bilər və ya hədəf ola bilər. Kiber cinayət-fırıldaqçılıq, şəxsiyyət oğurluğu və ya məxfiliyin pozulması kimi cinayətlərin törədilməsi üçün kompüterdən silah kimi istifadə edilməsidir. Kompüter ticarət, əyləncə və hökumət kimi hər bir sahənin mərkəzi halına gəldiyindən İnternet vasitəsilə kiber cinayətlərin əhəmiyyəti artmışdı. Kiber cinayət insan və ya xalqın təhlükəsizliyinə və maddi sağlamlığına təhlükə yarada bilər. Kibercinayətkarlıq geniş fəaliyyət sahələrini əhatə edir lakin bunları ümumiyyətlə iki kateqoriyaya bölmək olar:

- Kompüter şəbəkələrini və ya cihazlarını hədəf alan cinayətlər. Bu növ cinayətlərə virus, bug və DoS hücumları aiddir.

- Digər cinayət əməllərini həyata keçirmək üçün kompüter şəbəkələrindən istifadə edən cinayətlər aiddir.

Kibercinayətlərin təsnifatı aşağıdakı kimidir:

1. Kiber Terrorizm.Kiber terrorizm, insanların həyatını itirməsi ilə nəticələnən zorakılıq aktlarını həyata keçirmək üçün kompüter və internetdən istifadəsidir. Buraya vətəndaşların həyatını təhdid edən proqram və ya avadanlıqla müxtəlif fəaliyyət növləri daxil ola bilər. Ümumiyyətlə, kiber terrorizm kiberməkanda və ya kompüter resurslarından istifadə etməklə törədilən terror aktı kimi müəyyən edilə bilər.

2. Kiber qəsb.Kiber qəsb veb saytın, e-poçt serverinin və ya kompüter sisteminin zərərli xakerlər tərəfindən dəfələrlə xidmətdən və ya digər hücumlardan məruz qaldığı və ya təhdid edildiyi zaman baş verir. Bu xakerlər hücumların dayandırılması və qorunması üçün böyük pul tələb edirlər.

3. Kiber müharibə.Kiber müharibə, kompüterlərin, onlayn idarəetmə sistemlərinin və şəbəkələrinin bir döyüş məkanında və ya müharibə şəraitində istifadəsi yaxud hədəf alınmasıdır.

4. İnternet saxtakarlığı.İnternet fırıldaqçılığı, internetdən istifadə edən və qənaət etmək yaxud pul qazanmaq üçün qurbanları aldatmaq üçün saxta məlumatlar təqdim edən bir fırıldaqdır. İnternet fırıldaqçılığı tək və fərqli bir cinayət sayılmasa da, kiber məkanda bir sıra qanunsuz əməlləri əhatə edir.

5. Kiber İzləmə.Bu, qurbanların onlayn mesajlar və e-poçtlarına maneə törətdiyi bir növ onlayn təcavüzdür. Bu, onlayn təcavüzün bir formasıdır, burada qurbanın onlayn mesajı və e-mail bəndinə məruz qalmasıdır. Bununla birlikdə, kiber izləmə istənilən nəticəni vermədiyini görsələr, qurbanların həyatlarını daha acınacaqlı hala gətirmək üçün kiber izləmə ilə oflayn izləməyə başlayırlar.[16]

Kiber cinayətin qarşısının alınması:

1. Güclü parol istifadəsi.Hər bir hesab üçün şifrə və istifadəçi adlarının fərqli birləşmələrini yaradın və onları yazmaq istəyinə qarşı durun. Zəif şifrələr, Brute güc hücumu, Rainbow masa hücumu və s. kimi hücum metodlarından istifadə edərək asanlıqla qırıla bilər.

2. Cihazlarda etibarlı antivirusdan istifadə edilməsi.Həmişə mobil və fərdi kompüterlərdə etibarlı və yüksək inkişaf etmiş antivirus proqramlarından istifadə etmək lazımdır. Bunlar, cihazlara müxtəlif virus hücumlarının qarşısını alırlar.

3. Sosial medianın gizli saxlanması.Həmişə sosial media hesablarındakı məlumatların məxfiliyini dostlardan belə qorumaq lazımdır.

4. Cihazın proqram təminatının yenilənməsi.Sistem proqram təminatı yeniləmələrini hər dəfə əldə etdiyiniz zaman eyni anda yeniləyin çünki bəzən əvvəlki versiyaya asanlıqla hücum edilə bilər.Kiber cinayət hüquq mühafizə orqanları tərəfindən çox ciddi qəbul edilir. Kiber təhlükəsizlik dünyasının erkən dövrlərində standart kibercinayətkarlar bir ev noutbukundan işləyən yeniyetmələr idi. Bu gün kibercinayətkarların planeti təhlükəli hala gəldi. Cinayətkarlar şəxsi və ya maddi mənfəət üçün zəifliklərdən istifadə etməyə çalışan şəxslər və ya komandalardır [17].

## 2.3. Bank işçilərinin autentifikasiyası və istifadəçilərin identifikasiyası üçün mühafizə vasitələrinin tətbiqi

Banklar autentifikasiya prosesinə çox ciddi yanaşmalı olan təşkilatlardır. Banklar müəyyənləşdirilmiş kritik informasiyaların anbarıdır. Bu informasiyalar ola bilər: sosial təminat nömrələri, fiziki ünvanlar, telefon nömrələri, e-poçt ünvanları, hesab nömrələri, kredit tarixləri, məşğulluq tarixləri və təşkilatın müştərilərinə və işçilərinə aid digər məlumatlar. Bank binalarının özü ilə əlaqəli fiziki təhlükəsizliyi də unudulmamalıdır. Fiziki təhlükəsizlik yoxdursa, texniki onlayn identifikasiya metodlarına ehtiyac da yoxdur. Sənədli prosedurlar və çoxsaylı müdafiə xətləri bankın fiziki əmlakını təmin etmək üçün vacibdir. Əmlakın qorunması üçün görülən tədbirlər, təşkilatın ehtiyaclarından asılı olaraq çox dəyişəcəkdir. Kritik məlumatlar və ya dəyərli əşyaları olan yerlərdə daha çox təhlükəsizlik tədbirləri tələb olunur. Texniki ehtiyatların təhlükəsizliyinə gəldikdə, sənədləşdirilmiş prosedurlar mövcud

olmalıdır və işçilər üçün əlçatan olmalıdır.Banklarda bir çox təhlükəsizlik tədbirləri olmalıdır. Müəssisənin quruluşundan kənar bütün əmlak yaxşı işıqlandırılmalı və təhlükəsizlik əməkdaşları, gözətçi köpəklər və ya sadə təhlükəsizlik kameralarından faydalana bilər. Bütün bina girişlərində düzgün kilidləmə mexanizmləri olmalıdır.

AAA autentifikasiya, avtorizasiya və hesabat (bəzən giriş nəzarətləri, doğrulanma, hesabat deyilir) mənasını verən bir qisimdir. AAA modeli istifadəçi girişi üzərində nəzarəti qorumaq üçün yaradılmışdır. Kimin hansı mənbələrə, nə vaxt və nə vaxta qədər istifadə edə biləcəyini göstərir. AAA bina girişi və ya mürəkkəb kompüter şəbəkə sistemlərində əsas formalarda həyata keçirilə bilər. Belə bir modelin səbəbi, təşkilatların etibarlı istifadəçilər üçün mənbələrə girişi məhdudlaşdırmasıdır.

Autentifikasiya metodları bir neçə əsas kateqoriyaya bölünə bilər. Onlar birbaşa istifadəçi ilə əlaqəli bir neçə şeydən biri ola bilər. Əsasən, bu istifadəçinin bildiyi bir şey, istifadəçinin sahib olduğu bir şey, istifadəçinin davranış tərzi və ya istifadəçinin fiziki xüsusiyyətləridir. Aşağıdakı autentifikasiya metodları vardır:

Parollar. Yəqin ki, istifadəçi identifikasiyasının ən əsas forması istifadəçi adı və parol birləşməsidir. Bu identifikasiya növü olduqca zəifdir. Onun istifadəsi getdikcə daha çox problem yaradır. Autentifikasiyanı təsdiqləmək üçün şifrələrdən istifadə etmək sadə fikirdir. İstifadəçiyə bənzərsiz identifikator təyin edilməli və bu identifikatorla əlaqələndirmək üçün istifadəçiyə şifrə qeyd etməsini tələb etmək lazımdır. İdarəetmə də olduqca sadədir. Demək olar ki, bütün kompüter sistemlərində şifrələri idarə etmək üçün quraşdırılmış proqramlar mövcuddur. İstifadəçi identifikatorları və şifrələr bütün prosesi insan girişinin yeganə mənbəyi kimi istifadəçi ilə tamamlamağa imkan verən verilənlər bazasında saxlanıla bilər. Şübhəsiz ki, bu texnika ilə bir çox problem müəyyən edilə bilər. İstifadəçi adı və şifrə birləşmələrində insan psixologiyasından irəli gələn bəzi qüsurlar var. Məsələn, şifrələr yadda saxlamalı və sürətli identifikasiyanı təmin etmək üçün kifayət qədər asan olmalıdır. Buna görə də bir çox insan parollarını fiziki olaraq qeyd etmək ehtiyacını hiss edir. Bundan əlavə, texnologiya artdıqca parolları hədəf alan

hücumların həyata keçirilməsi asanlaşır. Yüksək güclü kompüterlər, şifrə əldə etmək üçün lüğət və kobud zorakılıq hücumlarını başlatmağı olduqca səmərəli edir.

PIN kod. Şəxsi identifikasiya nömrəsi (PIN) parol kimi eyni şəkildə istifadə edilə bilər. Bu format parol kimi gizli olmalıdır. PİN koddan ən çox istifadə avtomatik bankomat (ATM) üçün istifadə olunur. Ən çox PİN kodlar 0000-9999 aralığında 4 rəqəmli nömrələrdir ki, nəticədə 10000 mümkün nömrələr olur ki, təcavüzkarın düzgün PİN kodu əldə etməsi üçün ortalama 5000 dəfə təxmin etməsi lazımdır. Lakin bu problem yaradır. Xakerin PİN kodu tapmağa çalışması, statistik hesablamalara görə müəyyən vaxt tələb olunur. Amma kompüter vasitəsilə bu vaxt daha da azalır. Buna görə bir PİN tətbiq edən sistemlərin əksəriyyəti kilidləmə xüsusiyyətinə malikdir. İstifadəçi və ya başqası səhv PIN-i əvvəlcədən müəyyən edilmiş saydan çox daxil edərsə, sistem administratoru hesabı yenidən aktivləşdirənə qədər istifadəçi hesabı kilidlənəcəkdir.

Müəyyən oluna bilən şəkil (Identifiable Picture). Əl qurğularının istifadəsi və şifrələr yaxud fərdi identifikasiya nömrələri ilə bağlı problemlərin təşviqi ilə yeni identifikasiya forması meydana çıxdı. Şifrə və ya PIN-nin əvəzinə şəkillərdən istifadə etmənin ideyası istifadəçilərin şəkil tanıdıqları halda şifrəni tanımasıdır. Bu, sistemə birdən çox şəkil göstərməyə və istifadəçiyə hesaba girişi təmin edən düzgün şəkil tanımağa imkan verir. Tədqiqatlar sübut etdi ki, bu identifikasiya metodu xakerin düzgün identifikasiya açarını tapmaq və şifrəni düzgün yazmaq qabiliyyətini azalda bilər. Bəzi banklar şəkilləri identifikasiya sistemlərinin bir hissəsi kimi birləşdirməyə başlayır.

Birdəfəlik parollar (One time password). Başqa bir metod birdəfəlik şifrədir. Şifrə heç vaxt ümumi şəbəkə üzərindən keçməməsi istisna olmaqla, əsas istifadəçi adı və şifrə birləşməsinə çox oxşardır. RFC 2289 birdəfəlik parol identifikasiyası üçün üsul izah edir. Bu sistem müştəri generatoru və server istifadə edir. Əsasən, generator istifadəçidən gizli bir şifrə qəbul edir və onu autentifikasiyanı idarə etmək üçün serverdən göndərilən məlumatlarla əlaqələndirir. Bu tip sistem, əsas şifrə sistemlərinin həssas olduğu passiv hücumlardan qoruya bilər.

Sürüşdürmə kartları (Swipe Card). Müasir bankçılıqla maraqlanan hər kəs ümumi maqnetik sürüşdürmə kartı ilə tanışdır. Buna nümunə kimi debet yaxud kredit kartını misal göstərmək olar. Maqnetik sürüşdürmə kartları kiçikdir və istifadəçinin şəxsiyyəti haqqında məlumat saxlayan maqnit zolaqdan ibarətdir. Bu identifikasiya növü, PİN kimi digər identifikasiya üsulları ilə birlikdə istifadə edilə bilər. Kart özü oğurluğa meylli olduğundan yetərli təsdiqləmə vasitəsi deyil. Kartdakı məlumatlar müvafiq avadanlıq vasitəsi ilə çoxalda bilər. Bu o deməkdir ki, üçüncü tərəf eyni məlumatı olan bir kart yarada və istifadə edə bilər.

Proximity Card. Proximity kartı maqnetik sürüşdürmə kartları ilə eyni şəkildə çalışır ancaq satıcıdan satıcıya dəyişən məsafədən çalışır. Kartda kartı saxlayan şəxsin müəyyən bir mənbəyə və ya qapıya girmək səlahiyyətinə malik şəxs olduğunu təsdiqləyəcək məlumatlar mövcuddur. Həmin şəxs sadəcə kartı kart oxuyucusunun yanında yerləşdirir və məlumat simsiz mübadilə olunur. Bu tip kartlardan universitetlər də daxil olmaqla banklarda geniş istifadə olunur.

USB token. USB tokenlər plastik kartlara çox bənzəyirlər. Token istifadəçinin şəxsiyyəti haqqında məlumatı ehtiva edir və istifadəçinin qorunan mənbələrə daxil olma üsuluna xidmət edir. USB token kompüterin məlumat əldə etmək üçün kompüterin USB portuna qoşulmalıdır. Çox vaxt proqram qurğularında lisenziyalaşdırma məlumatları saxlanıla bilər. Bu, hüquqi və maliyyə qeydlərinin aparılmasını asanlaşdırır. İstifadəçilərin sahib olduğu digər identifikasiya elementləri kimi, USB tokenlərini itirmək, oğurlamaq və ya qırmaq olar.

Nitq identifikasiyası (Speech) - istifadəçi identifikasiyası üçün müasir bir yanaşmadır. Səs identifikasiyası aparatı və proqram təminatının birləşməsi banka telefon, divarda quraşdırılmış cihaz və ya internet vasitəsilə istifadəçilərin şəxsiyyətini yoxlamağa imkan verə bilər. Səs identifikasiyası bir insanın səsini - vokal traktının fiziki xüsusiyyətlərini və harmonik və rezonanslı tezliklərini özündə cəmləşdirir və qeydiyyat prosesi zamanı yaradılan səsli səs yazısı ilə müqayisə edir. Bu o deməkdir ki, istifadəçinin əvvəlcədən sistemdə saxlanmış səs yazısı vardır. Kompüter həmin istifadəçinin səsinin fərqli xüsusiyyətlərini hesablayır və məlumatları saxlayır. İstifadəçi doğrulamaq istədikdə, ilk qeyddə istifadə olunan

əvvəlcədən təyin edilmiş bir söz danışır. Kompüter səs nümunələrinin uyğun olub olmadığını və həmin hesablamalar əsasında müəyyənləşdirə bilər, mənbəyə giriş verə və ya rədd edə bilər. Bu identifikasiya metodunun çatışmazlığı ondan ibarətdir ki, istifadəçidə şiddətli laringit varsa, sistem istifadəçinin səsini tanımaya bilər.

