Azərbaycan Respublikası
Mərkəzi Bankı İdarə Heyətinin
"__21___"___dekabr__2015-ci il
tarixli qərarı ilə təsdiq edilmişdir.
Protokol №__43__
D/Reyestr №__316_

Azərbaycan Respublikasında elektron bankçılıq xidmətlərinin göstərilməsinə və bu xidmətlər üzrə təhlükəsizliyin təmin olunmasına dair

Metodoloji Rəhbərlik

1. Ümumi müddəalar

Bu Metodoloji Rəhbərlik Azərbaycan Respublikasının ərazisində elektron bankçılıq xidmətlərinin növlərinə, təqdim edilməsi və istifadəsi üzrə tələblərə, habelə elektron bankçılıq xidmətlərinin etibarlılığının və təhlükəsizliyinin artırılmasına dair tövsiyələri müəyyən edir.

2. Anlayışlar

2.1. Bu Metodoloji Rəhbərlikdə istifadə olunan anlayışlar aşağıdakı mənaları ifadə edir:

2.1.1. **elektron bankçılıq xidməti (bundan sonra - E-bankçılıq xidməti)** - müvafiq proqram təminatı, elektron autentifikasiya üsulu və kommunikasiya vasitələri ilə istifadəçiyə məsafədən girişi təmin etməklə aidiyyəti hesab üzrə bank əməliyyatlarının aparılması və/və ya məlumatların əldə edilməsi;

2.1.2. **istifadəçi -** E-bankçılıq xidmətindən istifadə edən bank hesabı sahibi və E-bankçılıq xidmətindən istifadə etmək hüququ olan şəxs;

2.1.3. **elektron autentifikasiya** - E-bankçılıq xidmətindən istifadə edərkən müxtəlif texniki və/və ya proqram təminatları (elektron imza, istifadəçi adı və şifrə, birdəfəlik şifrələr, simmetrik şifrələmə, sadə sessiya açarlarının istifadəsi və digər üsullar) vasitəsilə istifadəçinin və əməliyyatın avtorizasiyası prosesi;

2.1.4. **əməliyyatın istinad nömrəsi** - E-bankçılıq xidməti ilə həyata keçirilən hər bir elektron əməliyyat üçün təyin edilmiş təkrarolunmaz eyniləşdirmə nömrəsi;

2.1.5. **təhlükəsizlik prosedurları** - ödəniş sənədlərinin elektron formada tərtibi, emalı, göndərilməsi və qəbul edilməsi zamanı istifadəçinin və əməliyyatın eyniləşdirilməsi üçün nəzərdə tutulan informasiyanın təhlükəsizliyi üzrə proqram texniki vasitələr və təşkilati tədbirlər kompleksi.

3. E-bankçılıq xidmətinin növləri

3.1. E-bankçılıq xidməti istifadəçilərə təqdim etdiyi funksional imkanlar və məruz qala biləcəyi risk səviyyəsindən asılı olaraq məlumat və əməliyyat xarakterli E-bankçılıq xidmətinə ayrılır:

3.1.1. Məlumat xarakterli E-bankçılıq xidməti istifadəçi tərəfindən yalnız məlumatın əldə edilməsinə əsaslanır. Bank və ya poçt rabitəsinin milli operatoru (bundan sonra - bank) bu xidmət vasitəsilə istifadəçilərə bank hesabı, aparılmış əməliyyatlar, həmçinin öz məhsul və xidmətləri barədə məlumatı çatdırır.

3.1.2. Əməliyyat xarakterli E-bankçılıq xidməti istifadəçilərə ödəniş etmək, vəsaiti hesabdan köçürmək, konvertasiya əməliyyatını aparmaq və digər bank xidmətlərini həyata keçirmək imkanlarını verir.

3.2. Bu Metodoloji Rəhbərliyin əhatə dairəsinə E-bankçılıq xidmətinin aşağıdakı növləri aid edilir:

3.2.1. PC bankçılıq xidməti - xüsusi proqram təminatının quraşdırılması ilə elektron cihazlar üzərindən rabitə kanalları vasitəsilə təmin edilən E-bankçılıq xidməti;

3.2.2. internet bankçılıq xidməti - xüsusi proqram təminatı quraşdırılmadan elektron cihazlar üzərindən rabitə kanalları vasitəsilə təmin edilən E-bankçılıq xidməti;

3.2.3. mobil bankçılıq xidməti - xüsusi proqram təminatı quraşdırılmaqla və ya quraşdırılmadan mobil cihazlar (mobil telefon, planşet kompüter və s.) üzərindən mobil rabitə kanalları (GSM, CDMA, 3G, HSPA+, WiFi, LTE və s.) vasitəsi ilə təmin edilən E-bankçılıq xidməti.

4. E-bankçılıq xidmətinin təqdim edilməsi və istifadəsi

4.1. E-bankçılıq xidməti bank ilə istifadəçi arasında bağlanmış müqavilə (kağız və ya elektron formada) əsasında həyata keçirilir.

4.2. Bank istifadəçini müqavilənin ayrılmaz tərkib hissəsi olan E-bankçılıq xidmətindən istifadə qaydaları ilə tanış edir.

