Azərbaycan Milli Elmlər Akademiyası
İNFORMASİYA TEXNOLOGİYALARI İNSTİTUTU

Yadigar İmamverdiyev

İNFORMASİYA TƏHLÜKƏSİZLİYİ terminlərinin izahlı lüğəti

Bakı - 2015

İmamverdiyev Y.N. **İnformasiya təhlükəsizliyi terminlərinin izahlı lüğəti.** Bakı: "İnformasiya Texnologiyaları" nəşriyyatı, 2015, 160 səh**.**

Təqdim olunan izahlı lüğətdə informasiya təhlükəsizliyi üzrə elmi və kütləvi ədəbiyyatda rast gəlinən 600-dən çox ingilis dilli termin toplanmış və onların azərbaycan dilində tərcüməsi variantı verilmişdir. Terminlər informasiya təhlükəsizliyi üzrə elmi və praktiki fəaliyyətin əsas istiqamətlərini əhatə edir.

İnformasiya təhlükəsizliyi üzrə ixtisaslaşan mütəxəssislər, tələbələr və elmi tədqiqat aparan şəxslər üçün nəzərdə tutulmuşdur.

Vəsait AMEA İnformasiya Texnologiyaları İnstitutu Elmi Şurasının qərarı ilə çapa məsləhət görülmüşdür.

Elmi redaktor: tex.f.d. R.H.Şıxəliyev

ISBN: 978-9952-434-72-9

Mündəricat

Giriş.....4
A……7
B……..16
C……..23
D……..44
E……...52
F……...56
G……..…61
H……..…63
I……..…...65
J……..…...73
K……..…74
L……..…..76
M……...…78
N……..…..…82
O……..……84
P……...……88
Q……..…96
R……...…97
S……..…101
T……....…112
U……....…117
V……....…118
W……....……120
X……....…124
Z……....……125
Qısaltmalar.....126
Ədəbiyyat…….....158

Giriş

Azərbaycan dili milli dövlətçiliyin başlıca rəmzlərindən biridir. Azərbaycan Respublikası Prezidentinin 9 aprel 2013-cü il tarixli sərəncamı ilə təsdiq edilmiş "Azərbaycan dilinin qloballaşma şəraitində zamanın tələblərinə uyğun istifadəsinə və ölkədə dilçiliyin inkişafına dair Dövlət Proqramı" Azərbaycan dilinin zənginləşməsi və tətbiqi imkanlarının genişləndirilməsi istiqamətində aparılan işlərin yeni səviyyəyə qaldırılmasını tələb edir.

Müstəqillik illərində Azərbaycan dilinin funksional imkanlarının inkişafı istiqamətində məqsədyönlü dövlət siyasəti həyata keçirilmişdir və Azərbaycan dili dövlət və cəmiyyət həyatın bütün sahələrində, o cümlədən ictimai-siyasi və elmi-texniki sahədə geniş istifadə edilir. Nəticədə müasir Azərbaycan dilinin leksik sistemində terminlərin xüsusi çəkisi olduqca böyükdür.

Terminlərə ümumişlək sözlərdən daha çox ehtiyac var. Elmin və texnikanın istənilən sahəsi öz ifadəsini terminlərdə tapır. Terminlər informasiya əldə etmək və paylaşmaq, bilik qəbul etmək və ixtisası mənimsəmək alətidir. Terminologiyanı mənimsəmədən heç bir elm sahəsini öyrənmək olmaz. Məlumdur ki, informasiya ana dili vasitəsilə daha sürətlə qəbul edilir (dekodlaşdırma prosesi) və ötürülür (kodlaşdırma prosesi). Standartlaşdırılmış terminologiya dəqiq ünsiyyət imkanı yaradır, səhv başa düşülmə və səhv interpretasiyadan qaçmağa kömək edir və ünsiyyətin keyfiyyətini yüksəldir.

Müasir dünyada elmi-texniki biliklərin artması nəticəsində dillərdə meydana çıxan sözlərin 90%-dən çoxunu xüsusi sözlər təşkil edir. Bəzi elmlərdə terminlərin sayının artma sürəti ümumişlək sözlərin sayının artma sürətini qabaqlayır və bəzi elmlərdə terminlərin sayı qeyri-xüsusi sözlərin sayından çoxdur.

Terminologiya qloballaşma və sürətli elmi-texniki tərəqqi şəraitində xüsusi əhəmiyyət qazanır. Hazırda dünyada 20 mindən çox terminoloji standart mövcuddur. Onların əsas hissəsi inkişaf etmiş sənaye ölkələrində yaradılmış milli standartlardır. Bundan

başqa, beynəlxalq standartlar, regional standartlar, şirkətlərin və beynəlxalq təşkilatların standartları da vardır. Bir sıra böyük şirkətlər terminologiyanın menecmetinə şirkətin qloballaşma strategiyasının tərkib hissəsi kimi baxırlar, şirkətin standart terminologiyasından istifadəni korporativ mədəniyyətin vacib komponenti kimi qəbul edirlər.