İmza identifikasiyası(Signature) - istifadəçini təsdiqləmək üçün başqa bir üsuldur. İstifadəçilər ya sistemdən istifadə etməzdən əvvəl imzalarını qeydiyyata almalı və ya fəal şəkildə istifadə etməlidirlər. Hazırda imza identifikasiyası fırıldaqçılığı azaltmağa və iş proseslərini asanlaşdırmağa kömək edən aparıcı banklarda və digər maliyyə qurumlarında yerləşdirilib. Artıq imza identifikasiyasından bəhrələnən digər sahələrə hökumət, tibb, telekommunikasiya, enerji, aviasiya, silahlı qüvvələr və hüquq sahələri daxildir. Banklar gündəlik olaraq çox sayda sənəddəki imzaları yoxlamalıdırlar.

Klaviatura ritm identifikasiyası (Keyboarding Rhythm). Bu gün bir çox iş klaviaturanın istifadəsini tələb edir. Buna görə də klaviatura ritm identifikasiyası iş yerinə asanlıqla quraşdırıla bilər. Klaviatura ritm identifikasiyası insanın yazma texnikasına aid bir neçə fərqli xüsusiyyətləri ölçməklə həyata keçirilə bilər. Düymə vuruşları, tuş vuruşlarının uzunluğu, barmaq mövqeləri və düymələrə tətbiq olunan təzyiq miqdarı bu istifadəçiyə bənzərsiz bir şəxsiyyət yaratmaq üçün birləşdirilə bilər. İstifadəçinin identifikasiyası üçün lazım olan yeganə cihaz identifikasiya sisteminə qoşulmuş standart klaviaturadır. Bu identifikasiya metodu gələcək tətbiqlərdə dərin üstünlüklərə malik ola bilər.

Barmaq izi (Fingerprint). Bu gün biometriyadan faydalanan bir çox fərqli identifikasiya cihazı mövcuddur. Bu üsul biometriyanı "bioloji müşahidələrin və hadisələrin statistik təhlili" olaraq təyin edir. Onların hər birinin faydaları və çatışmazlıqları var. Ən etibarlı identifikasiya üsullarına çox faktorlu biometrik prosedurlar daxildir. Biometrik xüsusiyyətləri saxtalaşdırmaq çətindir, çünki hər bir şəxs irsiyyət əsasında unikal fiziki xüsusiyyətlərə malikdir.

Yer üzündə heç bir insanın eyni barmaq izi yoxdur. Eyni şəxs üçün hətta hər barmağın fərqli bir çizgiləri var. Bu, əkiz olan insanlara da aiddir. Bu səbəbdən barmaq izi identifikasiyası istifadəçiləri fərqləndirmək üçün əla yoldur.

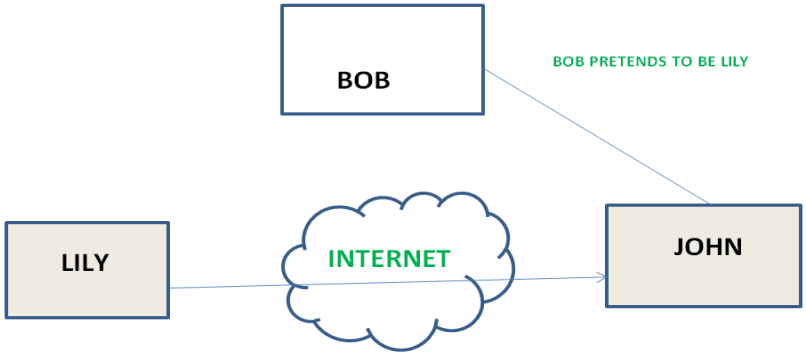
İstifadəçilərin əvvəlcə barmağın kompüter sisteminə skan etməsini tələb edilir. Bu istifadəçinin fayldakı bənzərsiz barmaq izi ilə, identifikasiyanın zəruri olduğu nöqtələrdə yerləşdirilə bilər. İstifadəçi daha sonra barmağını biometrik oxucuya yaxınlaşdırır. Sistem, barmaq izləri arasındakı oxşarlıqları yoxlayır və müəyyən bir həddən yuxarı və ya aşağı olduqda girişə icazə verir və ya rədd edir. Bu sistemin üstünlüyü ondan ibarətdir ki, istifadəçi hər zaman şəxsiyyəti təsdiqləmə vasitələrinə sahibdir. Daha əvvəl deyildiyi kimi digər bir üstünlük bütün barmaq izlərinin unikal olmasıdır. Barmaq izlərini saxtalaşdırmaq və ya yenidən yaratmaq demək olar ki, mümkün deyil. Bu texnologiyanın çatışmazlığı ondan ibarətdir ki, bəzi insanların barmaq izlərinin olmamasıdır. Yanıq qurbanlarının ümumiyyətlə barmaq izləri olmaya bilər.

Əl ölçülü identifikasiya (Hand Geometry). Əl həndəsi biometrik skanerlər, avtorizasiyanın əsaslandığı insan əlinin xüsusiyyətlərini ölçən cihazdır. Barmaq izləri kimi, hər bir insanın əlində barmaq uzunluğu, eni və qalınlığı fərqlidir. Əl skaneri, istifadəçinin əlini yoxlamaq üçün cihaz, infraqırmızı işıq və işıq yayan diodlardan istifadə edir. Cihaz iki tərəfdən - yuxarı və yan tərəfdən ölçmə aparmaq üçün güzgülərdən istifadə edir. Yetkinlərin əl ölçüləri nadir hallarda dəyişir. Əllərdə yaralanma saxta mənfi halların baş verməsinə səbəb ola bilər. Barmaq izi skanerləri ilə müqayisədə divarda quraşdırılmış yoxlama cihazı daha böyük olacaqdır.

Göz tanıma identifikasiyası (Iris scanners). Iris skanerləri istifadəçilər arasında gözün xüsusiyyətlərini ölçərək fərqləndirir. Bu iris çoxlu kollagen liflər, daralma kökləri, koronalar, kriptlər, rəng, serpantin damarlığı, soyma, qırıqlar, qırışlar və çuxurlardan ibarətdir. Bu xüsusiyyətlərin bir-birlərinə fəza əlaqələrinin ölçülməsi şəxsiyyət prosesi üçün faydalı olan digər ölçülən parametrləri təmin edir. Digər biometrik üsullar kimi, istifadəçi əvvəlcə gözünü sistemə skan etməlidir. İstifadəçi daha sonra mənbələrə daxil olmaq üçün divarda quraşdırılmış yoxlama cihazlarından istifadə edə bilər. İnformasiya təhlükəsizliyində kiber hücumlar aktiv və passiv olaraq 2 hissəyə bölünür.Aktiv hücumlar: aktiv hücumlar sistem qaynaqlarını dəyişdirməyə və ya əməliyyatlarına təsir etməyə çalışırlar. Aktiv

hücum data ötürülməsində bəzi dəyişikliklər edilməsini yaxud yanlış ifadələrin yaradılmasını ehtiva edir. Aktiv hücumların növləri aşağıdakılardır:

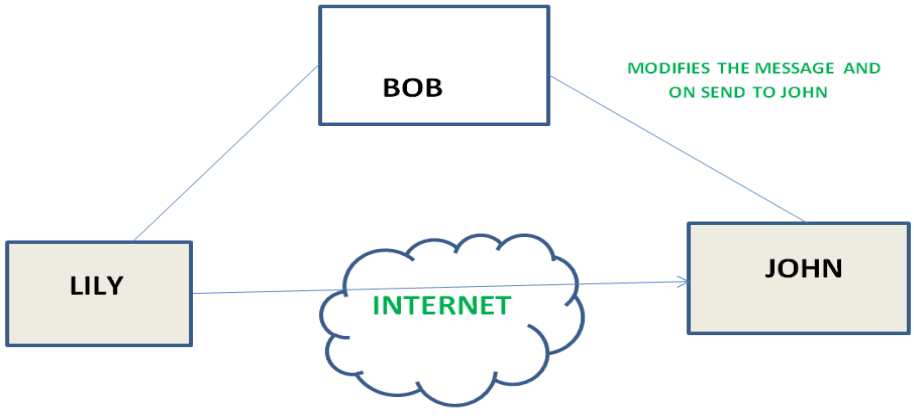
Masquerade – Maskarad hücumu, bir varlığın özünü başqa bir varlıq kimi aparması zamanı baş verir.




**Şəkil 2.1 Maskarad hücumunun qısa məzmunu**

Yuxarıdakı sxemdə Bob özünü Lily kimi apararaq John ilə əlaqə yaradır.

Mesajların dəyişdirilməsi – mesajın bir hissəsinin dəyişdirildiyini və ya icazəsiz bir effekt vermək üçün mesajın gecikdirildiyini yaxud dəyişdirildiyini göstərir. Məsələn, "JOHN-a məxfi X sənədini oxumağa icazə verin" mənasını verən bir mesaj "Bob-a məxfi sənəd X oxumağa icazə ver" olaraq dəyişdirilir.

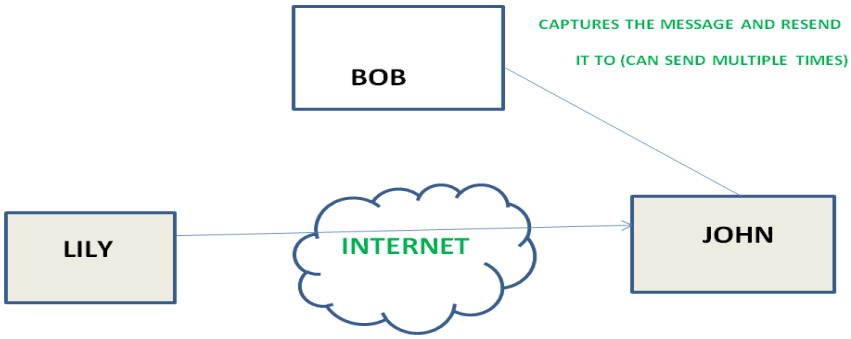



**Şəkil 2.2 Mesajların dəyişdirilməsinin qısa məzmunu**

Təkzib (Repudiation) –Bu hücum ya göndərici ya da qəbuledici tərəfindən edilir. Göndərən və ya qəbul edən şəxs sonradan mesaj göndərdiyini və ya aldığını

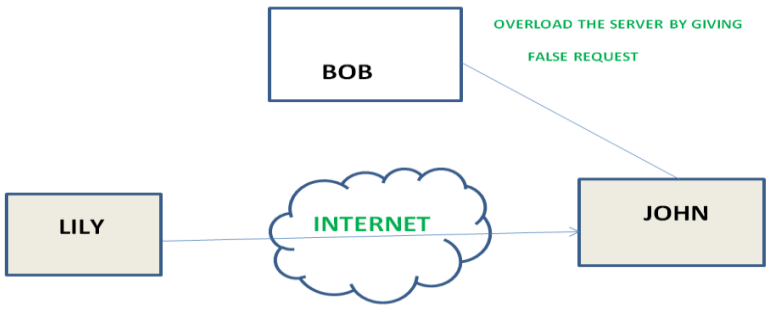
inkar edə bilər. Məsələn, müştəri bankından “Birinə pul köçürməsini” xahiş edir və sonra müştəri belə bir tələb etdiyini rədd edir. Bu təkzibdir.

Təkrar (Replay) – Mesajın passiv tutulmasını və səlahiyyətli bir effekt vermək üçün sonradan ötürülməsini əhatə edir.




**Şəkil 2.3 Mesajların təkrar göndərilməsinin qısa məzmunu**

Xidmətin rədd edilməsi (Denial of Service) –Rabitə vasitələrinin normal istifadəsinə mane olur. Bu hücumun müəyyən bir hədəfi ola bilər. Məsələn, müəssisə müəyyən bir yerə yönəldilmiş bütün mesajları bağlaya bilər. Xidmətdən imtinanın başqa bir forması, şəbəkəni söndürmək və ya işini pisləşdirmək üçün mesajlarla həddən artıq yükləməklə bütün bir şəbəkənin sıradan çıxmasıdır.

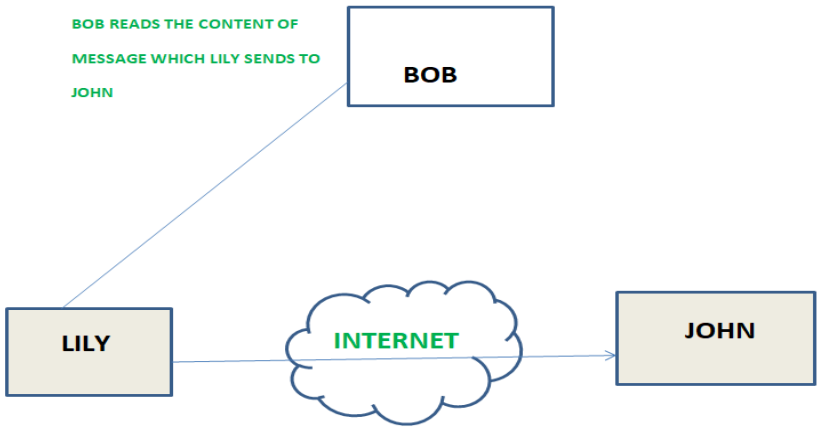



**Şəkil 2.4 Xidmətin imtina edilməsinin qısa məzmunu**

Passiv hücumlar: Passiv hücum sistemdən məlumat əldə etməyə və ya istifadə etməyə çalışır lakin sistem qaynaqlarına təsir etmir. Passiv hücumlar trafikə qulaq

asmaq və ya ötürülməsini izləmək xarakterindədir. Rəqibin məqsədi məlumat əldə etməkdir. Passiv hücumların növləri aşağıdakılardır:

Mesaj məzmununun buraxılması –Telefon danışıqları, elektron poçt mesajı və ya ötürülən sənəd həssas və ya məxfi məlumatları ehtiva edə bilər. Rəqibin bu ötürmələrin məzmununu öyrənməsinə mane olmaq şərtdir.




**Şəkil 2.5 Mesajların məzmunun buraxılmasının qısa məzmunu**

Trafikin analizi – Tutaq ki, kiber cinayətkarın mesajı ələ keçirsə də, mesajdan heç bir məlumat ala bilməməsini təmin edən şifrələmə metodumuz var. Cinayətkar ünsiyyət quran tərəfin yerini və kimliyini müəyyənləşdirə və mübadilə edilən mesajların tezliyini və uzunluğunu müşahidə edə bilər. Bu məlumat baş verən əlaqənin təbiətini tapmaqda faydalı ola bilər.

# III FƏSİL. BANKLARDA İSTİFADƏÇİ HESABININ MÜHAFİZƏSİ MODELİNİN TƏDQİQİ

## 3.1. Simmetrik və asimmetrik şifrələmə

Kriptoqrafiya, yalnız informasiyaları nəzərdə tutulan şəxsin başa düşə və emal edə bilməsi üçün kodlardan istifadə edərək informasiya və kommunikasiya təmin etmək texnikasıdır. Bununla da informasiyanın icazəsiz əldə edilməsinin qarşısı alınır. "Crypt" sözü "gizli" , “graphy” şəkilçisi isə "yazı" deməkdir. Bu alqoritmlər kriptoqrafik açar, rəqəmsal imza, məlumatların məxfiliyini qorumaq üçün və autentifikasiya, kredit yaxud debet kart əməliyyatları kimi məxfi əməliyyatları qorumaq üçün istifadə olunur.

İndiki kompüter əsrində kriptoqrafiya çox vaxt adi düz mətnin şifrələmə mətninə çevrildiyi proseslə əlaqələndirilir; bu mətn, nəzərdə tutulan alıcının yalnız şifrələməsini və bu səbəbdən şifrələmə olaraq bilinməsini təmin edən mətndir. Şifrəli mətnin düz mətnə çevrilməsi prosesi deşifrələmə kimi tanınır.