4.3. E-bankçılıq xidməti göstərildikdə bank:

4.3.1. server otağının, kommunikasiya vasitələrinin və avadanlıqların, habelə elektron əməliyyatların həyata keçirilməsi üçün istifadə edilən proqram təminatının təhlükəsizliyini təmin edir;

4.3.2. istifadəçiləri autentifikasiya üsulları (E-token, e-imza sertifikatları və s.) və müvafiq proqram təminatı ilə təmin edə bilər;

4.3.3. bu Metodoloji Rəhbərliyin tərkib hissəsi olan Əlavə №1-də qeyd edilən E-bankçılıq xidməti üzrə məsafədən həyata keçirilən hücumların qarşısının alınması tədbirlərini mütəmadi olaraq yerinə yetirir;

4.3.4. "Cinayət yolu ilə əldə edilmiş pul vəsaitlərinin və ya digər əmlakın leqallaşdırılmasına və terrorçuluğun maliyyələşdirilməsinə qarşı mübarizə haqqında" Azərbaycan Respublikası Qanununun tələblərinə əsasən istifadəçinin eyniləşdirilməsini və verifikasiyasını təmin edir;

4.3.5. bu Metodoloji Rəhbərliyin 4.6-cı bəndində qeyd edilən hallar baş verdikdə bu barədə istifadəçini ("Cinayət yolu ilə əldə edilmiş pul vəsaitlərinin və ya digər əmlakın leqallaşdırılmasına və terrorçuluğun maliyyələşdirilməsinə qarşı mübarizə haqqında" Azərbaycan Respublikası Qanununda nəzərdə tutulmuş hallar

istisna olmaqla) müqavilədə nəzərdə tutulmuş qaydada və müddətdə məlumatlandırır;

4.3.6. E-bankçılıq vasitəsilə həyata keçirilən ödəniş əməliyyatına düzgün sərəncam verilməsinin və icra olunmasının yoxlanılması üçün istifadəçini dövri olaraq və ya onun tələbi ilə ödəniş əməliyyatları haqqında məlumatla təmin edir;

4.3.7. istifadəçiləri ödəniş əməliyyatlarının cari icra vəziyyəti və hesab üzrə çıxarışla təmin edir;

4.3.8. həyata keçirilən ödəniş əməliyyatları üzrə məlumatların qanunvericiliyə uyğun olaraq saxlanılmasını təmin edir.

4.4. Bank istifadəçini aşağıdakı hallardan hər hansı biri baş verdikdə dərhal banka bildirişin verilməsi zərurəti haqqında məlumatlandırır:

4.4.1. bank hesabında olan vəsaitdən səlahiyyətsiz olaraq istifadə edildikdə;

4.4.2. bank hesabı üzrə əməliyyatlarda hər hansı səhv və ya uyğunsuzluq aşkar etdikdə;

4.4.3. autentifikasiya məlumatlarına səlahiyyətsiz giriş üzrə şübhə doğuran halları müəyyən etdikdə;

4.4.4. E-bankçılıq üzrə texniki nasazlığın mövcudluğu və ya eyniləşdirmə üsullarında səhv baş verdikdə.

4.5. Bank istifadəçinin müəyyən etdiyi qayda və prosedurlara, həmçinin müqavilə şərtlərinə uyğun olaraq E-bankçılıq xidmətindən istifadə etməsi və elektron autentifikasiya üsullarını (açarlar, şifrələr və s.) məxfi saxlaması barədə məlumatlandırır.

4.6. Bank aşağıdakı hallarda istifadəçiyə E-bankçılıq xidmətinin göstərilməsini müvəqqəti dayandırmaq və ya ləğv etmək hüququna malik olmalıdır:

4.6.1. istifadəçi tərəfindən bankın E-bankçılıq xidməti üzrə qayda və prosedurları və ya istifadəçi ilə bank arasında bağlanmış müqavilə şərtləri pozulduqda;

4.6.2. E-bankçılıq xidmətinin göstərilməsi texniki cəhətdən mümkün olmadıqda;

4.6.3. qanunvericilikdə nəzərdə tutulmuş digər hallarda.

4.7. Bu Metodoloji Rəhbərliyin 4.6-cı bəndində bank tərəfindən E-bankçılıq xidmətinin göstərilməsinin müvəqqəti dayandırılmasına səbəb olan hallar aradan qaldırıldıqdan sonra bank bu haqda qayda və prosedurlarında və ya müqavilədə nəzərdə tutulan qaydada və müddətdə istifadəçini məlumatlandırır.

4.8. Əməliyyat xarakterli E-bankçılıq xidməti vasitəsi ilə aparılmış bank əməliyyatları üzrə ən azı aşağıdakı məlumatlar bankın daxili informasiya sistemində saxlanılır:

4.8.1. E-bankçılıq xidmətinin növü;

4.8.2. əməliyyatın istinad nömrəsi;

4.8.3. əməliyyatın həyata keçirilməsi tarixi və vaxtı;

4.8.4. əməliyyatın təyinatı;

4.8.5. əməliyyatın məbləği;

4.8.6. əməliyyatın valyutası;

4.8.7. emitent (ödəyiciyə xidmət göstərən) bankın və benefisiar (vəsait alana xidmət göstərən) bankın rekvizitləri;

4.8.8. ödəyicinin və vəsaiti alanın rekvizitləri.

5. E-bankçılıq xidməti üzrə təhlükəsizliyin təmin olunmasına dair tövsiyələr

Tövsiyə 1: Risklərin idarə olunması

5.1. Bank E-bankçılıq xidməti üzrə təhlükəsizliyin təmin olunması və risklərin idarə edilməsi üzrə xüsusi prosedurlara (bundan sonra - təhlükəsizlik prosedurları) malik olur.

5.2. Bankın E-bankçılıq xidməti üzrə təhlükəsizlik prosedurları bankın səlahiyyətli idarəetmə orqanı tərəfindən təsdiq edilir və müntəzəm olaraq icra vəziyyəti yoxlanılır.