Qloballaşma şəraitində terminologiya strateji resursdur və ölkənin inkişafında vacib rol oynayır. Ölkə vətəndaşlarının səmərəli iqtisadi, texniki və elmi ünsiyyət bacarıqları düzgün və standartlaşdırılmış terminologiyadan istifadə ilə inkişaf etdirilir. İstənilən ölkənin terminologiya təcrübəsi müxtəlif sahələrdə ünsiyyəti genişləndirir və rəsmi dilin funksional dil imkanları inkişaf edir.

Beləliklə, terminologiya ölkədə iqtisadi, siyasi, elmi, texniki ünsiyyəti təmin edən vahid informasiya fəzasının yaradılmasına imkan verən inteqrasiya faktorlarından birinə çevrilir. Bunu nəzərə alaraq, yuxarıda istinad edilən Dövlət Proqramı terminologiya sahəsində kompleks tədbirlərin həyata keçirilməsini nəzərdə tutur.

Hər bir predmet sahəsində inkişafla əlaqədar terminlərin sayı artır, bu informasiya təhlükəsizliyi sahəsində daha sürətli və dinamikdir. İnformasiya təhlükəsizliyi sahəsində yeni terminlərin sürətlə meydana çıxması mütəxəssislər qarşısında bir sıra ciddi terminşünaslıq problemləri qoyur. İnformasiya təhlükəsizliyi sahəsində vahid anlayışlar sisteminin (terminlərin və tərifl ərin) yaradılması informasiya təhlükəsizliyi üzrə elmi tədqiqatların prioritet problemləri sırasına daxil olur.

İnformasiya təhlükəsizliyi üzrə terminlərin formalaşmasında bir cəhəti xüsusilə vurğulamaq lazımdır. AMEA İnformasiya Texnologiyaları İnstitutunda AMEA-nın həqiqi üzvü, akademik Rasim Əliquliyevin bilavasitə rəhbərliyi altında informasiya təhlükəsizliyi sahəsində 20 ildən artıq müddətdə elmi-tədqiqat işləri aparılır. Həmin müddət ərzində informasiya təhlükəsizliyi üzrə 10-dan çox fəlsəfə doktoru hazırlanmışdır. İnstitutun Tədris-İnnovasiya Mərkəzində bir sıra dövlət təşkilatlarının əməkdaşları üçün müntəzəm kurslar təşkil olunur. Eyni zamanda, institut əməkdaşları

bir sıra ali məktəblərdə informasiya təhlükəsizliyinin müxtəlif istiqamətləri üzrə mühazirələr və seminar məşğələləri aparırlar. Azərbaycan dilində informasiya təhlükəsizliyinin müxtəlif istiqamətləri üzrə ona yaxın kitab nəşr olunmuşdur. Sadalanan bütün proseslərdə müzakirələr azərbaycan dilində aparılmışdır və bunlar informasiya təhlükəsizliyi üzrə terminlərin formalaşmasında əhəmiyyətli rol oynamışdır.

Qeyd etmək lazımdır ki, Rabitə və Yüksək Texnologiyalar Nazirliyində (RYTN) fəaliyyət göstərən Standartlaşdırma üzrə "İnformasiya-kommunikasiya texnologiyaları" Texniki Komitəsi (TK 05) tərəfindən mövcud beynəlxalq standartlar əsasında bir sıra informasiya təhlükəsizliyi standartları işlənmişdir və bu standartlarda da bir sıra informasiya təhlükəsizliyi terminlərinə tərifər verilir.

Təqdim olunan vəsaitdə informasiya təhlükəsizliyi üzrə elmi və kütləvi ədəbiyyatda rast gəlinən 600-dən çox ingilis dilli termin toplanmışdır və onların azərbaycan dilində tərcüməsi variantı verilmişdir. Terminlər informasiya təhlükəsizliyi üzrə elmi və praktiki fəaliyyətin əsas istiqamətlərini əhatə edir. Aydındır ki, bu vəsait çərçivəsində informasiya təhlükəsizliyi üzrə terminlərin kiçik bir hissəsini əhatə etmək mümkün olmuşdur.

A

A3
GSM (**Global System for Mobile Communications**, əvvəllər **Groupe Spécial Mobile**) standartlı mobil rabitə şəbəkəsində abonentin autentifikasiyası üçün kriptoqrafik alqoritm.

A5
GSM standartlı mobil rabitə şəbəkələrində mobil terminal ilə baza stansiyası arasında ötürülən trafikin mühafizəsi üçün istifadə edilən axın şifri üçün Avropa standartıdır. Kriptoqrafik açarın uzunluğu 64 bitdir. Kriptoqrafik məhsulların ixracına olan məhdudiyyətlərə görə A5/1 və A5/2 (zəiflədilmiş) kimi iki variantı mövcuddur.

A8
A5 axın şifri üçün seans açarının generasiyası alqoritmi. A3/A8-i reallaşdırmaq üçün COMP 128 heş-funksiyası istifadə edilir.

Acceptable Internet Use Policy (AUP)
İnternetdən münasib istifadə siyasəti − İnternetdən istifadə müddətlərini və şərtlərini, o cümlədən, onlayn davranış və giriş imtiyazlarını təsvir edən yazılı müqavilə. Bu siyasət istifadəçilər tərəfindən imzalanır.