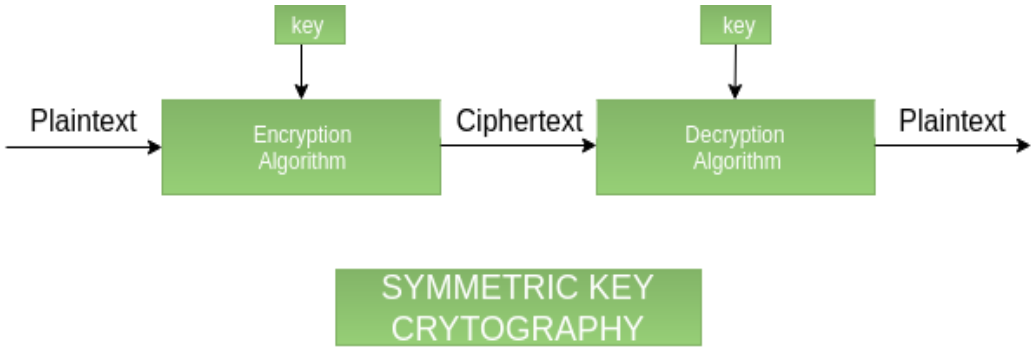
Kriptoqrafiyanın xüsusiyyətləri aşağıdakılardır:

- Məxfilik: İnformasiya yalnız nəzərdə tutulan şəxs tərəfindən əldə edilə bilər və ondan başqa heç kim onu əldə edə bilməz.
- Bütövlük: İnformasiyanın göndərən və qəbul edən arasında hərəkəti zamanı heç bir halda redaktə edilə bilməz.
- İnkar edilə bilməmək: İnformasiya yaradan / göndərən şəxs sonrakı mərhələdə informasiya göndərmək niyyətini inkar edə bilməz.
- İdentifikasiya: Göndərənin və alıcının şəxsiyyətləri təsdiqlənmişdir. Eləcə də informasiyanın mənşəyi təsdiqlənmişdir.

Ümumilikdə kriptoqrafiyanın 3 növü vardır:

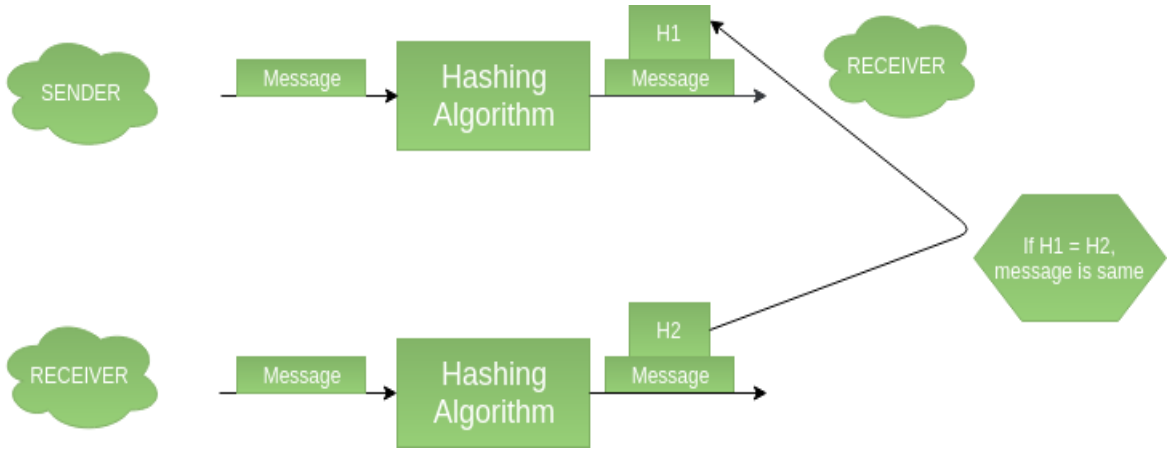
1. Simmetrik açar kriptoqrafiyası. Mesaj göndərən və qəbul edən şəxs mesajların şifrələnməsi və deşifrələnməsi üçün vahid bir açarın istifadə olunduğu

şifrləmə sistemidir. Simmetrik Açar Sistemlər daha sürətli və sadədir lakin problem göndərən və qəbuledicinin açarı etibarlı şəkildə dəyişdirməsidir. Ən populyar simmetrik açar kriptoqrafiya sistemi Məlumat Şifrələmə Sistemidir (DES).




**Şəkil 3.1. Simmetrik açar kriptoqrafiyasının işləmə prinsipi**

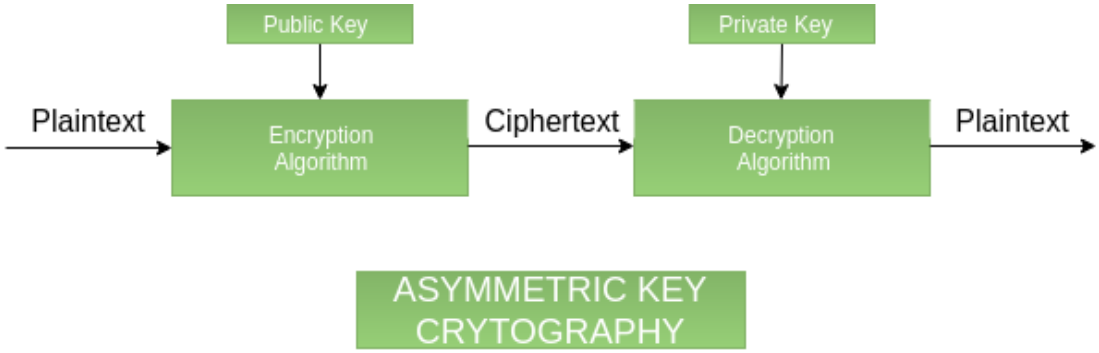
2. Hash funksiyaları. Bu alqoritmdə hər hansı bir açar istifadə edilmir. Sabit uzunluqdakı hash dəyəri düz mətnə görə hesablanır, bu da mətnin məzmununu bərpa etməyi qeyri-mümkün edir. Bir çox əməliyyat sistemi parol şifrələmək üçün hash funksiyasından istifadə edir.




**Şəkil 3.2. Hash funksiyalarının işləmə prinsipi**

3. Asimmetrik açar kriptoqrafiyası: Bu sistemdə informasiya şifrələmək və deşifrələmək üçün 2 ədəd açardan istifadə olunur. Ümumi açar (public key) informasiyanı şifrələmək, xüsusi açar (private key) informasiyanı deşifrələmək üçün istifadə edilir. Ümumi açar və xüsusi açar fərqlidir. Ümumi açarı hər kəs bilsə də

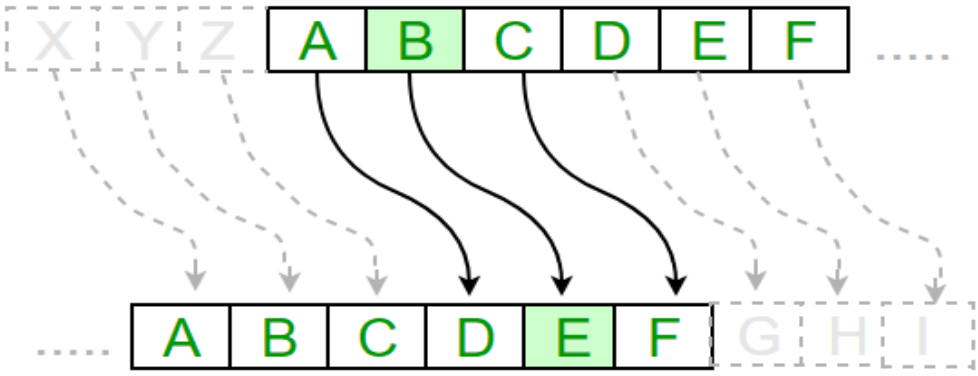
göndərilən məlumatı yalnız nəzərdə tutulan qəbuledici xüsusi açarı olduğuna görə deşifrələyə biləcək.




**Şəkil 3.3 Asimmetrik açar kriptoqrafiyasının işləmə prinsipi**

Klassik kriptoqrafiya. Kriptoqrafiyanın ən qədim istifadəsi standart olmayan heroqliflər şəklində Misirin köhnə krallığı dövründə e.ə. 1900-cü ilə aid edilə bilər. Heroqliflər misirlilərin bir-biri ilə əlaqə qurduğu gizli bir ünsiyyət forması idi. Bu gizli mətn yalnız onun adından mesajlar çatdıran padşahların müəlliflərinə məlum idi. Qədim yunanlar şifrlərin istifadəsi ilə məşhur idilər. Sezar şifrələməsi ən erkən və sadə tanınmış kriptoqrafiya texnikalarından biridir. Bu, bir sözdəki hər bir simvolun müəyyən sayda mövqe ilə əvəz olunduğu əvəzetmə şifrəsinin bir formasıdır. Məsələn, 3 sürüşmə ilə “A” simvolu “D” ilə əvəz olunur.

Birinci Dünya müharibəsi və II Dünya müharibəsi zamanı müttəfiq qüvvələrin qələbəsində kriptoqrafiya mühüm rol oynadı. İkinci Dünya Müharibəsində elektro-mexaniki şifrə maşınlarından istifadə edilmişdir. Müttəfiqlərin almanlar üzərində dünyaca məşhur Enigma maşınını sındıraraq qalib gəlməsi hekayəsi də məlumdur. Bütün rotor maşınları kimi Enigma da elektro-mexaniki alt sistemlərin birləşməsidir. Üç-beş rotordan ibarət idi.




**Şəkil 3.4 Sezar sifrələmənin işləmə prinsipi**

Data şifrələmə standartı (DES) - 1970-ci illərin əvvəllərində Məlumat Şifrələmə Standartı və ya DES yarandı. Feistel şifrinə əsaslanan simmetrik açar alqoritmdir və elektron məlumatların şifrələnməsi üçün istifadə olunur. Nisbətən kiçik açar ölçüsü 56 bit və 64 bit və ya bir anda şifrələnmiş 8 simvoldan ibarətdir. Lakin sonradan nisbətən kiçik açar ölçüsünün səbəb olduğu güclü hücumlara məruz qaldığına görə istifadəsi azalmışdır.

İnkişaf etmiş şifrələmə standartı (AES) - DES 2001-ci ildə Advance Encryption Standard və ya AES ilə əvəz edildi. DES-dən fərqli olaraq, AES əvəzetmə-permutasiya şəbəkəsinə əsaslanır. AES, Rijndael'in alt dəstidir. Fərqli açar və blok ölçüləri olan şifrələmə ailəsidir. AES vəziyyətində blok ölçüsü 128 bit və ya 16 simvoldur, yəni eyni anda 16 simvol şifrələnə bilər. Üç fərqli açar ölçüsü variantları var: 128 bit, 192 bit və 256 bit.

Şifrələmə normal mesajın (düz mətnin) mənasız mesaja (şifrəli mətn) çevrilməsi prosesidir. Amma deşifrələmə mənasız mesajın (şifrəli mətn) orijinal formasına (düz mətn) çevrilməsi prosesidir.

Şifrələmə hər hansı informasiyanı hər kəs tərəfindən oxumaqdan qorumaq üçün onun formasını dəyişdirmək üçün istifadə olunan prosesdir. Simmetrik açar şifrələmədə informasiya açardan istifadə etməklə şifrələnir və eyni açar həmin informasiyanı deşifrələmək üçün istifadə edilir.Bu istifadəni asanlaşdırır ancaq təhlükəsizlik səviyyəsi aşağı düşür.Digər problem isə açarı bir tərəfdən digərinə ötürmək üçün təhlükəsiz üsuldan istifadə olunmasıdır [25].

**Şifrələmə və deşifrələmənin özünəməxsus xüsusiyyətləri** **Cədvəl 3.1.**

| Şifrələmə | Deşifrələmə |
|---|---|
| 1. Şifrələmə normal mesajın mənasız mesaja çevrilməsi prosesidir. | 1. Deşifrələmə mənasız mesajın (şifrəli mətn) orijinal formasına çevrilməsi prosesidir. |
| 2. Şifrələmə göndərən tərəfdə baş verən sonuncu prosesdir. | 2. Deşifrələmə alıcı tərəfdə baş verən sonuncu prosesdir. |
| 3. Onun əsas vəzifəsi düz mətni şifrəli mətninə çevirməkdir. | 3. Əsas vəzifəsi şifrəli mətni düz mətnə çevirməkdir. |
| 4. Hər hansı mətn ya gizli açar(secret key) ya da açıq açar (public key) ilə şifrələnə bilər. | 4. Şifrəli mətn ya gizli açar (secret key) ya da xüsusi açarla (private key) deşifrələnə bilər. |
| 5. Şifrələmə prosesində göndərən informasiya şifrələdikdən sonra qəbulediciyə data göndərir. | 5. Deşifrələmə prosesində alıcı informasiyanı (şifrəli mətn) alır və düz mətnə çevirir. |

Asimmetrik açar şifrələmə açıq və xüsusi private açar şifrələmə texnikasına əsaslanır. İnformasiyanı şifrələmək və deşifrələmək üçün iki fərqli açardan istifadə olunur.

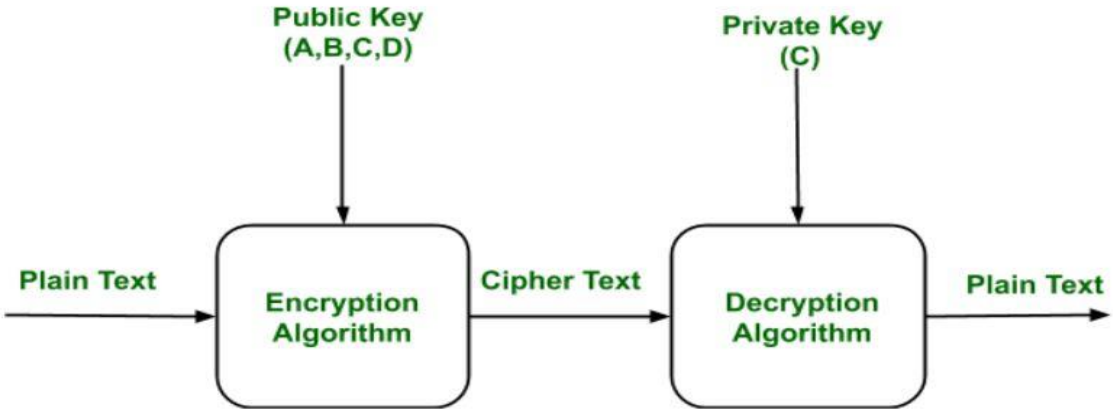
**Simmetrik və asimmetrik açar şifrələmənin fərqləri** **Cədvəl 3.2.**

| Simmetrik açar şifrələmə | Asimmetrik açar şifrələmə |
|---|---|
| 1. Həm şifrələmə, həm də deşifrələmə üçün tək bir açardan istifadə olunur. | 1. İki açar tələb olunur, biri şifrələm digəri deşifrələmək üçün lazımdır. |
| 2. Şifrəli mətnin ölçüsü orijinal düz mətn ilə ya eyni ya da ondan kiçikdir. | 2. Şifrəli mətnin ölçüsü orijinal düz mətn ilə ya eyni ya da ondan böyükdür. |
| 3. Şifrələmə prosesi çox sürətlidir. | 3. Deşifrələmə prosesi yavaşdır. |
| 4. Çox miqdarda data ötürülməsi tələb olunduqda istifadə olunur. | 4. Az miqdarda məlumat ötürmək üçün istifadə olunur. |
| 5. Yalnız məxfiliyi təmin edir. | 5. Məxfilik, autentifikasiya və non-repudiation təmin edir. |
| 6. DES, AES, 2DES,3DES və RC4 | 6. Diffie-Hellman, ECC, El Gamal, DSA və RSA |

Açıq açarda iki açardan istifadə olunur.Bir açar şifrələmə üçün digər açar isə deşifrələmə üçün istifadə olunur.Açıq açar düz mətni şifrəli mətnə çevirmək üçün istifadə olunur.Digər açar isə (xüsusi açar) informasiyanı oxumaq üçün şifrəli mətni deşifrələmək üçün alıcı tərəfindən istifadə olunur. Açıq açar şifrələmənin xüsusiyyətləri aşağıdakılardır:

- Açıq açar şifrələmə vacibdir çünki kriptoqrafik alqoritm və şifrələmə açarı haqqında verilmiş məlumat şifrəni açmaq üçün kifayət etmir.
- İki açardan (açıq və xüsusi açar) biri deşifrələmk üçün digər açar isə şifrələmək üçün istifadə edilə bilər.
- Açıq açar kripto sistemi sayəsində açıq açarlar sərbəst şəkildə bölüşdürülərək istifadəçilərə məzmunun şifrələnməsi və rəqəmsal imzaların yoxlanılması üçün asan və rahat bir üsula imkan verir.Həmçinin xüsusi açarlar gizli saxlanıla bilər, yalnız xüsusi açarların sahibləri məzmunu deşifrəliyə bilər və rəqəmsal imza yarada bilirlər.
- Ən çox istifadə edilən açıq açar kripto sistemi RSA (Rivest-Shamir-Adleman)-dır.