5.3. E-bankçılıq xidməti üzrə təhlükəsizlik prosedurlarında ən azı aşağıdakılar nəzərə alınır:

5.3.1. informasiya təhlükəsizliyinin təmin olunması məqsədi ilə məlumatların məxfiliyinin qorunması üsulları;

5.3.2. bank və istifadəçi arasında göndərilən, emal olunan və saxlanılan məlumatın dəqiqliyinin, etibarlılığının və bütövlüyünün təmin edilməsi üsulları;

5.3.3. elektron autentifikasiyanın tətbiq edilməsi üsulları;

5.3.4. istifadəçinin səlahiyyəti olmayan məlumatlara girişinin məhdudlaşdırılması üçün məntiqi və fiziki giriş üzrə tədbirlər;

5.3.5. E-bankçılıq xidmətinin göstərilməsində üçüncü tərəfin (proqram və şəbəkə təchizatçısı) cəlb olunduğu hallarda üçüncü tərəf fəaliyyətini qəflətən dayandırdıqda və ya onunla bağlanılmış müqavilə üzrə öhdəliklərini yerinə yetirə bilmədikdə görüləcək tədbirlər;

5.3.6. informasiya texnologiyaları sahəsində çalışan əməkdaşlar üzrə səlahiyyət bölgüsünün aparılması, habelə onların peşəkarlığının artırılması məqsədilə mütəmadi qaydada təlimlərin təşkil edilməsi.

Tövsiyə 2: Risklərin qiymətləndirilməsi

5.4. Bank texnoloji həlləri, üçüncü tərəfin təqdim etdiyi xidmətləri və istifadəçilərin texniki mühitini nəzərə almaqla E-bankçılıq xidməti üzrə risklərin monitorinqini aparır.

5.5. Bank E-bankçılıq xidmətinə təsir edə biləcək əsas insidentlər üzrə risk ssenarilərini təhlil edir, eləcə də mövcud təhlükəsizlik tədbirlərinin adekvatlığını və effektivliyini qiymətləndirir.

5.6. Risklərin qiymətləndirilməsi nəticəsində E-bankçılıq xidməti üzrə mövcud təhlükəsizlik tədbirlərində, tətbiq edilən texnologiyalarda və prosedurlarda, habelə xidmətlərdə dəyişikliklərin aparılması zərurəti yarandıqda bank, bu dəyişikliklər üçün tələb olunan keçid müddəti ərzində mümkün insidentlərin və fırıldaqçılıq hallarının ehtimalını və təsirini minimallaşdırmaq üçün tədbirlər görür.

5.7. Risklərin qiymətləndirilməsinin ümumi təhlili ildə ən azı bir dəfə aparılır və nəticələr bankın aidiyyəti idarəetmə orqanı tərəfindən təsdiq edilir.

Tövsiyə 3: Baş vermiş insidentin monitorinqi və hesabatlılıq

5.8. Bank baş vermiş təhlükəsizlik insidentlərinin, o cümlədən təhlükəsizliklə bağlı istifadəçi şikayətlərinin real vaxt rejimində qeydiyyatını və monitorinqini aparır. Bank insidentlər üzrə hesabatları bankın aidiyyəti idarəetmə orqanına və zəruri olduqda insident barədə məlumatı hüquq-mühafizə orqanına təqdim edir.

5.9. Bank E-bankçılıq xidməti üzrə baş vermiş insidentlərin reyestrini aparır. Reyestrdə ən azı aşağıdakı məlumatlar qeydə alınır:

5.9.1. E-bankçılıq xidmətinin növü (PC bankçılıq, internet bankçılıq, mobil bankçılıq);

5.9.2. əməliyyatın istinad nömrəsi

5.9.3. insidentin baş vermə səbəbi;

5.9.4. insidentin məzmunu;

5.9.5. insidentin tarixi və vaxtı;

5.9.6. insidentin aradan qaldırılması üçün görülmüş tədbirlər.

Tövsiyə 4: Təhlükəsizlik tədbirləri və onların icrasına nəzarət

5.10. Bank şəbəkəni, internet səhifəni, serverləri və kommunikasiya əlaqələrini sui-istifadə və hücum hallarına qarşı müdafiə etmək üçün uyğun təhlükəsizlik həllərinə malik olur. Saxta internet səhifələrin istifadəsinə məhdudiyyətin qoyulması üçün əməliyyat xarakterli E-bankçılıq xidməti təqdim edən bankın internet səhifəsi genişləndirilmiş yoxlama sertifikatları vasitəsilə eyniləşdirilir.

5.11. Bank şəbəkə, sistem, verilənlər bazası və təhlükəsizlik modulları kimi məntiqi və fiziki əhəmiyyət daşıyan resurslara girişə nəzarət etmək, izləmək və məhdudlaşdırmaq üçün müvafiq funksionallıqlara malik olur. Bank müvafiq loqları və audit fayllarını yaradır, saxlayır və təhlil edir.

5.12. Bank E-bankçılıq xidməti üzrə təhlükəsizlik tədbirlərinin ildə bir dəfədən az olmayaraq auditini aparır. Auditin aparılmasına etibarlı və müstəqil (daxili və ya xarici) mütəxəssislər cəlb edilir.

5.13. Bank E-bankçılıq xidməti üzrə üçüncü tərəflə bağlanan müqavilədə xidmətin təhlükəsizliyi ilə əlaqədar bu Metodoloji Rəhbərlikdə göstərilən tövsiyələrin nəzərə alınmasını təmin edir.

5.14. Üçüncü tərəf fəaliyyətini qəflətən dayandırdıqda və ya öhdəliklərini yerinə yetirmək iqtidarında olmadıqda bankın müştərilərə E-bankçılıq xidmətinin göstərilməsinin ehtiyat variantları, müvafiq üsul və vasitələri qabaqcadan müəyyən olunur.

Tövsiyə 5: Əməliyyatların izlənilməsi

5.15. Bank E-bankçılıq vasitəsilə aparılan bütün əməliyyatların, o cümlədən əməliyyatların icrası üzrə razılığın verilməsi prosesinin istifadəçi tərəfindən izlənilməsini təmin edir.