Misal: Hər bir istifadəçinin açıq açarları açıq açar reyestrində mövcuddur. Əgər B məxfi mesajı C-yə göndərmək istəsə, B C-nin açıq açarından istifadə edərək mesajı şifrələyir. C mesajı B-dən aldıqda, öz xüsusi açarından istifadə edərək mesajı deşifrələyə bilər. C-dən başqa heç bir qəbuledici mesajı deşifrələyə bilməz çünki yalnız C-nin şəxsi açarı istifadə edilir.




**Şəkil 3.5 Şifrələmə prosesinə aid misalın təsviri**

Açıq açar şifrələmənin komponentləri:

- Düz Mətn (Plain Text): Bu oxunan və ya başa düşülən mesajdır. Bu mesaj şifrələmə alqoritminə giriş kimi verilir.
- Şifrəli mətn (Cipher Text): Şifrəli mətn şifrələmə alqoritminin nəticəsi olaraq iyaranır. Bu mətn başa düşülən deyildir.
- Şifrələmə alqoritmi: Şifrələmə alqoritmi düz mətni şifrəli mətnə çevirmək üçün istifadə olunur.
- Deşifrələmə alqoritmi: şifrəli mətni giriş xüsusi açar və ya açıq açar istifadə edərək düz mətnə çevirir.

Açıq açar şifrələmənin mənfi cəhətləri:

- Açıq açar şifrələmə güclü hücumlara (Brute-force) həssasdır.
- İstifadəçi xüsusi açarı itirəndə də bu alqoritm uğursuz olur.
- Açıq açar şifrələmə orta dərəcəli hücumlara qarşı təhlükəsiz deyildir.

**Açıq və xüsusi açarların fərqi** **Cədvəl 3.3.**

| **Açıq açar** | **Xüsusi açar** |
|---|---|
| 1. Xüsusi açardan daha yavaşdır. | 1. Xüsusi açar açıq açardan daha sürətlidir. |
| 2. Açıq açarda iki açardan istifadə olunur.Bir açar şifrələmə üçün digər açar isə deşifrələmə üçün istifadə olunur. | 2. Xüsusi açarda eyni açar həm şifrələmək həm də deşifrələmək üçün istifadə olunur. |
| 3. Açıq açar kriptoqrafiyasında iki açardan biri gizli saxlanılır. | 3. Xüsusi açar kriptoqrafiyasında açar gizli saxlanılır. |
| 4. Açıq açar asimmetrikdir çünki iki növ açarı var: xüsusi və açıq açar. | 4. Xüsusi açar simmetrikdir çünki gizli deyilən yalnız bir açarı var. |
| 5. Bu kriptoqrafiyada göndərənin və alıcının eyni açarı paylaşmasına ehtiyac yoxdur. | 5. Bu kriptoqrafiyada göndərənin və alıcının eyni açarı bölüşməsi lazımdır. |

Simmetrik alqoritmlərin istifadəsi ilə bağlı böyük problem açarların dəyişdirilməsi prosesidir. Digər əsas məsələ gizli simmetrik açarı bölüşən iki tərəf arasında etimad məsələsidir. Şifrələmə identifikasiya və bütövlüyə nəzarət üçün istifadə edildikdə güvən problemlərinə rast gəlmək olar.

Açar dəyişmə problemi (The Key Exchange Problem)

Əsas açar problemi, əlaqəli tərəflərin hər hansı etibarlı rabitə başlamazdan əvvəl bir şəkildə gizli açarı bölüşməsindən irəli gəlir və hər iki tərəf də açarın gizli qalmasını təmin etməlidir. Əlbəttə ki, birbaşa açar mübadiləsi risk, əlverişsizlik və xərc amillərinə görə həmişə mümkün olmur.

Tutma-22 analogiyası, hər hansı etibarlı rabitənin başlamazdan əvvəl ortaq açarı necə etibarlı şəkildə əlaqələndirmək məsələsinə aiddir. Bəzi hallarda birbaşa açar dəyişməsi mümkündür. Lakin əvvəllər bir-biri ilə heç vaxt ünsiyyət qurmayan tərəflər arasında bir çox kommersiya məlumat mübadiləsi baş verirdi və əvvəlcədən açar dəyişmə imkanı yox idi. Bu tərəflər tez-tez identifikasiya məqsədləri üçün simmetrik alqoritmlərdən istifadə üçün tələb olunan etimadı yaratmaq üçün bir-birini yaxşı tanımırdılar. İnternetin partlayıcı böyüməsi ilə, əvvəllər heç vaxt ünsiyyət qurmayan tərəflərin bir-biri ilə etibarlı və təsdiq edilmiş qaydada kortəbii şəkildə əlaqə qurmaları tələb olunurdu. Xoşbəxtlikdən, bu məsələni asimmetrik alqoritmlərdən istifadə etməklə səmərəli həll etmək olar.[26]

Etimad problemi (The Trust Problem)-alınan dataların bütövlüyünün təmin edilməsi və həmin data mənbəyinin kimliyini yoxlamaq çox vacib ola bilər. Məsələn, dataların müqavilə yaxud maliyyə əməliyyatı ilə əlaqəli olması halında çox şey təhlükə altına düşə bilər. Müxtəlif dərəcələrdə bu məsələlər hətta adi elektron poçt yazışmaları üçün hüquqi baxımdan vacib ola bilər.

Simmetrik açar, müəyyən bir datalar toplusunu yaradan şəxsiyyətin şəxsiyyətini yoxlamaq üçün istifadə edilə bilər lakin bu identifikasiya sxemi etibarlılıqla əlaqəli bəzi çətin problemlərlə qarşılaşa bilər.

Bu texnikada məlumatlar hash olunur və nəticədə ortaya çıxan hash simmetrik alqoritm ilə paylaşılan gizli açardan istifadə edərək şifrələnir. Gizli açarı da bilən alıcıya datalar şifrəli hash dəyəri ilə birlikdə göndərilir. Alıcı daha sonra paylaşılan

açarı istifadə edərək hash deşifrələyir və nəticədə alınan məlumatlarda hash dəyərinin yenidən hesablanması baş verir.Bunun səbəbi yalnız gizli açarı bilən şəxs alıcının hesabladığı yenidən hesablanmış hash dəyərinə uyğun olmaq üçün orijinal məlumatların hash-u düzgün şəkildə şifrələyə bilər. Bu data mənbəyinin düzgünlüyünü təsdiqləyir. Bu üsul məlumatların bütövlüyünü (integrity) yoxlayır çünki gizli açarı bilməyən hər kəs məlumatlara müdaxilə edə bilər.

Gizli açarın bölüşüldüyü digər tərəfə etimad edilə bilmirsə nə baş verməlidir? Problem ondadır ki, bu sxem ortaq açarı bilən iki şəxs arasında ayrıseçkilik edə bilməz. Məsələn, iki tərəfdən biri paylaşılan açardan istifadə edərək saxta bir mesaj göndərə bilər. Həmçinin ik tərəfdən birinin gizli açarı başqalarına icazəsiz paylaşması digər problemlərə gətirib çıxara bilər. Bütün bunların əsas problemi, hər hansı bir simmetrik alqoritm sxeminin bir tərəfin digər tərəfə etibarlı şəkildə etibar etməsini tələb etməsidir ki, bu da ümumiyyətlə real deyil.

Xoşbəxtlikdən, asimmetrik alqoritmlər eyni əsas əməliyyatları yerinə yetirərək bu problemləri həll etmək üçün istifadə edilə bilər. Sonra hər kəs hashı yoxlamaq üçün əlaqəli açıq açarı istifadə edə bilər. Bu etimad və rədd problemlərini effektiv şəkildə aradan qaldırır.

Müasir simmetrik şifrələmə alqoritmlərinə DES, 3DES, AES, RC4 və RC5 misal göstərmək olar.

DES (Data Encryption Standard) - simmetrik açar blok şifrələmə alqoritmidir. Alqoritm Feistel şəbəkəsinə əsaslanır. Alqoritm 64 bitlik bloklarda məlumatları şifrələmək üçün 56 bitlik bir açardan istifadə edir.DES-in gücü ilə bağlı problemlərin əsasən iki kateqoriyası var:

- İstifadə olunan xüsusi alqoritmlə bağlı problemlər.
- 56 bit ölçülü açarların istifadəsi ilə bağlı problemlər.

İstifadə olunan alqoritmlə bağlı ilk problem DES alqoritminin xüsusiyyətlərindən istifadə etməklə kripto analizin aparılmasıdır. Açar uzunluğu 56 bit olan 2 ^ 56 mümkün sayda açar ola bilər. Bu halda güclü hücum (brute-force) mümkünsüz görünür.

2DES (Double DES)-eyni düz mətndə iki DES nümunəsi istifadə edən bir şifrələmə üsuludur. Hər iki halda da düz mətni şifrələmək üçün müxtəlif açardan istifadə olunur. Şifrənin açılması zamanı hər iki açar tələb olunur. 64 bit düz mətn ilk açarı istifadə edərək 64 bitlik orta mətnə çevrilmiş ilk DES instansiyasına, sonra ikinci açarı istifadə edərək 64 bit şifrələmə mətni verən ikinci DES instansiyasına keçir. Bununla birlikdə ikiqat DES 112 bit açar istifadə edir, lakin 2 ^ 56 deyil 2 ^ 112 təhlükəsizlik səviyyəsini verir və bunun səbəbi ikiqat DES-dən keçmək üçün istifadə edilə bilən orta hücumdur.

3DES (Triple DES)- eyni düz mətndə üç DES nümunəsini istifadə edən bir şifrələmə üsuludur. Orada ilk növbədə istifadə olunan açarların hamısı fərqli, ikincisində isə iki açar eyni və biri fərqli, üçüncüsü isə bütün açarlar eynidır.
3DES də orta səviyyəli hücumda həssasdır, buna görə 168 bit açarı istifadə etmək əvəzinə 2 ^ 112 sayda ümumi təhlükəsizlik səviyyəsini verir. Blok toqquşma hücumu, qısa blok ölçüsü və böyük mətni şifrələmək üçün eyni açarı istifadə edilməsi ilə aparıla bilər.Sweet32 hücumuna qarşı həssasdır.

AES (Advanced Encryption Standard)-indiki dövrdə rast gəlinə biləcək daha populyar və geniş yayılmış simmetrik şifrələmə alqoritmi Advanced Encryption Standard (AES) -dir. 3DES-dən ən az altı dəfə daha sürətli tapılır. Açar ölçüsü çox kiçik olduğundan DES başaqa bir alqoritmlə əvəz edilməli idi. Artan hesablama gücü ilə, tükənən açar axtarış hücumuna təhlükəsiz olmadığına qərar verilmişdir. 3DES bu çatışmazlığı aradan qaldırmaq üçün hazırlanmışdı lakin tapma sürəti yavaş idi. AES-in xüsusiyyətləri aşağıdakılardır:

- 3DES-dən daha güclü və daha sürətlidir;
- 128 bitlik datalar və 128/192/256 bit açarları vardır;
- Tam spesifikasiya və dizayn məlumatları təmin edir;
- C və Java-da tətbiq oluna bilir.

AES, Feistel şifrələməsindən daha iterativdir. Bu "əvəzetmə - permutasiya şəbəkəsi" -nə əsaslanır. Bu, bir sıra əlaqəli əməliyyatlardan ibarətdir, bunlardan bəziləri girişləri xüsusi çıxışlar (əvəzetmə) ilə əvəz etmək, digərləri isə ətrafdakı qarışıq bitləri (permutasiyalar) əhatə edir.

**AES və DES arasındakı fərqlər** **Cədvəl 3.4.**

| AES | DES |
|---|---|
| 1. AES inkişaf etmiş şifrələmə standartıdır. | 1. DES dataların şifrələmə standartıdır. |
| 2. Açar uzunluğu 128 bit, 192 bit və 256 bit ola bilər. | 2. Açar uzunluğu DES-də 56 bitdir. |
| 3. Dövrlərin sayı açarların uzunluğundan asılıdır: 10 (128 bit), 12 (192 bit) və ya 14 (256 bit). | 3. DES –də dövrlərin sayı standart olaraq 16-dır. |
| 4. Struktur əvəzetmə-permutasiya şəbəkəsinə əsaslanır. | 4. Struktur Feistel şəbəkəsinə əsaslanır. |
| 5. AES, DES şifrələməsindən daha etibarlıdır və faktiki olaraq dünya standartıdır. | 5. DES, məlum zəifliklər olduğu üçün asanlıqla qırıla bilər. 3DES adi DES-dən daha etibarlı olan DES-in dəyişməsidir. |
| 6. AES-dəki dövrlər bunlardır: bayt əvəzləmə (byte substitution), shift sırası (shift row), qarışıq sütun (mix column) və açar əlavə (key addition). | **6.** DES-dəki dövrlər bunlardır: expansion, dövri açar ilə XOR əməliyyatı, əvəzetmə və permutasiya. |
| 7. AES 128 bit düz mətni şifrələyə bilər. | 7. DES 64 bit düz mətni şifrələyə bilər. |
| 8. AES şifrəsi kvadrat şifrələmədən əldə edilir. | 8. DES şifrəsi Lusifer şifrələmədən əldə edilir. |
| 9. AES, Vincent Rijmen və Joan Daemen tərəfindən hazırlanmışdır. | 9. DES, IBM tərəfindən tərtib edilmişdir. |
| 10. AES-ə qarşı məlum kripto-analitik hücumlar mövcud deyil, lakin AES tətbiqlərinə qarşı bəzi hücumlar mümkündür. Biclique hücumu güclü hücumdan daha yaxşı bir mürəkkəbliyə malikdir lakin hələ də təsirsizdir. | 10. DES-ə qarşı məlum hücumlar bunlardır: güclü hücum (brute-force), xətti kripto-analizlər və diferensial kripto-analizlər. |

Bu gün ki, kriptoqrafiyada AES həm aparat, həm də proqram təminatında geniş qəbul edilir və dəstəklənir. Bu günə qədər AES-ə qarşı praktik kripto analitik hücumları aşkar edilməmişdir.

Mənfi cəhətləri:

AES çox sadə açar cədvəli və sadə şifrələmə əməliyyatlarına malikdir. Bir çox AES hücumu bu əsas cədvəlin sadəliyinə əsaslanır və bir gün AES şifrələməsini qırmaq üçün hücum yaradılması mümkündür.

RC4-RSA-nın yaradıcısı Ronald Rivest tərəfindən hazırlanmış bu alqoritm, ortaq bir açarın etibarlı mübadiləsi tələb olunan ortaq açar axını şifrəsi alqoritmidir. RC4 axın şifrəsi və dəyişən uzunluq açar alqoritmidir. Bu alqoritm eyni anda bir bayt (və ya birdən çox ədəd) şifrələyir. RC4 şifrələmə alqoritmində açar axını istifadə olunan düz mətndən tamamilə fərqlidir. 8 * 8 S-Box (S0 S255), burada girişlərin hər biri 0 ilə 255 nömrələrinin permutasiyasıdır və permutasiya dəyişən uzunluq açarının funksiyasıdır. 256 baytlıq bir vəziyyət vektoru S-nı işə salmaq üçün 1 ilə 256 bayt arasında dəyişən uzunluqlu açar, S [0] ilə S [255] elementləri ilə birgə istifadə olunur. Şifrələmə və şifrəni açmaq üçün sistemdən bir şəkildə 255 girişdən birini seçməklə S-dən bir bayt k əmələ gəlir, sonra S-dəki girişlər yenidən permutasiya olunur. Şifrələmə və deşifrələmə üçün 255 girişdən birini seçərək S-dən bir bayt k əmələ gəlir, sonra S-dəki girişlərə yenidən icazə verilir.

RC4-ün üstün cəhətləri:

- Cədvəldə hər hansı dəyərin harada olduğunu bilməkdə çətinlik çəkir;
- Ardıcıllıqla hər bir dəyəri seçmək üçün cədvəldə hansı mövqedən istifadə edildiyini bilməkdə çətinlik çəkir;
- Şifrələmə DES-dən təxminən 10 qat daha sürətlidir.

RC4-ün mənfi cəhətləri:

- RC4 artıq etibarlı hesab edilmir;
- Hər 256 açardan biri zəif açar ola bilər. Bu açarlar, daha çox yaradılan baytdan birinin açarın bir neçə bayt ilə güclü əlaqələndirildiyi şərtləri tapmağı bacaran kripto-analistlər tərəfindən təyin olunur.
- Müəyyən bir RC4 alqoritmi açarı yalnız bir dəfə istifadə edilə bilər.

## 3.2. AİS-in təhlükəsizliyinin təmin edilməsində parolun köməyi ilə müdafiənin rolu

Ənənəvi metodlardan biri dövri şifrə dəyişdirmə qaydasıdır.Burada cinayətkarın şifrəsini əldə etdiyi hesabın vaxtı bitəndə bağlamaq məqsədi daşıyır, lakin istifadəçilər yeni şifrədə yalnız bir neçə simvol dəyişdirdiklərinə görə köhnə şifrəni saxlayan cinayətkarkarın yeni şifrəni qırması çətin olmayacaq.Dövri şifrənin dəyişdirilməsi, yəni istifadəçi şifrəsinin bir neçə aydan bir parolun yenilənməsi şifrə təhlükəsizliyini gücləndirməkdən daha çox çətinləşdirir, eyni zamanda ötən ilin iyun ayında NIST tərəfindən verilmiş hesabatda dövri şifrə dəyişdirmə qaydasının aradan qaldırılması tövsiyə olunur.

Hərflərin, rəqəmlərin və xüsusi simvolların birləşməsi ilə mürəkkəb parolların yaradılmasını tələb etmək artıq təhlükəsizlik tədbiri hesab edilmir. Bunun səbəbi, istifadəçilərin tapılması çətin olan parol yaratmalarının qarşısını almasıdır.

Yeni yaradılan parolların məcburi təsdiqlənməsi yeni bir metod kimi təqdim olunur. Tez-tez istifadə olunan, asanlıqla tapılan və ya oğurlanmış parolların siyahısına görə yaradılan yeni parolun yoxlanılması parolun etibarlılığının qiymətləndirilməsi üçün vacibdir ki, istifadəçilərin "12345678" və ya "parol" kimi asanlıqla proqnozlaşdırıla bilən şifrələrin seçilməsinin qarşısını alsınlar.

Şifrə təhlükəsizliyində çox faktorlu identifikasiya və iki faktorlu identifikasiya texnologiyaları vacibdir. İki faktorlu identifikasiyada istifadəçi identifikasiyası iki mərhələli bir proses kimi hazırlanmışdır. İki faktorlu doğrulamada istifadəçidən həm bildiyi bir şey yəni şifrəsi, həm də sahib olduğu bir şey yəni mobil telefondan istifadə edərək sistemə daxil olması tələb olunur.

Parol - PassWord PassssWord1 Paasword9876 ... və ya sevimli idman şəxsiyyətlərinin, məşhurların və hətta markaların adları bir çox insan tərəfindən parol kimi istifadə olunur. Parol ilə əlaqəli müxtəlif vəziyyətlər vardır. Bunun üçün ən çox görülən vəziyyətlər aşağıdakı kimidir:

- Çoxlu sayda olan parolu necə yadda saxlamaq lazımdır;

- Bu mənim hesabımda baş verə bilməz (bu, hər kəsin düşünə biləcəyi ən ağıla gəlməz arqumentdir)
- Heç kim parolun nə olduğunu təxmin edə bilməz.

Bu planetdə heç kimin kiminsə parolunu tapa bilmədiyini düşünmək gülünc olar. Çünki müasir texnologiya dünyasında inkişaf etdirilən alqoritmlər, proqram təminatı və datara ziyan verən mütəxəssislər var.Bu sadəcə istifadəçilərin internetə qoşulu olması ilə kifayətlənir.

Parolu, OTP, pin və digər giriş icazələrini heç kəslə paylaşmaq olmaz.Hətta bu tip hallar çox olduğundan banklar bele mesajları istifaçələrə göndərirlər.Bununla bağlı sosial mediya platformaları təhlükəsizlik qaydalarında parolları heç kimlə paylaşmamağı tövsiyyə edir.

Parol ilə əlaqədar nələr edilməlidir?

- Parol uzunluğu 8 ilə 15 arasında olmalıdır.
- Parolda ən azı bir rəqəm (0-9) olmalıdır.
- Parolda ən azı bir kiçik hərf (a-z) olmalıdır.
- Parolda ən azı bir böyük hərf olmalıdır (A-Z).
- Parolda ən azı bir xüsusi simvol olmalıdır (@, #, %, &, ! , $ və s. ...).
- 'Alphanumeric' yolun gedilməsi;
- Hər giriş (log in) üçün fərqli parollar istifadə edilməsi;
- Cümlələr və ya ifadələrin istifadə edilməsi, bunlar 'parol ifadələr' adlanır.

Məsələn: 'Mən ulduzlara baxmağı xoşlayıram və ay işığı xoşbəxtdir'. Cümlənin heç bir mənası yoxdur və ya şifahi yaxud qrammatik cəhətdən düzəldilməsinə ehtiyac yoxdur. Sadəcə istifadəçi tərəfindən yadda saxlanılmalıdır.

- Çox faktorlu identifikasiyadan istifadə: İstifadəçi ID, şifrə və vaxtlı bir işarə və ya OTP –nin tələb olunduğu MFA. MFA seçiminin olduğu hər yerdə istifadə edilməlidir. Bulud xidmətlərindən istifadə edərək iş məqsədləri üçün MFA siyahını təsdiqləmək üçün ağıllı seçimdir.
- Bankın müştəriləri hər 180 gündən bir istifadə etdikləri parolları dəyişdirməlidirlər;

- Sosial mediya və email parolları 3 ayda bir dəyişdirilməlidir. MFA və ya 2FA parolun uzunluğu 4 simvola qədər ola biləcəyini və telefon və ya e-poçtla alınan OTP-nin icazəsiz girişdən əlavə təhlükəsizlik təmin edəcək.
- Etibarlı parol menecerlərindən istifadə edilməlidir. Ancaq hər hansı bir xidməti kor-koranə istifadə etməkdən çəkinin. Çünki həmin xidmətlər təhlükəli ola bilər.
- Təhlükəsizlik sualları – misal üçün təhlükəsizlik sualı aşağıdakı kimi seçilir. - Ananızın adı nədir? Burada sualın cavabının doğru yaxud yanlış olduğu önəmli deyil. Cavab - '5T0ficEj', 'G @ ngA', '$ w @ mm!', 'R0binMaria' kimi ola bilər. Mətni Hexadecimal converterdən istifadə dəyişmək olar. 'Ganga' '47616e6761' ya da SHA1 Generator - <'Ganga' 'aefd2ef64c405c930bbc32049d3c2e09e64a'.

Valideynlərin, uşaqların, həyat yoldaşın, avtomobilin və s. adlarını habelə müvafiq tarixləri, qeydiyyat nömrələri, doğum yeri, yaşayış şəhəri kimi statik məlumatı tapmaq çox asandır [29].

Parol ilə əlaqədar nələr edilməməlidir?

- Parolda boşluq olmamalıdır.
- Hər giriş (log in) üçün eyni və ya oxşar parol istifadə olunmamalıdır;
- Heç vaxt istifadə edilməməli olan lüğət paroludur. Bu lüğət hücumu ən çox yayılmış üsuldur.
- Atalar sözləri və ya deyimlər olan parollar istifadə olunmamalıdır çünki açıq seçimlərin sadə məntiqi ilə bu parol qırıla bilər.
- Ailə, dostların və yaxud ev heyvanlarınn doğum tarixlərinin kombinasiyasından istifadə etmək olmaz.
- Şəxsiyyəti təsdiq edən sənədlərin nömrələrinin kombinasiyaları- pasport, sürücülük vəsiqəsi və s. istifadə edilməməlidir.
- Hər hansı bir markanın, məşhurların, şəxsiyyətlərin, yerlərin, bəyəndiyiniz şeylərin və s. adlarını istifadə etmək olmaz.
- Hər parol Google-da yaddaşda saxlanılmamalıdır.

- Böyük hərf və ya kiçik hərflərlə yaxud rəqəmlərin məntiqi ardıcılığı olmamalıdır.Məsələn, ‘Parol12345678’, ‘Qwerty12345678’ və s. kimi parollardan istifadəsi böyük şirkətlərdə qadağan olunmuşdur.
- Parollar böyük,kiçik,rəqəm və xüsusi simvoların kombinasiyası şəklində olmalıdır.
- Zaman keçdikcə yaddaşda saxladığınız eyni parolun müxtəlif kombinasıyalarından istifadə etmək olmaz.

İnternetə gəzərkən müntəzəm istifadə edilən demək olar ki, hər veb saytda giriş məlumatları tələb olunur. Ən vacib giriş məlumatı paroldur.

Kriptoqrafik hash funksiyası kriptoqrafiyada istifadəyə yararlı hala gətirən xüsusi hash funksiyalar sinifidir. Təsadüfi ölçülü məlumatları bir tərəfli funksiya, tərs edilə bilməyən bir funksiya olaraq hazırlanmış sabit ölçülü bit sətirinə (hash funksiyası) xəritələyən riyazi alqoritmdir. Giriş kodlarına (log in) baxmış olsanız developerlərin istifadəçi şifrələrini "etibarlı" etmək üçün hash funksiyadan istifadə edilir. Bu şəkildə yaradılan parolları gülünc şəkildə sındırmaq olar.

- MD5 ilk vaxtlarda kriptoqrafik hash funksiyası olaraq istifadə edilmək üçün hazırlanmışdır ancaq ancaq təhlükəsizlik baxımından problemli olduğu müəyyənləşdirilmişdir.
- SHA-1 yaxşı maliyyələşdirilən rəqiblərə qarşı etibarlı hesab edilmir. 2005-ci ildə kripto analistlər SHA-1-yə hücumlar etdilər. Bu da alqoritmin davamlı istifadəsi üçün kifayət qədər etibarlı olmayacağını irəli sürdülər.
- Çox vaxt istifadə olunmayan SHA-2, SHA1-in varisidir. 4 növ hash funksiyasını birləşdirdi: SHA224, SHA256, SHA384 və SHA512. SHA1 ilə eyni şəkildə işləyir lakin daha güclü və daha uzun bir hash yaradır.
- BlowFish, bir çox şifrə paketlərində və şifrələmə məhsullarında olan simmetrik açar blok şifrəsidir. Blowfish proqramda yaxşı şifrləmə sürəti təmin edir və bu günə qədər effektiv kripto analizə rast gəlinməyib.

Bir veb saytda hesab yaradılan və parol qeyd olunan zaman parol olduğu kimi saytın verilənlər bazasında yadda saxlanılmır. Bunun əvəzinə ümumiyyətlə mənasız

kimi görünən amma olduqca yararlı olan təsadüfi funksiyalardan (hash funksiyaları) istifadə olunur. Düz mətnli parol əvəzinə hash kimi verilənlər bazasında saxlanılır ki, veb sayt hücuma uğrayan zaman yaxud parollar onlayn olaraq sızdırılan zaman əldə olunan həqiqi mətn parolu deyil. Məsələn, parolumuz 'global' - dır və ancaq o SHA256 hash funksiyası ilə verilənlər bazasında yaddaşda saxlanır.

Düz mətn parol: global

Hash funkiyası sonrası: f8d59362da74ffe833332dc20508f

İstifadəçi veb sayta hər dəfə daxil olduqda eyni düz mətn parolu daxil edir və sonra bu hash verilənlər bazasında saxlanılan eyni hash funksiyaları ilə qarşılaşdırılır.Əgər uyğun gələrsə istifadəçi hesabdan istifadə edə biləcək.

Fərqli bir istifadəçi eyni parol seçərsə hər iki girişin eyni olması səbəbindən toqquşma deyilən vəziyyət meydana gəlir. Bu vəziyyətdə orijinal parola digər bir mətn əlavə edilir və daha sonra unikal bir hash yaradır və verilənlər bazasında saxlanılır. Parolların saxlanmasının bu üsulu müxtəlif hash funksiyalarının təkrarlanması ilə onları daha etibarlı etmək olar. Bütün tədbirlərə və informasiya təhlükəsizliyi sahəsində ən yaxşı təcrübələrə riayət olunmasına baxmayaraq yenə də səhvlik ola bilər.Toqquşma zamanı 2 metoddan istifadə olunur.

1.Güclü Hücumlar (Brute Force Attacks): Ən çox yayılmış olduğu üçün əksəriyyət insanlar bu növ ilə tanışdırlar. Adından da göründüyü kimi düz mətnli parolların bütün kombinasiyalarını hash funksiyası ilə çalışdırır.Əldə olan bütün kombinasilar mətn faylında saxlanılan müxtəlif hashlər ilə qarşılaşdırır. Bunun bir hash funksiyası vasitəsilə bütün permutasiyaları çalışdıran və bunları mətn faylindakılarla qarşılaşdırılması illər ala bilər.Lakin xakerin kompüter vasitəsilə yüksək performanslı serverə daxil olduğu üçün saniyədə 40 milyard hash –i çalışdıra bilir.Bunun üçün ən yaşxşısı NVIDIA qrafik kartlarıdır.

CUDA HashCat adlı bir proqramdan istifadə edərək krekinq etmək olar.Misal üçün bütün hash -in hamısını özündə cəmləşdirən test.hash adlı fayl vardır. 7 simvoldan ibarət olan parolların hamısını kiçik hərflər şəklində əldə etmək istəyirik.Aşağıdakı əmrdən istifadə edirik:

./hashcat –a 3 test.hash ?l?l?l?l?l?l?l

‘a’ – hücumdur;

‘3’ – güclü hücum modu deməkdir;

‘? l’ – kiçik hərf deməkdir;

7 dəfə təkrar yazılması 7kiçik hərf mənasını verir.

Bir neçə saniyə ərzində hash test. hash ilə uyğun gələn bütün birləşmələr ekranda görünəcəkdir. Əgər 6 kiçik hərf və sonda 2 ədəd olan parolları sındırmaq istəyiriksə o zaman bunu yazmalıyıq:

./hashcat –a 3 test.hash ?l?l?l?l?l?d?d

Simvol sayının artması ilə kombinasiyaların sayıda düz mütənasib olaraq artır. Buda əlbəttə parolun qırılmasının vaxtını uzadır. Hər iki misal üçün aparılan riyazi əməliyyatları göstərək:

1-ci misal: $26^7$

2-ci misal: $26^6 * 10^2$ sayda əməliyyat icra edir.