5.16. Bank izlənilən əməliyyatlar barədə məlumat bazasına hər hansı əlavənin, dəyişikliyin və ya silinmənin loqlarını yaradır.

Tövsiyə 6: İstifadəçinin eyniləşdirilməsi və məlumatlandırılması

5.17. Bank E-bankçılıq xidmətini təqdim etməmişdən əvvəl aşağıdakı məlumatları kağız və ya elektron formada istifadəçilərə açıqlayır:

5.17.1. avadanlıq, proqram təminatı və digər zəruri vasitələrin (antivirus proqramları, firewall və s.), həmçinin fərdiləşmiş təhlükəsizlik alətlərinin (PİN-kod, E-token və s.) reyestri, texniki təsviri, onlardan düzgün və təhlükəsiz istifadə qaydası;

5.17.2. sistemdə ödəniş əməliyyatının daxil edilməsi və avtorizasiyası və/və ya hər bir əməliyyatın nəticəsi də daxil olmaqla məlumatların əldə edilməsi mərhələləri;

5.17.3. elektron autentifikasiya vasitələrinin və ya ödəniş əməliyyatının aparılması üçün avadanlıqların və proqram təminatının itirilməsi və ya oğurlanması zamanı görüləcək tədbirlər;

5.17.4. fırıldaqçılıq və şübhəli hallar aşkar olunduqda tətbiq olunan prosedurlar.

Tövsiyə 7: Gücləndirilmiş istifadəçi autentifikasiyası

5.18. Bank E-bankçılıq xidməti üzrə aparılan əməliyyatın məbləğindən, habelə risk səviyyəsindən asılı olaraq gücləndirilmiş istifadəçi autentifikasiya üsullarından istifadə edir.

5.19.Bank istifadəçinin rahatlığı məqsədilə E-bankçılıq xidməti üçün vahid autentifikasiya üsullarından istifadə edə bilər.

Tövsiyə 8: İstifadəçiyə çatdırılan autentifikasiya üsullarının və/və ya proqram təminatının qeydiyyatının aparılması və onların təchiz edilməsi

5.20. Bank istifadəçinin E-bankçılıq xidmətindən istifadə etməsi məqsədilə autentifikasiya üsullarının və proqram təminatının təhlükəsiz qaydada istifadəçiyə çatdırılmasını və onların qeydiyyatının aparılmasını təmin edir.

5.21. Bank internet resurslarından istifadə etməklə proqram təminatının istifadəçiyə bütöv və dəyişməz şəkildə çatdırılmasını təmin edir.

Tövsiyə 9: Sistemə daxil olma cəhdləri, sistemin fəaliyyəti üzrə sessiya vaxtının başa çatması və autentifikasiyanın həqiqiliyi

5.22. Bank E-bankçılıq xidməti üzrə sistemə daxil olan zaman şifrələrin daxil edilməsi cəhdləri və/və ya sistemin aktiv olmayan fəaliyyət vaxtı üzrə limit təyin edir.

5.23. Autentifikasiya aparılması məqsədi ilə birdəfəlik şifrə istifadə edildikdə bank müəyyən etdiyi minimum tələbə uyğun olaraq belə şifrələrin qüvvədə olma müddətinə limit təyin edir.

Tövsiyə 10: Əməliyyatların monitorinqi

5.24.Bank əməliyyatları avtorizə etməmişdən əvvəl şübhəli əməliyyatları müəyyən etmək üçün fırıldaqçılığı aşkar edən və onun qarşısını alan sistemlərdən istifadə edir.

5.25.Bank E-bankçılıq xidməti üzrə aparılan ödəniş əməliyyatına sərəncamın verilməsi və icrasının gecikməməsi üçün müvafiq vaxt çərçivəsində əməliyyatın məsafədən monitorinq edilməsi və onların qiymətləndirilməsi prosedurlarına malik olur.

5.26.Bank ödəniş əməliyyatından şübhələndikdə təhlükəsizlik məsələləri həll edilənə kimi həmin əməliyyatı blokda saxlayır və bu barədə istifadəçini dərhal məlumatlandırır.

Tövsiyə 11: Ödəniş məlumatlarının qorunması

5.27. Bank istifadəçilərini eyniləşdirmək və autentifikasiya etmək üçün istifadə edilən bütün məlumatların və istifadəçi interfeys vasitələrinin səlahiyyətsiz girişə və ya onların dəyişdirilməsinə qarşı təhlükəsizliyini təmin edir.

5.28. Bank E-bankçılıq xidməti vasitəsilə ödəniş məlumatının mübadiləsini həyata keçirdikdə məlumatların məxfiliyini və tamlığını qorumaq üçün tərəflər arasında şifrələnmənin aparılmasını təmin edir.

Tövsiyə 12: İstifadəçinin maarifləndirilməsi və onunla kommunikasiyanın təşkili

5.29. Bank istifadəçilərlə E-bankçılıq xidmətindən düzgün və təhlükəsiz istifadə edilməsi məqsədilə davamlı olaraq əlaqə yaratmaq üçün ən azı bir təhlükəsiz kommunikasiya vasitəsi yaradır və ondan istifadə qaydaları barədə istifadəçiləri məlumatlandırır.

5.30. Bank bu Metodoloji Rəhbərliyin 4.4-cü bəndində qeyd edilən hallardan biri baş verdikdə istifadəçinin bildirişinin mümkün kommunikasiya vasitələri (ən azı telefon, mobil, internet) ilə sutkanın 24 saatı ərzində fasiləsiz qəbul edilməsini təmin edir (bildirişin qəbul edilməsi tarixi, vaxtı (saat və dəqiqə) və hadisənin təfərrüatının qeydiyyatı göstərilməklə).

5.31. Bank E-bankçılıq xidmətindən istifadə zamanı risklərin minimallaşdırılması məqsədilə istifadəçiləri aşağıdakılar barədə maarifləndirir:

5.31.1. E-bankçılıq xidmətinə daxil olma üzrə autentifikasiya vasitələrinin və digər məlumatların qorunması;

5.31.2. təhlükəsizlik elementlərinin (antivirus proqramları, şəbəkə qoruyucusu (firewall), təhlükəsizlik yenilənmələri (patches)) kompyuterə quraşdırılması və yenilənməsi üzrə şəxsi kompyuterin təhlükəsizliyinin təmin edilməsi;

5.31.3. istifadəçinin əmin olmadığı proqram təminatını internetdən istifadə etməklə yükləməsi ilə bağlı məruz qalacağı əhəmiyyətli təhlükələrin və risklərin nəzərə alınması;

5.31.4. bankın həqiqi internet səhifəsindən istifadə etməsi.

Tövsiyə 13: Bildirişlərin və limitlərin təyin edilməsi

5.32. E-bankçılıq xidməti ilə həyata keçirilən ödəniş əməliyyatlarının məbləği üzrə limit bankın daxili qayda və prosedurlarında və/və ya istifadəçi ilə bağlanılan müqavilə əsasında müəyyən edilir.

5.33. Bank şübhəli ödəniş əməliyyatları aşkar etdikdə istifadəçiyə mümkün kommunikasiya vasitələri (telefon, SMS, elektron poçt ünvanı və s.) ilə dərhal məlumat verir.

Tövsiyə 14: Ödəniş sərəncamının verilməsi və icra statusu barədə məlumatın istifadəçi tərəfindən əldə olunması

5.34. Bank E-bankçılıq xidməti üzrə istifadəçinin müraciətinə əsasən onları sistemdən son istifadə tarixi və saatı, habelə son uğursuz daxilolma cəhdinin tarixi və saatı haqqında məlumatlarla təmin edir.

5.35. Bank istifadəçiyə E-bankçılıq xidməti vasitəsilə apardığı əməliyyatların icra statusuna, həmçinin hesabı üzrə qalığa nəzarət etmək imkanı yaradır.

Azərbaycan Respublikasında elektron bankçılıq xidmətlərinin göstərilməsinə və bu xidmətlər üzrə təhlükəsizliyin təmin olunmasına dair Metodoloji Rəhbərliyə Əlavə № 1

E-bankçılıq xidmətlərindən istifadə zamanı məsafədən həyata keçirilən hücumların növləri, onların aşkar edilməsi və qarşısının alınması üzrə tədbirlər

№	Məsafədən hücumların növləri	Hücumların qısa təsviri	Hücumların aşkar edilməsi və onların qarşısının alınması tədbirləri
1	Back doors (Arxa yol)	"Back door" təhlükəsizlik nəzarəti keçmədən proqramçıların tətbiqi proqramlara və ya əməliyyat sistemlərinə daxil olması üçün yazılmış proqram kodudur. "Back door" həm məlumatın daxil edilmə ardıcıllığı, həm də xüsusi giriş hüquqları verilən istifadəçi kimliyi vasitəsilə istifadə oluna bilər. Proqramçılar hazırlanan proqramlardakı səhvlərin yoxlanılmasında və onlara nəzarət edilməsində sürətli giriş əldə etmək məqsədilə "back door"lardan istifadə edirlər. Proqramdakı səhvlər yoxlanıldıqdan sonra "back door" aradan qaldırılmadıqda təhlükəsizlik problemi yaranır. Bundan əlavə proqrama hücum edən istifadəçi sistemə giriş əldə etdikdən sonra özünün gələcək fəaliyyəti üçün "back door" yarada bilər.	➢ üçüncü tərəfdən məhsullarında heç bir sənədləşdirilməmiş "back door"un olmamasını təsdiq edən sertifikatlar əldə etmək və yalnız etibarlı mənbələrdən sistemləri qəbul etmək; ➢ sistemlərin real rejimdə istismarından əvvəl "back door"ların mövcud olmamasını aparılan sınaqlarla təsdiq edən prosedurları tətbiq etmək; ➢ real rejimdə istismarda olan sistemlərin tamlığının (dəyişikliklərə uğramadığının) yoxlanılması məqsədilə sistemlərin "bütövlüyü" sınaqlarını həyata keçirtmək.

2	Brute force (Kobud qüvvə metodu)	“Brute force” hücumu şifrələnmiş məlumatların əldə edilməsi məqsədilə istifadə edilir. Bu hücum zamanı əldə edilən şifrələnmiş məlumatlar xüsusi proqram təminatı vasitəsilə deşifrələnir və məlumatlarda saxlanılan şifrələrə, istifadəçi adlarına və məlumatlara giriş əldə edilir. Hücum edən istifadəçi məlumatlara giriş əldə etdikdən sonra özünün gələcək fəaliyyəti üçün “back door” yarada bilər.	➢ məlumatların, istifadəçi adlarının və şifrələrin məxfiliyini qorumaq məqsədilə mürəkkəb şifrələmə texologiyasından və sertifikatın idarəedilməsi metodundan istifadə etmək; ➢ mürəkkəb şifrə siyasətini tətbiq etmək (şifrələrin minimum uzunluğu və dəyişdirilmə dövrü, yenidən istifadə tələbləri və s.); ➢ sistemlərdəki təhlükəsizlik zəifliklərinin və şifrələnmə metodunun mürəkkəbliyinin müəyyən edilməsi məqsədilə sanksiya olunmamış kənardan müdaxilə testlərini həyata keçirmək; ➢ təhlükəsizlik tədbirləri (xüsusilə şifərlərin müəyyən edilməsi sahəsində) üzrə istifadəçiləri maarifləndirmək.
3	Xidmətlərdən imtina (denial of service - DOS)	“Xidmətlərdən imtina” (DOS) şəbəkə və ya sistemə giriş hüquqlarının əldə edilməsinə hədəflənmir. DOS sistemə və ya şəbəkəyə həddindən artıq məlumatların və ya sorğuların göndərilməsi ilə həm sistemin, həm də şəbəkənin işinin dayandırılmasına yönləndirilmiş hücumdur. DOS hücumu bir və ya bir neçə mənbələrdən həyata keçirilə bilər. Paylanılan DOS (Distributed DOS) hücumunda isə hücum edən şəxs məqsədli şəkildə onlayn DOS hücumunu bir neçə və ya	➢ sistemlərin fəaliyyətində zəruri olmayan şəbəkə trafikini bloklaşdırmaq məqsədilə uyğun şəbəkə təhlükəsizliyini tətbiq etmək; ➢ yalnız avtorizasiya edilmiş mənbələrdən trafiki qəbul etmək üçün internet provayderləri ilə danışıqlar aparmaq; ➢ uyğun ehtiyat və bərpaetmə mexanizmləri yaratmaq; ➢ sistemlərin və şəbəkənin DOS və/və ya paylanılan DOS