2. Lüğət hücumları (Dictionary Attacks): Mətn faylında saxlanılan çoxsaylı istifadə olunan parolların lüğəti var və saytın verilənlər bazasında bunlar bir birilə qarşılaşdırılır.Bu, güclü hücumlardan daha səmərəlidir.Misal üçün milyonlarla parol toplusundan ibarət siyahıdan parolu ‘global’ olanı tapmaq lazımdır.[30]

./hashcat -a 0 test.hash ./dictionaries/global.dict

‘0’ – lüğət hücum modudur.

Bu hücumlar lüğətə bir sıra qaydalar tətbiq etməklə xüsusiləşdirilə bilər. Bu qaydalar insanların parollarını daha etibarlı etməkdən başqa bir şey deyildir.Məsələn, ‘I’ hərfi ‘1’ ilə, ‘E’ hərfi isə ‘3’ ilə əvəz edilə bilər.Tutaq ki, bütün qaydalar myrules adlı faylda saxlanılır. İndi bu faylı istifadə edərək hücum həyata keçirilirsə, bütün lüğətə eyni anda qayda tətbiq edən bir sıra lüğət hücumları həyata keçirir.

./hashcat -a 0 -r ./rules/myrules.rule test.hash ./dictionaries/global.dict

Parol Entropiyası- parolda saxlanan informasiyaların miqdarıdır. Parolun entropiyası nə kadar yüksək olarsa, qırılması da bir o qədər uzun sürər. Yəni, 6 simvoldan ibarət parol varsa entropiya çox aşağıdır və ona asanlıqla güclü hücum etmək olar. Bir xüsusi simvolu olan 10 simvoldan ibarət parol varsa güclü

hücumdan qorunmaq asandır.Ancaq onu lüğətl hücum ilə sındırmaq hələ də mümkündür.Bəzən elə ola bilər ki, xüsusi simvoldan istifadə etmədəndə parolun entropiyası yüksək ola bilər. Simvol birləşmələrini istifadə etmək əvəzinə fərqli söz birləşmələri ilə lüğət hücumundan istifadə edə bilərik. Həqiqətən parolun etibarlı olması üçün sadə 3 yaxud 4 söz götürülməli və sözlərin ortasına xüsusi simvoldan istidfadə edilməlidir. Bu qayda parolu həm güclü hücumdan həm də lüğət hücumundan qoruyur. Bu qaydanı tətbiq etməklə etibarlı parol menecerindən istifadə etmək tövsiyyə olunur.

Bir çox insan özləri özlərinə sual verirlər ki, "Necə şifrə seçməliyəm?" və ya "Şifrəmi necə təhlükəsiz edə bilərəm". Elə üsullar var ki, onlar həm yaddda saxlanılması həm də tətbiqi çox sadədir. Bu üsulda kitabdan istifadə edilir.

- Gözlər bağlı şəkildə hər hansı bir səhifə seçilir və göstərici barmaq səhifənin istənilən yerində saxlanılır.
- Əgər hansısa sözün üzərində deyilsə yenidən edilməlidir
- Həmin söz olan səhifənin nömrəsi qeyd edilməlidir. Daha sonra həmin sözün səhifədəki neçənci cümlənin daxilində olduğu qeyd edilir. Həmin sözün cümlə daxilində neçənci olduğu qeyd edilir. Bu üç ədəd yadda saxlanılmalıdır.
- Əgər bu yadda qalmırsa doğum tarixindən istifadə edilə bilər. Tutaq ki,9-cu ayın 22-dirsə ad günü, o zaman, 9 səhifənin nömrəsi, 2 həmin səhifədə olan cümlənin nömrəsi, 2 isə həmin cümlədə neçənci səhifə olduğunu göstərir. Yəni, ən çox altı simvol yadda saxlanılacaq.
- Daha sonra həmin sözdən sonra gələn sözləri aralarında boşluq olmadan yan yana yazılmalıdır.Beləliklə heç kəsin təxmin edəməyəcəyi parol mətni əmələ gəlir. Təhlükəsizliyi daha da artırmaq üçün bir sözü ya da hərfi xüsusi simvol ilə əvəz etmək olar.Məsələn, "S" hərfi "$" işarəsi ilə, "O" hərfi "0" ilə əvəz edilə bilər. Beləliklə, parolun təhlükəsizliyi daha da artır. Bu dəyişikliyin edilməsi unudulmamalıdır. Parolu daha da qarışdırmağın başqa yolları vardır amma bu qədəri kifayətdir. Onsuz da bu qayda ilə əldə edilən parol çox təhlükəsiz olur.

Credential Stuffing- hücumları eyni hesab məlumatlarını birdən çox hesab üçün təkrar istifadə etməyin təhlükəsini sübut edir. Parollar və digər məlumatlar

pozuntudan sonra yenidən qurulandan sonra, xakerlər digər platformalarda istifadəçilərin hesablarına giriş əldə etmək üçün əvvəllər oğurlanmış credential – ı istifadə etməyə cəhd edə bilərlər. Xakerlər, oğurlanan şifrələrin siyahısını satırlar ki, bu da geniş zərərli fəaliyyətlə nəticələnə bilər və şəbəkələrdəki pozuntu riskini artırır.

Password Spraying. Bir hesaba daxil olmaq üçün çox şifrəni sınamaq əvəzinə, parol partlatma hücumları, birdən çox hesaba daxil olmaq üçün ümumi şifrələrdən istifadə etməkdir. Bu, hakerlərə təkrar uğursuz girişlərdən sonra normal tetiklenen hesab qəzaları ətrafında işləməyə imkan verən yavaş və müntəzəm bir hack metodudur. Password Spraying getdikcə daha çox yayılır və tez-tez tək giriş (SSO) hesablarını, bulud əsaslı tətbiqləri və e-poçt hesablarını hədəfləmək üçün istifadə olunur. Bu spesifik sahələri hədəf alaraq xakerlər şəbəkələrə daha geniş daxil ola bilər və daha böyük miqdarda məlumatları oğurlaya bilərlər.

Traffic Interception. Şəbəkələr boyunca hərəkət edən paketlər, xakerlər trafikə nəzarət etmək və daxil etmək üçün istifadə etdiyi paket detektorlarına qarşı həssasdır.

Sniferlər tərəfindən əldə edilən bütün parol məlumatları icazəsiz şəbəkəyə giriş imkanı verə bilər. Bəzi hallarda xakerlər şifrəli paarolları açmaq üçün əlavə vasitələrdən istifadə edə bilər və bununla da şifrələmənin təhlükəsizlik vasitəsi kimi istifadəsinə xələl gətirir.

Rainbow Table. Şifrələrin qarışdırılması çox vaxt etibarlı təhlükəsizlik praktikası hesab olunur, lakin rainbow table onun effektivliyini təhdid edir. Xakerlər, bilinən alqoritmlər üçün hash dəyərlərinin yığımlarından istifadə edərək, doğru yolu tapana qədər sistematik şəkildə bütün mümkün hash ilə işləyə bilərlər. Bu, əhəmiyyətli dərəcədə hesablama gücünü tələb edir və hash parollarını sındıra bilməyəcəyinə zəmanət verilmir ancaq parol təhlükəsizliyini təmin etmək üçün hər hansı bir texnikaya güvənmək təhlükəsi barədə xəbərdar etməlidir.

Veb tətbiqlərinin əksəriyyəti istifadəçilərdən istifadəçi adları və parollarını istəyərək özlərini təsdiqləmələrini tələb edir. İstifadəçilərin təqdim etdikləri istifadəçi adı və parol verilənlər bazasında saxlanılan məlumatlarla müqayisə edilir

və məlumatlar uyğun gəlsə istifadəçiyə giriş imkanı verilir. Veb saytın parolların saxlandığı verilənlər bazası təhlükə ilə qarşılaşarsa bu ciddi problemlərə səbəb ola bilər.

Aparılan araşdırmalara görə xalis istifadəçilərin 55% -i əksər saytlarda eyni paroldan istifadə edir! Şifrəni düz mətndə saxlayan veb sayt təhlükədə olduğu təqdirdə, cinayətkarın yalnız həmin veb saytdakı hesaba daxil olmağı deyil, eyni parol istifadə edilən bütün sosial media, e-poçt, forumlar və s. hesablarını əldə edə biləcəyini göstərir.Əgər bu hal baş verərsə kiber cinayətkar istifadəçilərin bütün məxfi məlumatlarına sahib olacaq.

Bazadan parolun alınması prosesini mürəkkəbləşdirmək üçün bir çox yol vardır. Hətta bəzi developerlər əsas qaydalara məhəl qoymayaraq və parolları düz mətndə saxlayırlar. Parolları düz mətndə saxlayan (bəzi nüfuzlu saytlar da daxil olmaqla) 30% -dən çox sayt var. Veb sayt parolu düz mətndə saxlayırsa, nə qədər güclü şifrə seçməkdən asılı olmayaraq heç kəs təhlükəsiz deyil! Verilənlər bazasında parolları düz mətn kimi saxlamaq cinayətdir.

Parol düz mətn deyilsə belə yenə də şifrələməli və saxlanılmalıdır. Şifrələmə funksiyaları giriş və çıxış arasındakı bire bir bərabərlik təmin edir və onlar həmişə geri çevrilir. Əgər cinayətkar açarı qəbul etsə parolu deşifrələyə biləcək. Daha yaxşı yol kriptoqrafik hash funksiyasından istifadə etməkdir. Hash funksiyası giriş və çıxış arasında çoxsaylı bərabərliyi təmin edir və çıxışı geri qaytarmaq demək olar ki, mümkün deyil. Yaxşı kriptoqrafik hash funksiyasının daha az toqquşması (collisions) var.Parolları hash etmək üçün hash funksiyasının unikal çıxışı olacağını güman edə bilərik, yəni iki fərqli parol üçün eyni hash dəyərini əldə edirik.

Məşhur kriptoqrafik hash funksiyalarından bəziləri MD5 və SHA1-dir. Düzgün mətn parolunu verilənlər bazasında saxlamaq əvəzinə, parolun hash - i saxlamaq digər başqa yoldur. Bu sadədir istifadəçi tərəfindən daxil edilmiş parol ilə eyni hash funksiyasını tətbiq etmək və daha sonra verilənlər bazasında saxlanılan hash ilə müqayisə etmək lazımdır. Hər ikisi də uyğun gəlirsə, istifadəçi şəxsiyyəti təsdiqlənir. Cinayətkarın verilənlər bazasına girişi varsa həqiqi parolu deyil yalnız hash çıxışı görə bilər.

Developerlər istifadəçilərin parollarını gizli saxlamaq üçün digər üsullardan da istifadə edirlər. Belə ki, istifadəçinin parolundan sonra əlavə olaraq başqa simvollar yığımı qeyd olunur.Məsələn, parol abc-dir amma verilənlər bazasında sonuna !ZaP0#8 əlavə edilərək hash olunub saxlanılır.Nəticə etibarilə hashFunction ('abc') əvəzinə verilənlər bazasında hashFunction ('abc! ZaP0 # 8') kimi saxlanılacaqdır.Bu tip əlavələr verilənlər bazasında saxlanılmır.Onlar kənar dünya ilə əlaqəsi olmayan proqramın konfiqurasiyasında (mənbə sənədləri) saxlanılır. Mənbə sənədlərinə giriş əldə etmək verilənlər bazasına daxil olmaqdan daha çətindir.

Yuxarıdakı simvollar yığımının əlavə edilmə üsulu statikdir. Bütün parollar üçün sabit simvollar yığımı vardır. İstifadəçini eyniləşdirmək üçün əvvəlcə sabit simvollar yığımını istifadəçiyə daxil edilmiş giriş (şifrə) ilə bağlamaq və sonra dəyəri hashing funksiyasına keçirmək və verilənlər bazasında saxlanılan dəyərlə müqayisə etmək lazımdır. Lakin bu yanaşma hələ də güclü hücumlara qarşı həssasdır və cinayətkar statik simvollar yığımı əldə edə bilirsə, hər sözü simvollar yığımı ilə birləşdirərək köhnə hücum metodologiyasından istifadə edə bilər.

Daha yaxşı yanaşma dinamik simvollar yığımından istifadə etməkdir. Hər bir istifadəçi üçün kriptoqrafik cəhətdən güclü təsadüfi olaraq generator tərəfindən yeni bir simvollar yığımı yaranır. İstifadəçi tərəfindən daxil edilən parol, təsadüfi yaranan simvollar yığımı ilə yanaşı həm də statik simvollar yığımı ilə birləşdirilir.Birləşdirilmiş simvollar hash funksiyasının girişi kimi çıxış edir. Alınan nəticə verilənlər bazasında saxlanılır. Dinamik simvollar yığını müxtəlif istifadəçilər üçün fərqli olduğuna görə verilənlər bazasında saxlanılmalıdır. İstifadəçi şəxsiyyətinin təsdiqlənməsi lazım olduqda, əvvəlcə həmin istifadəçi üçün dinamik simvollar yığınının dəyəri verilənlər bazasından daxil edilir və istifadəçi tərəfindən verilmiş statik simvollar yığını ilə birləşdirilir. Nəticə verilənlər bazasında saxlanılan hash ilə müqayisə olunur.

### 3.3. Parolun təhlükəsizliyinin təmin edilməsi

Verilənlər bazasının təhlükəsizliyi pozulursa, cinayətkar yalnız hash olunmuş parolları deyil həm də istifadə olunan dinamik simvollar yığınını əldə edə bilər. Cinayətkarın dinamik simvollar yığını olsa belə, verilənlər bazasında hər bir istifadəçi üçün yeni bir hash cədvəli yaratmalıdır. Bu, bütün istifadəçilər üçün tək bir cədvəl yaratmaqdan daha çətindir.

Yuxarıdakı yanaşma cinatətkarın işini yavaşlatmaq üçün olduqca yaxşı üsuldur. Lakin MD5 / SHA1 əvəzinə bcrypt və scrypt kimi alqoritmlərdən istifadə etmək tövsiyə olunur. Bcrypt Blowfish-ə əsaslanan hashing alqoritmidir. Bir xərc / iş amilini təyin etməyinizi tələb edir. İş faktoru ümumi prosesi daha da yavaşladır və buna görə də hash cədvəl yaratmaq üçün sərf olunan vaxt dəfələrlə artacaqdır.

Güclü parolu qorumaq üçün aşağıdakılar tövsiyyə edilir:

- Parol hər hansı bir səbəblə heç kim ilə bölüşülməməlidir.Birinin başqa bir şəxsin qorunan mənbələrinə girməsini tələb etdiyi hallarda, icazə seçimlərinin nümayişi araşdırılmalıdır. Məsələn, Microsoft Exchange təqvimi istifadəçiyə heç bir parol paylaşmadan öz təqviminə nəzarəti digər istifadəçiyə həvalə etməyə imkan verir. Parollar hətta kompüter təmiri üçün də bölüşdürülməməlidir. Bunun alternativi kompüter ustası üçün müvafiq giriş səviyyəsi olan yeni hesab yaratmaqdır.
- Əgər şübhə varsa parol dəyişdirilməlidir.Parolun normal istifadə edilməyən kompüterdən dəyişdirildiyinə əmin olmaq lazımdır. Parolu bərpa etdikdən sonra hadisə rəhbər şəxslərə və informasiya təhlükəsizliyi mütəxəssislərinə bildirilməlidir.
- Sadə parol əvəzinə mürəkkəb parollardan (passphrase) istifadə edilməlidir.Parol frazası, daxil edilmiş ədədi və / və ya simvolik simvolları olan sözlər ardıcıllığından ibarət bir şifrədir. Parol frazası hər hansı musiqinin sözləri ola bilər. Parol frazası adətən daha uzun olur. Məsələn, "Mənim p@r0lum $uperdir!" kimi parol 23 simvoldan ibarətdir həm də xüsusi simvollardan istifadə edilmişdir. Xatırlamaq da nisbətən asandır.Burada istifadə edilən boşluqlarda parolun mürəkkəbliyini artırır.[31]

- Parolu yazmaq və ya etibarsız şəkildə saxlamaq olmaz.Bir qayda olaraq parolu yazmaqdan çəkinmək lazımdır.Parolu yazmaq lazım olduqda etibarlı yerdə saxlanılmalı və artıq lazım olmadıqda düzgün şəkildə yox edilməlidir. Parol meneceridən güclü şifrələmədən və istifadə etmədən əvvəl identifikasiyasını tələb etmədikcə parolları saxlamaq üçün istifadə etmək tövsiyə edilmir. ISO bu tələblərə cavab verən bəzi parol menecerlərini yoxlamışdır.