		yüzlərə sistemlərə eyni anda yönləndirə bilər.	hücumlarına qarşı müqavimət gücünün yoxlanılması məqsədilə skan alətlərindən1 və ya sanksiya olunmamış kənardan müdaxilə testlərindən istifadə etmək.
4	Təhlükəsizlik üzrə məlum zəifliklərin qiymətləndirilməsi (exploiting known security vulnerabilities)	Hücum edən istifadəçilər sistemlərə səlahiyyətsiz girişə nail olmaq üçün təhlükəsizlik üzrə məlum zəifliklərindən istifadə edirlər. İnternetdə bu tip zəifliklər haqqında bir çox mənbələr mövcuddur. Alternativ olaraq hücum edən istifadəçilər təhlükəsizlik üzrə zəiflikləri müəyyən etmək məqsədilə xüsusi avtomatlaşdırılmış alətlərdən istifadə edir. Təhlükəsizlik zəiflikləri avadanlıqlar, veb serverlərdə olan proqram təminatları, şəbəkə qoruyucuları (firewalls) və ya veb serverlərdə proqram təminatlarının yaradılması üçün istifadə edilən alətlər ilə əlaqəli ola bilər. Məs: müəyyən təhlükəsizlik üzrə zəiflikləri veb səhifənin məzmununun səlahiyyətsiz olaraq dəyişdirilməsinə imkan yaradır.	➢ serverlərdən və şəbəkə qoruyucularından (firewalls) istifadə edilməyən proqramları və kompyuter proseslərini silmək və ya de-aktiv etmək; ➢ əməliyyat sistemlərinə və sistemlərin tətbiqi proqramlarına ən son təhlükəsizlik paket tapşırıqlarını və yenilənmələri tətbiq etmək; ➢ ən son hücum üsullarının qarşısını almaq məqsədilə effektiv texnoloji imkanlara malik olan proqram və avadanlıq təchiz edən üçüncü tərəfi seçmək; ➢ proqram səhvləri və/və ya protokol nöqsanları (flaws) kimi təhlükəsizlik zəifliklərini müəyyən etmək üçün skan alətlərindən və ya sanksiya olunmamış kənardan müdaxilə testlərindən istifadə etmək; ➢ il ərzində 1 dəfədən az olmamaq şərti ilə xarici təmasla olan avadanlıqları və daxili şəbəkəni penetrasiya testi etmək.
5	Şifrələrin təxmin edilməsi	Şifrələrin təxmin edilməsi proqram təminatı vasitəsilə sistemə və ya şəbəkəyə daxil olmaq məqsədilə bütün mümkün şifrə kombinasiyalarının yoxlanılması üsuludur. Şifrələrin təxmin	➢ mürəkkəb şifrələmə siyasətini tətbiq etmək (şifrələrin minimum uzunluğu və dəyişdirilmə dövrü, yenidən istifadə

[1] Scanning alətlər şəbəkədə, əməliyyat sistemlərində və verilənlər bazasında təhlükəsizlik çatışmazlıqlarını müəyyən etmək və təhlil etmək üçün istifadə edilən mümkün alətlərdir.

	(guessing passwords)	edilməsi hücumlarının bəziləri ən çox istifadə edilən şifrə kombinasiyalarını birinci yoxlamaqla bu prosesi sürətləndirir.	tələbləri və s.); ➢ sərt giriş nəzarəti mexanizmləri tətbiq etmək (bir neçə uğursuz daxil olma cəhdlərindən sonra istifadəçi kimliyini ləğv etmək); ➢ kritik şəbəkə komponentlərində mövcud olan şifrələri dəqiqliklə dəyişmək; ➢ təhlükəsizlik tədbirləri (xüsusilə şifrələrin yaradılması sahəsində) ilə bağlı istifadəçiləri maarifləndirmək.
6	Hijacking (Oğurlama)	"Hijacking" istifadəçi özünü sistemdə təsdiq etdikdən sonra əlaqənin oğurlanması ilə bağlı hücumdur. Ümumiyyətlə hijacking hücumları məsafədən kompyuter (istifadəçinin şəxsi kompyuteri) üzərindən baş verir, lakin, bəzən məsafədən kompyuter və bankların daxili sistemləri arasında marşrut üzərində olan bir kompyuterdən də əlaqəni oğurlamaq mümkündür.	➢ məsafədən giriş əldə etmək üçün mürəkkəb autentifikasiya üsullarını tətbiq etməklə uyğun şəbəkə təhlükəsizliyini həyata keçirmək, məs: məxfi məlumata "hijacking" tətbiq edən şəxsin girişini məhdudlaşdırmaq üçün kritikliyi yüksək olan sessiyalara girişin dövri olaraq dayandırılması və yenidən autentifikasiyanın tələb edilməsi; ➢ uyğun yerlərdə düzgün formada konfiqurasiya edilmiş şəbəkə qoruyucuları (firewalls) quraşdırmaq; ➢ davamlı əsasda şəbəkə trafikinin və ya potensial müdaxilələrin monitorinqini aparmaq; ➢ "Hijacking" hücumları ilə bağlı zəifliklər müəyyən etmək üçün skan alətlərindən və ya sanksiya olunmamış kənardan müdaxilə testlərindən istifadə etmək; ➢ yüksək məxfiliyə malik məlumatlara güclü şifrələnmə