- Eyni parolu təkrar istifadə etməkdən çəkinmək lazımdır.Hesab parolunu dəyişdirərkən yenidən əvvəlki paroldan istifadə edilməməlidir. Parol hər hansı bir səbəbdən paylaşılmışsa, bu parolu təkrar istifadə etmək başqasının hesaba icazəsiz giriş əldə etməsinə səbəb ola bilər.

- Birdən çox hesab üçün eyni paroldan istifadə etmək təhlükəlidir.Eyni parolu birdən çox hesab üçün istifadə edərkən parolu yadda saxlamağı asanlaşdırır, eyni zamanda cinayətkarın birdən çox sistemə icazəsiz giriş əldə etməsinə imkan verən bir zəncir effekti də ola bilər. Bu onlayn bank hesabı kimi daha həssas hesablarla əlaqəli olduqda xüsusilə vacibdir. Bu parollar sürətli mesajlaşma, veb poçt və digər veb əsaslı hesablar üçün istifadə edilən paroldan fərqli olmalıdır.

- Avtomatik giriş funksiyasından istifadə etmək olmaz.Avtomatik giriş funksiyasından istifadə parol istifadə etməyi əhəmiyyətli dərəcədə aradan qaldırır. Zərərli istifadəçi avtomatik giriş konfiqurasiyası ilə sistemə fiziki olaraq daxil ola bilirsə, sistemə nəzarəti ələ keçirə və potensial təhlükəli məlumatlara sahib ola bilər.

- Güclü parol tətbiq edilməlidir. Bir çox sistem və tətbiqlərdə istifadəçinin müəyyən meyarlara cavab verməyən parol təyin etməsinə mane olan funksiyalar mövcuddur. Bu kimi funksiyalar yalnız güclü parolların təyin olunmasını təmin etmək üçün istifadə edilməlidir.

- İlkin parolların dəyişdirilməsinin tələb edilməsi. İstifadəçini başlanğıc parolunu dəyişdirməyə məcbur etmək yalnız istifadəçiyə şifrələrini bilmək imkanı verir. Şifrə yaratmaq və istifadəçiyə paylamaq üçün hansı prosesdən istifadə olunduğundan asılı olaraq, bu tətbiqetmə ilk köçürmə zamanı istifadəçinin proqnozlaşdırılması və ya tutulma riskini azaltmağa kömək edə bilər. Bu təlimat parolun əl ilə yenidən qurulması lazım olduğu hallara da aiddir.

- İlkin parolların müddətinin bitməməsinin məcbur edilməsi. Müəyyən hallarda istifadəçiyə yeni hesab verilə bilər və müəyyən müddətə daxil olmaya bilər. Daha əvvəl qeyd edildiyi kimi, parolların yaranması və yayılması üçün hansı hərəkətin tətbiq olunduğundan asılı olaraq ilkin parolun daha çox güzəşt olunduğu ehtimal olunur. Başlanğıc parolunu müəyyən bir müddətə məcbur etmək (məsələn, 72 saat) bu riskin azaldılmasına kömək edir. Bu hesabın tələb olunmadığı bir işarə ola bilər.
- İlkin parol üçün məhdudlaşdırılmış datalardan istifadə edilməməsi. Dataların təsnifatı qaydaları, dataların təsnifatı sxemində məhdudlaşdırılmış dataları müəyyənləşdirir. Məhdud datalara sosial təminat nömrəsi, adı, doğum tarixi və s. daxildir, lakin bununla da məhdudlaşmır. Belə datalar ilkin parolun formalaşdırılması üçün tamamilə və ya qismən istifadə edilməməlidir.
- Parol sıfırlamazdan əvvəl həmişə istifadəçinin doğruluğunun təsdiqlənməsi. İstifadəçinin şəxsiyyətini sıfırlamazdan əvvəl həmişə təsdiqlənməlidir. İstək şəxsəndirsə fotoşəkilli şəxsiyyət vəsiqəsi ilə bunu etmək kifayətdir. Tələb telefonla edildiyi təqdirdə şəxsiyyəti təsdiqləmək daha çətindir. Bunun bir yolu, istifadəçinin fotoşəkilli şəxsiyyət vəsiqəsi ilə uyğunlaşmasını yoxlamaq üçün video konfrans (məsələn, Skype) keçirilməlidir. Ancaq bu çətin bir proses ola bilər. Başqa seçim, şəxsin rəhbərinə zəng etmək və tələbi təsdiqləməkdir. Müəyyən səbəblərə görə, bu tələbə istəkləri üçün işləməyəcəkdir. İstifadəçiyə bir sıra özəl sualları soruşan bir self-service parol sıfırlama yaxşı yanaşmadır.
- Heç vaxt istifadəçinin parolu soruşulmamalıdır. Yuxarıda da qeyd edildiyi kimi, fərdi istifadəçi hesab parolları bölüşülməməlidir. İcazənin bölüşdürülməsi istifadəçidən şifrələrini istəməyin alternatividir. Bəzi tətbiqlər, bir idarəçinin başqa bir istifadəçini təqlid etməsinə və hərəkətləri hələ də menecerin istifadəçi hesabına bağlamasına imkan verən funksionallıq daxildir. Bu da məqbul alternativdir. Kompüter təmiri hallarında istifadəçidən sistemlərində müvəqqəti hesab yaratmağı xahiş etmək alternativdir.

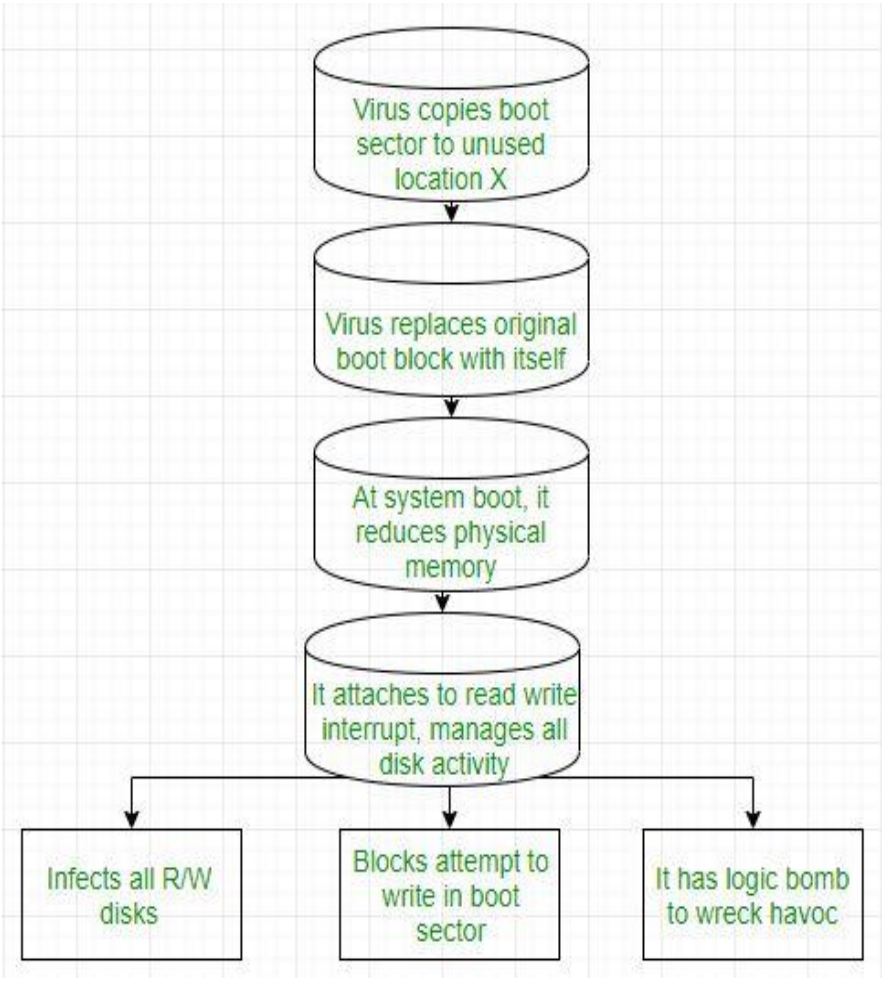
Aşağıda sistemlərin və tətbiqlərin dizaynı və tətbiqi üçün məsul olanlar üçündür.

- Default hesab parollarını dəyişdirmək lazımdır. Default hesablar çox vaxt zərərli istifadəçi tərəfindən icazəsiz giriş mənbəyidir. Mümkün olduğu qədər istifadə edilməməlidir. Hesabı istifadəsiz etmək mümkün deyilsə standart parol sistemi və ya tətbiq quraşdırıldıqdan yaxud konfiqurasiya edildikdən dərhal sonra dəyişdirilməlidir.
- Sistem səviyyəsində və ortaq xidmət hesabı parollarına ciddi nəzarət tətbiq edilməlidir. Birgə xidmət hesabları tez-tez sistemə yüksək səviyyədə girişi təmin edir. Root və administrator kimi sistem səviyyəli hesablar sistemə tam nəzarəti təmin edir. Bu, belə hesabların zərərli fəaliyyətə qarşı həssas olmasına səbəb olur. Nəticədə daha uzun və daha mürəkkəb bir şifrə tətbiq edilməlidir. Sistem səviyyəsi və ortaq xidmət hesabları sistem və ya tətbiqin işləməsi üçün çox vacibdir. Bu səbəbdən də bu parollar ümumiyyətlə birdən çox administratora məlumdur. Parol məlumatları olan şəxs iş vəzifələrini dəyişdirdikdə və ya işə xitam verildikdə parollar dəyişdirilməlidir. Root və administrator kimi hesabların istifadəsi mümkün qədər məhdud olmalıdır. Alternativ root yerinə sudo istifadə etmək və standart hesablardan istifadə etmək əvəzinə Windows administratoru üçün unikal hesablar yaratmaq kimi alternativlər araşdırılmalıdır.
- Birdən çox administrator hesabı üçün eyni paroldan istifadə edilməməlidir. Birdən çox hesab üçün eyni paroldan istifadə sistemlərin və tətbiqlərin idarə edilməsini asanlaşdıra bilər. Bununla birlikdə, bu tətbiq cinayətkarın hesab parolunun təhlükəsizliyi nəticəsində çox sayda sistemə girməsinə imkan verən zəncirvari təsir göstərə bilər.
- Parolların düz mətndə ötürülməsinə icazə verilməməlidir. Düz mətnlə ötürülən parollar zərərli şəxs tərəfindən asanlıqla tutulur. FTP, HTTP, SMTP və Telnet kimi protokollar bütün dataları düz mətndə (parol daxil olmaqla) ötürür. Təhlükəsiz alternativlərə şifrəli tuneldən (məsələn, IPSec, SSH və ya SSL) istifadə edərək bir tərəfli hash istifadə edərək parolların ötürülməsi və ya Kerberos kimi bilet əsaslı identifikasiya sxeminin tətbiqi daxildir.
- Parolları asanlıqla təkrar istifadə edilə bilən yerdə saxlamaq olmaz. Parollar zəif şifrələmə və ya hash alqoritmlərindən istifadə edərək saxlanılmamalı və

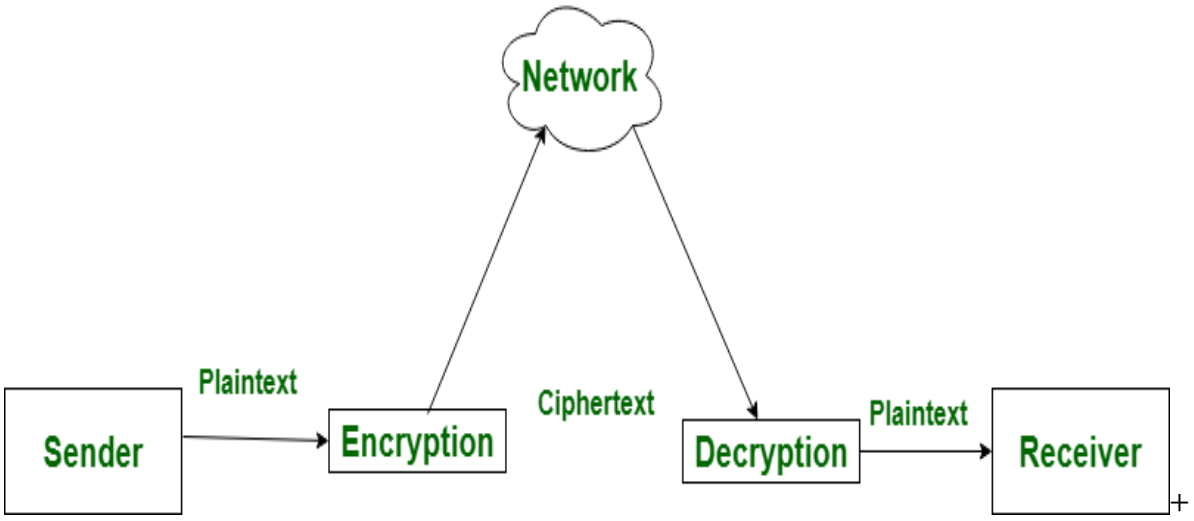
ötürülməməlidir. Məsələn, həm DES şifrələmə alqoritmi, həm də MD-4 hash alqoritmi qorunan dataların parolunun açılmasına imkan yarada biləcək təhlükəsizlik zəifliklərinə malikdir. 3DES və ya AES kimi şifrləmə alqoritmləri və SHA-1 və ya SHA-256 kimi qarışıq alqoritmlər daha əvvəl qeyd olunan alqoritmlərə daha güclü alternativlərdir.

- Parolun dəyişdirilməsi və ya yenidən qurulması üçün avtomatik bildiriş tətbiq edilməlidir. Parol dəyişdirildikdə və ya sıfırlandıqda, avtomatik olaraq istifadəçi hesabı sahibinə e-poçt göndərilməlidir. Bu istifadəçiyə dəyişikliyin və ya sıfırlamanın müvəffəq olduğunu təsdiqləyir və parolu bilərəkdən dəyişdirdisə və ya sıfırlasa istifadəçini xəbərdar edir.

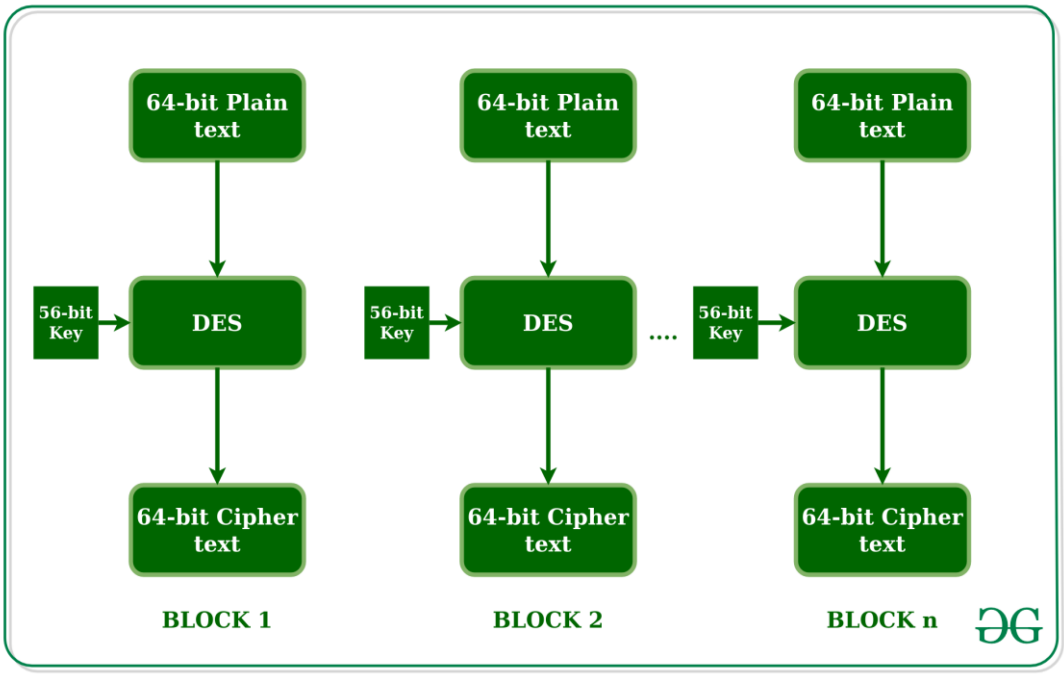
# ƏLAVƏLƏR



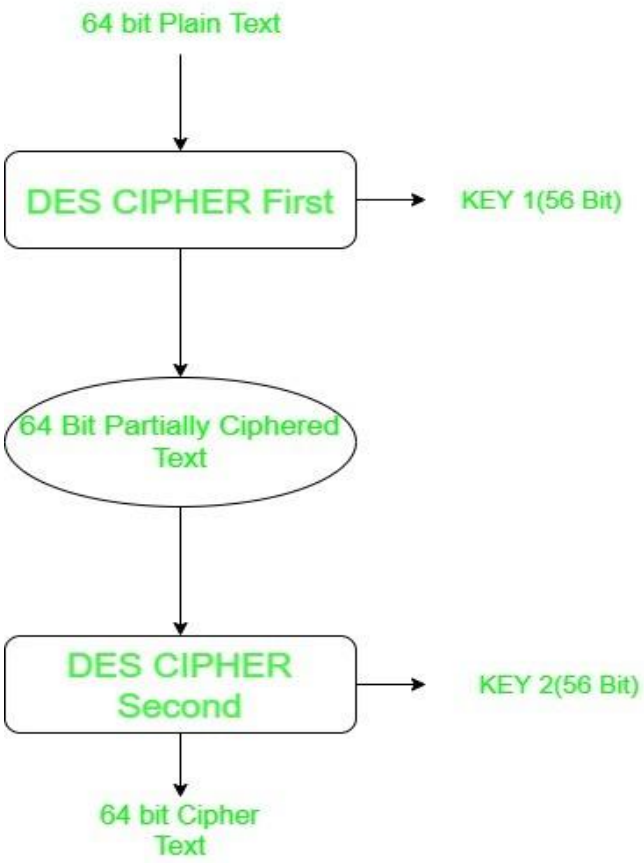

**Boot sektor viruslarının işləmə prinsipi**



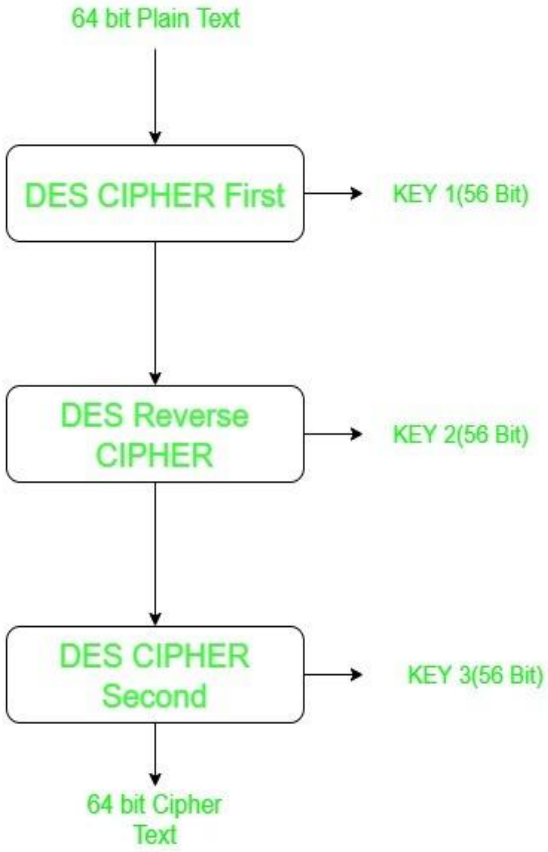

**Şifrələmə və deşifrələmə prosesi**



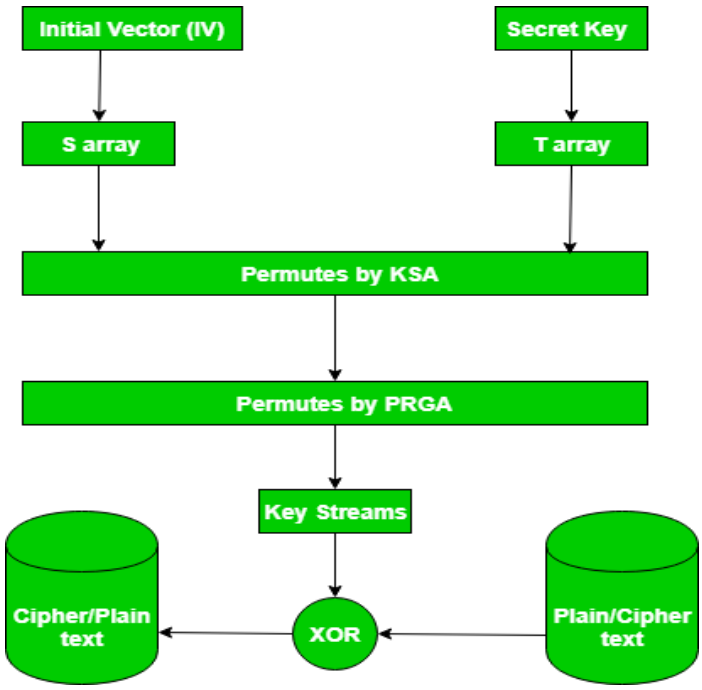

**DES şifrələmə alqoritminin işləmə prinsipi**




**2DES şifrələmə alqoritminin işləmə prinsipi**




**3DES şifrələmə alqoritminin işləmə prinsipi**




**RSA şifrələmə alqoritminin işləmə prinsipi**

# N Ə T İ C Ə V Ə T Ə K L İ F L Ə R

“Bank informasiya sistemlərində istifadəçi hesabının mühafizəsi modelinin tətqiqi” zamanı aşağıdakı yekun nəticələr əldə edilmişdir:

Bank sektorunda informasiya sistemlərini kiber hücumlardan qorumaq üçün mövcud olan şifrələmə alqoritmlər arasından araşdırılaraq həlli ən çətin ola biləcək biri seçilməlidir. Bundan başqa istifadə olunacaq proqram təminatlarının hər biri lisenziyalı olmalıdır. Əks halda proqramda olan gizli quraşdırılmış virus kompüterə daha sonra isə bütov şəbəkəyə keçə bilər. Virusların kompüterə bulaşmasının başqa bir yoluda yaddaş kartlarının kompüterin USB portuna qoşulması ilə baş verir. Buna görə də bank və digər korporativ sahələrdə kompüterlərin USB portuna giriş qadağası qoyulmalıdır.

İri müəssisələrdə istifadəçilərin internet qlobal şəbəkəsində hərəkətləri məhdudlaşdırılmalıdır. Ancaq standart və rəsmi orqanlara, şirkətlərə və s. məxsus olan veb saytlara giriş təmin olunmalıdır. Əgər lazım gələrsə, qurumun informasiya təhlükəsizliyi departamentinə rəsmi olaraq müraciət olunaraq həmin mənbədən istifadə edilə bilər.

İstifadəçilərin təhlükəsiz şəkildə informasiya sistemlərinə girişini təmin edən ən əlverişli üsul parol vasitəsilə girişdir. Hər bir mühitin özünün daxili təhlükəsizlik tələbləri olur. Amma istifadəçilərin çoxu bu qoyulan tələblərə əməl etmir. Bunlardan ən vacibi parolun mürəkkəbliyinə qoyulan tələblərə əməl edilməməsidir. Buna görə də elə prosedurlar tətbiq oluna bilər ki, mürəkkəb simvollardan, böyük və kiçik hərflərdən, rəqəmlərdən və s. istifadə olunmadıqda daxil olunan parol düzgün qəbul edilməsin.

Digər vacib məsələlərdən biri də istifadəçilərin şəxsi mail ünvanlarına mənşəyi bilinməyən mesajların daxil olmasıdır. Bu tipli mesajlarda insanları cəlb etmək üçün əgər verilən linkə daxil olub qeydiyyatdan keçərlərsə, müəyyən hədiyyələr yaxud endirim kampaniyalarından istifadə edə biləcəkləri qeyd olunur.

Həmin linkə daxil olan zaman kibercinayətkar artıq istifadəçi kompüterini ələ keçirmiş olur.

Belə halların baş verməməsi üçün mütəmadi olaraq istifadəçilərə onlayn şəkildə informasiya təhlükəsizliyinə dair təlimlər keçirilməli, yaxud elektron formada hazırlanmış təlim faylı istifadəçilərin şəxsi mail ünvanlarına göndərilməlidir. Ümumiyyətlə, istənilən qurumda rəsmi olaraq lisenziyalı antivirus proqramlarından istifadə olunmalıdır.

# İSTİFADƏ OLUNMUŞ ƏDƏBİYYAT SİYAHISI

1) Anderson C. (2008), “Security Engineering: A Guide to Building Dependable Distributed Systems” . Printed in USA, Second printing, 452 p.

2) Schneier A. (2000), “Secrets and Lies: Digital Security in a Networked World”. Printed in Germany, Sixteenth printing, 374 p.

3) Mark Dowd, John McDonald, Justin Schuh (2007) “The Art of Software Security Assessment: Identifying and Preventing Software Vulnerabilities”. Printed in USA, Third printing, 594 p.

4) Viega M., McGraw B., (2001), “Building Secure Software”. Printed in England, Third printing, 223 p.

5) Howard P., LeBlanc A., (2002), “Writing Secure Code”. Printed in USA, Second printing, 333 p.

6) Stamp S. (2011), “Information Security: Principles and Practice”. Printed in Germany, First printing, 213 p.

7) Paul van Oorschot, (2020), “Computer Security and the Internet: Tools and Jewels”. Printed in Holland, First printing, 321 p.

8) Wenliang Du, (2017), “Computer Security: A Hands-on Approach”. First printing, 114 p.

9) Smith D. (2011), “Elementary Information Security”. Printed in USA, Second printing, 178 p.

10) Gollmann A. (2011), “Computer Security”. Printed in Germany, First printing, 139 p.

11) Stallings C., Brown M., (2014), “Computer Security: Principles and Practice”. Printed in USA, Third printing, 199 p.

12) Goodrich A., Tamassia N., (2010), “Introduction to Computer Security”. Printed in England, Third printing, 431 p.

13) Keith M. Martin, (2017), “Everyday Cryptography”. Printed in USA, Second printing, 524 p.

14) Kaufman A., Perlman D., Speciner M, (2003), “Network Security: Private Communications in a Public World”. Printed in USA, Second printing, 491 p.

15) Əliquliyev R.M., İmamverdiyev Y.N. Kriptoqrafiyanın əsasları. Bakı: İnformasiya texnologiyaları. 2006. 698 s.

16)Таненбаум Э.С. Компьютерные сети. 4-е изд. 2004, СПб, Издательский дом "Питер", 992 стр.

17) Əliquliyev R.M., İmamverdiyev Y.N. İnformasiya təhlükəsizliyi insidentləri. Bakı: “İnformasiya Texnologiyaları” nəşriyyatı, 2012, 219 səh.

18) Kərimov S.Q. İdarəetmənin informasiya texnologiyaları və korporativ informasiya sistemləri, Bakı, 2010, 426 səh.

19) https://www.geeksforgeeks.org/rc4-encryption-algorithm/?ref=rp

20) https://www.identitymanagementinstitute.org/7-hacking-password-attack-methods/

21) https://www.geeksforgeeks.org/difference-between-cyber-security-and-information-security/

22) https://www.geeksforgeeks.org/top-5-information-security-breaches/?ref=rp

23)https://pecb.com/article/information-security-in-banks-and-financial-institutions

24)https://www.theglobaltreasurer.com/2019/09/25/the-importance-of-cyber-security-in-banking/

25)https://pdfs.semanticscholar.org/3475/8c819d3bb4d4e5e4b4d053db523684adac09.pdf

26)https://www.ciatec.com/2018/04/information-security-in-banking-sector/

27)https://www.infoguardsecurity.com/reasons-why-cyber-security-is-important-for-banks/

28)https://www.slideshare.net/SAMVELG/information-security-management-system-in-the-banking-sector

29)https://sqnbankingsystems.com/blog/the-5-biggest-threats-to-a-banks-cyber-security/

30)http://ijcsit.com/docs/vol1issue4/ijcsit2010010413.pdf

31)https://www.safesystems.com/blog/2019/06/5-key-areas-of-focus-for-a-new-bank-information-security-officer/
32)https://www.isdecisions.com/blog/it-infrastructure/information-security-in-banking-insider-threat/
33)https://cybersecurity.att.com/solutions/financial-services
34)https://cert.az/news/2016/informasiya-tehlukesizliyi-ve-ona-qarsi-yonelmis-hucumlar
35)http://www.technet.az/2014/03/25/informasiyanin_t%C9%99hluk%C9%99sizliyin%C9%99-giris/

# РЕЗЮМЕ

Информационная безопасность всегда была одной из самых важных проблем в той или иной форме. С древних времен для предотвращения захвата личной или общедоступной информации использовались специальные типы шифрования и криптографические методы, которые могут быть расшифрованы только отправителем или получателем. Конечно, со временем эти методы, как и другие виды мер, развивались и стали распространяться.

С развитием технологий использование программного обеспечения и продуктов, созданных банками клиентами, растет день ото дня. В этом случае одной из основных проблем банков является обеспечение безопасности создаваемого программного обеспечения и продуктов. Деньги, которые тысячи людей хранят на своих банковских счетах, могут быть украдены киберпреступниками из-за ненадлежащей безопасности информационной системы. Существующее исследование основано на принципе работы, изучении и применении новых технологий, программного обеспечения и современных алгоритмов шифрования информации для решения этого типа проблемы в реальной среде.

Ранее научные исследования, исследования и исследования безопасности информационных систем проводились в узких рамках. Однако в связи с недавним увеличением числа кибератак на финансовые учреждения, правительственные учреждения и частные компании возникает необходимость в научных исследованиях в этой области. Для этого были установлены общие международные стандарты безопасности. В соответствии с этими стандартами были предложены новые решения и концепции для преодоления проблем.

# SUMMARY

Information security has always been one of the most important problems in one form or another. Since ancient times, special types of encryption and cryptographic methods, which can only be decrypted by the sender or recipient, have been used to prevent the seizure of personal or public information. Of course, over time, these methods, as well as other types of measures, developed and began to spread.

With the development of technology, customers' use of software and products created by banks is increasing day by day. In this case, one of the main problems of banks is to ensure the security of the created software and products. The money that thousands of people keep in their bank accounts can be stolen by cybercriminals due to improper security of the information system. Existing research is based on the principle of operation, study and application of new technologies, software and modern information encryption algorithms to solve this type of problem in a real environment.

Previously, the scientific research, study and study of the security of information systems was carried out in a narrow framework. However, with the recent increase in cyber attacks on financial institutions, government agencies and private companies, there is a need for scientific research in this area. For this, common international security standards have been established. According to these standards, new solutions and concepts have been put forward to overcome the problems.