			tətbiq etmək.
7	Təsadüfi nömrə yığma (random dialling or war dialling)	Təsadüfi nömrə yığma hücumu zamanı hücum edən şəxs şəbəkə qoruyucularından və digər təhlükəsizlik mexanizmlərindən kənarda qalan modemlərin müəyyən edilməsi və sanksiya edilməmiş girişin həyata keçirilməsiməqsədilə telefon şəbəkəsində mövcud olan nömrələrin təsadüfi və ya ardıcıl şəkildə yığılması üsuludur.	➢ bütün modemlərə avtorizasiyanın verilməsini və nəzarəti təmin etmək məqsədilə adekvat şəbəkə təhlükəsizliyini təmin etmək, məs: təşkilatın telefon şəbəkəsində olan bütün nömrələri yığmaqla təsadüfi nömrə yığma hücumunu simulyasiya edərək sanksiya edilməmiş modemləri aşkar etmək; ➢ bütün modemləri eyni fikizi məkanda quraşdırmaq; ➢ şəbəkə seqmentlərini şəbəkədə yerləşən sistemlərin və giriş hüquqlarının kritikliyinə əsasən bir-birindən ayırmaq zəruridir. Bu zaman hücum edən şəxs bir şəbəkə seqmentinə sanksiya olunmamış giriş əldə etdiyi halda belə digər kritik şəbəkə seqmentlərinə giriş əldə etməyəcək; ➢ modemləri və digər oxşar qurğuları “Dial-back” rejimində konfiqurasiya edərək, uzaqdan şəbəkəyə qoşulmanı yalnız sanksiya edilmiş modemlər vasitəsilə təmin etmək; ➢ təsadüfi nömrə yığma hücumu ilə bağlı zəiflikləri müəyyən etmək üçün skan alətlərindən istifadə etmək və ya sanksiya olunmamış kənardan müdaxilə testlərindən istifadə etmək.
8	Sniffer	Şəbəkə nəzarətçiləri kimi tanınan “Sniffer” proqram təminatları şəxsi kompyuterlərdə yığılan komandaları (keystroke-ları) müəyyən etməklə şəbəkə vasitəsilə ötürülən məlumatları ələ keçirir.	➢ məlumatların səlahiyyətsiz şəkildə ələ keçirilməsinin qarşısının alınması məqsədilə uyğun şəbəkə təhlükəsizliyini təmin etmək (daxili şəbəkələrin seqmentlərə bölünməsi, şəbəkə qoruyucuları və ruter

			sazlamaları vasitəsilə məxfi məlumatlara giriş hüquqlarının yalnız müvafiq istifadəçi qruplarına verilməsi); ➢ davamlı şəkildə şəbəkə trafikinin və ya mümkün müdaxilələrin monitorinqini aparmaq; ➢ şəbəkə üzərindən ötürülən məlumatların sanksiya edilməmiş şəkildə əldə edilməsi ilə bağlı zəiflikləri müəyyən etmək üçün skan alətlərindən istifadə etmək və ya sanksiya olunmamış kənardan müdaxilə testlərindən istifadə etmək; ➢ təhlükəsizlik tədbirləri üzrə istifadəçiləri maarifləndirmək (istifadəçilərin maşınlara "sniffer"-lərin yüklənməsinin qarşısının alınması); ➢ məlumatların məxfiliyini təmin etmək üçün güclü şifrələnmə və autentifikasiya üsulları tətbiq etmək.
9	Sosial mühəndislik [2] (social engineering)	Sosial mühəndislik informasiya və ya giriş əldə etmək məqsədilə istifadə olunan sosial texniki üsuldur. Bu zaman hücum edən şəxs özünü səlahiyyətli bir şəxs (helpdesk əməkdaşı və ya təchizatçı) kimi təqdim edərək istifadəçinin kimliyini və şifrəsini ona bildirməyə cəhd göstərə bilər. Bundan əlavə, hücum edən şəxs öz gələcək fəaliyyəti üçün yeni istifadəçi hesabının açılması ilə bağlı müraciət də edə bilər. Hücum edən şəxs sistem barədə məlumat əldə etmək üçün səlahiyyətli istifadəçini özgəninkiləşdirərək təşkilatın helpdeskinə zəng edə bilər (hücum edən şəxs tərəfindən həqiqi sistem şifrəsini dəyişdirməyi helpdeskdən xahiş etməsi və	➢ xarici tərəflərdən səlahiyyətsiz girişin qarşısının alınması məqsədilə uyğun təhlükəsizlik tədbirləri həyata keçirmək; ➢ sosial mühəndisliyin texniki üsulları barədə tədbirli olmaq üçün helpdesk əməkdaşlarına (müvafiq digər əməkdaşlara) təlimlər keçirmək və məxfi məlumata səlahiyyətsiz girişlə nəticələnən məlumatın hazırlanması barədə təşkilatın siyasəti ilə yuxarıda qeyd edilən işçiləri

[2] Fishing hücumu sosial mühəndisliyə aid olan hücüm növüdür. Fishing müxtəlif vasitələrlə (telefon, elektron poçt ünvanı və s.) şəxs haqqında kifayət qədər məlumatların əldə edilməsi yolu ilə, həmin şəxsin adına saxta kart hesablarının açılması və daha sonra qeyri qanuni məqsədlər üçün istifadə olunmasıdır.

		s.)	təlimatlandırmaq; ➢ sosial mühəsndisliyə qarşı mübarizə aparmaq məqsədilə təhlükəsizlik tədbirləri ilə bağlı istifadəçiləri müvafiq qaydalarla təmin etmək.
10	Spoofing	"Spoofing" şəbəkəni aldatmaq məqsədi daşıyaraq şəbəkələrə və ya məxfi məlumatlara giriş əldə etmək üçün səlahiyyətsiz kompyuter sistemini səlahiyyətli kompyuter sistemi kimi tanıyır. Nümunə olaraq, hücuma məruz qalan istifadəçi öz şəxsi cihazından istifadəçi adı və şifrəsini daxil etdikdən sonra (məsələn, şəxsi kompyuteri) təşkilatın veb səhifəsi ilə autentifikasiya edilmiş sessiya yaradır. Hücum edən şəxs bu sessiyanı ələ keçirməklə istifadəçinin cihazının İP ünvanını oğurlayaraq həmin cihazı imitasiya edərək sistemə giriş əldə edə bilər. Bu halda, sanksiya edilmiş istifadəçinin sessiyasına heç bir təsir olmadığından kənar müdaxilədən xəbərdar olmaya bilər.	➢ autentifikasiya edilmiş sessiya üzərindən ötürülən məlumatların təhlükəsizliyinin təmin edilməsi məqsədilə yalnız İP ünvanı əsasında deyil, həmçinin sessiya üçün unikal olan şifrələnmiş eyniləşdirməyə əsaslanan autentifikasiya üsulları tətbiq etmək; ➢ lazımi qaydada konfiqurasiya edilmiş şəbəkə qoruyucusunu uyğun yerlərdə quraşdırmaq; ➢ davamlı şəkildə şəbəkə trafikini və ya kənardan potensial müdaxilələrin monitorinqini aparmaq.
11	Troya atları (trojan horses)	"Troya atları" sistemlərin normal əməliyyatlarına heç bir mənfi təsir göstərməyən, amma məlumat toplamaq və ya sistemin idarəetməsini ələ keçirmək kimi ziyanverici prosesləri özündə cəmləşdirən proqramlardır. "Troya atları" elektron məktublara (kompyuter oyunu kimi) əlavə oluna bilər və sistemə qadağan olunmamış girişə icazə verən "back door" (yuxarıda bax) yarada bilər. "Troya atları" hücum edən şəxsin fəaliyyətinin izlənilməməsi məqsədilə loqlaşdırma və digər məlumatları özündə saxlamaya bilər. Bu proqramların ən ilkin formalarından biri sistemdə saxta giriş ekranı göstərməklə istifadəçi tərəfindən daxil edilən istifadəçi adı və şifrəni əldə etməyə imkan verən proqram təminatıdır.	➢ sistemlərin real rejimdə istismara verilməsi ilə bağlı zəruri dəyişikliklərin idarəedilməsi prosedurlarını tətbiq etmək və sistemdə "Troya atları"nın olmadığını təsdiq edən testləri həyata keçirmək; ➢ istifadə olunan proqramların müntəzəm olaraq tamlığını yoxlamaq; ➢ məlumat təhlükəsizliyi siyasətini formalaşdırmaq və "Troya atları"na qarşı müdafiə olunmaq üçün uyğun təhlükəsizlik tədbirləri üzrə daxili işçi heyətinə müvafiq təlimlər keçirmək (məsələn, elektron poçt ünvanı və ya

			internetin düzgün istifadə edilməməsinə qarşı sərt siyasət); ➢ istifadəçiləri elektron məktublara əlavə edilmiş faylların açılması və internetdən istifadə ilə bağlı təhlükəsizlik tədbirləri barəsində müvafiq qaydalarla təmin etmək.
12	Viruslar	Kompyuter virusları başqa bir kodda yerləşdirilə bilinən və özü özünü aktivləşdirə bilən kompyuter proqramlarıdır. Aktiv olduqda şəbəkənin və ya sistemlərin dağılması ilə nəticələnəcək ziyanverici fəaliyyətləri həyata keçirə bilər. Virus proqramları bir çox platformalara, məlumat bazalarına, sistemdəki cihazlara və şəbəkə vasitəsilə əlaqələndirilən bir çox sistemə yayıla bilər. Virus proqramları elektron məktublardakı əlavələrə yerləşdirilə bilər və bu fayl açıldıqda aktivləşə bilər.	➢ üçüncü tərəf ilə müqavilənin bağlanması zamanı üçüncü tərəfin öhdəliklərində "banka daxil olan informasiya protokollarının viruslara qarşı yoxlanılması" bəndinin olmasını təmin etmək; ➢ yenilənmiş virus skan alətlərindən istifadə etmək; ➢ məlumat təhlükəsizliyi siyasətini formalaşdırmaq və kompyuter viruslarına qarşı müdafiə olunmaq üçün uyğun təhlükəsizlik tədbirləri üzrə daxili işçi heyətini müvafiq qaydalarla təmin etmək (məsələn, internetin və ya elektron poçt ünvanının düzgün istifadə edilməməsinə qarşı sərt siyasət); ➢ istifadəçiləri elektron poçt ünvanında faylların açılması və internetdən istifadə ilə bağlı təhlükəsizlik tədbirləri barəsində müvafiq qaydalarla təmin etmək.