Access
Giriş **–** subyekt və obyekt arasında qarşılıqlı təsir nəticəsində onların birindən digərinə informasiya axını yaranır.

Access category
Giriş kateqoriyası **–** digər obyektlərin paylaşa bildiyi, baxılan obyekti istifadə etməyə səlahiyyət verildiyi resurslara əsaslanan kateqoriya.

Access control
***Girişin idarə edilməsi* (*girişə nəzarət*)** − sistemin resurslarına girişin məhdudlaşdırılması prosesidir, yalnız icazə verilmiş proqramlara, proseslərə və ya başqa sistemlərə (şəbəkədə) girişə imkan verilir.

Access control mechanism
Girişin idarə edilməsi mexanizmi − avtomatlaşdırılmış sistemlərdə icazəsiz girişi aşkarlayan, onun qarşısını alan və qanuni girişə icazə verən avadanlıq və ya proqram təminatı, sistem proseduru, administrator proseduru və onların müxtəlif kombinasiyalarıdır.

Access level
Giriş səviyyəsi − təhlükəsizlik səviyyəsi nişanının verilənlərin kritikliyinin və ya subyektlərin şəffaflığının identifikasiyası üçün istifadə edilən iyerarxik hissəsidir. Giriş səviyyəsi qeyri-iyerarxik kateqoriyalarla birlikdə təhlükəsizlik səviyyəsini təşkil edir.

Access period
Giriş müddəti – göstərilən giriş hüquqlarının qüvvədə olduğu zaman müddəti.

Access permission
Giriş icazəsi – subyektin müəyyən obyektlə əlaqəli olan bütün giriş hüquqları.

Access right
Giriş hüququ – konkret obyektə giriş üçün spesifik əməliyyat tipinə görə subyektə verilən icazə.

Access type
Giriş növü − müəyyən qurğuya, proqrama, fayla və s. giriş hüququnun mahiyyəti (adətən, oxumaq, yazmaq, yerinə yetirmək, əlavə etmək, modifikasiya etmək, silmək).

Accountability
Hesabatlılıq − müəyyən hərəkətlərə görə cavabdehliyi müəyyən etmək üçün sistemin subyektlərinin fəaliyyətini qeyd etməyə və onları fərdi identifikatorlarla əlaqələndirməyə imkan verən sistem xassəsi.

Account harvesting
Hesab toplayan – çox vaxt e-poçt reklamı vasitəsilə başqalarına nəyisə satmağa və ya onları aldatmağa çalışan kompüter spamçılarını, fərdləri göstərmək üçün istifadə edilir.

Accreditation
Akkreditasiya – təhlükəsizlik tədbirlərinin müəyyən edilmiş çoxluğunun həyata keçirilməsinə əsaslanaraq informasiya sisteminin əməliyyatlarına icazə verilməsi və təşkilatın əməliyyatlarına (məqsədlər, funksiyalar, imic və ya nüfuz daxil olmaqla), təşkilatın aktivlərinə və ya əməkdaşlarına olan riskin qəbul edilməsi haqqında səlahiyyətli təşkilatın rəsmisi tərəfindən verilmiş rəsmi qərar.

Active threat
Aktiv təhdid – verilənlərin emalı sisteminin vəziyyətinə bilərəkdən hər hansı icazəsiz dəyişiklik etmək təhlükəsi.

Active wiretapping
Aktiv dinləmə – telefon danışıqlarının verilənləri dəyişdirmək və ya daxil etmək məqsədilə dinlənilməsi.

Advanced Encryption Standard (AES)
Qabaqcıl şifrləmə standartı – elektron məlumatları qorumaq üçün istifadə edilən, ABŞ hökuməti tərəfindən bəyənilmiş şifrləmə alqoritmini müəyyən edir (2000-ci ildən qüvvədədir). AES alqoritmi informasiyanın şifrlənməsi və deşifrlənməsi üçün simmetrik blok şifridir.

Advanced Persistent Threat (APT)
Qabaqcıl davamlı təhlükə – xüsusi hədəfə yönəlmiş gizli və fasiləsiz kompüter hakinqi prosesləri çoxluğu.

Advisory
Bülleten – informasiya sistemlərinə təhlükələrlə bağlı əhəmiyyətli yeni hadisələr və tendensiyalar haqqında bildiriş.

Adware
Reklam proqramları – istifadəçilərin baxdıqları veb-saytlarda üzə çıxan reklamlar verən proqram təminatı. Onlar istifadəçilərin brauzer vərdişlərini də izləyə bilərlər və adətən, istifadəçilərin icazəsi olmadan quraşdırılır.

Aggregation
Aqreqasiya – nisbətən az məlumat verən informasiyanın toplanması və korrelyasiyası yolu ilə mühüm informasiyanın əldə edilməsi.

AH (Authentication Header)
Autentifikasiya başlığı protokolu – IPSec-in nüvəsini təşkil edən üç protokoldan biri (digərləri ESP və IKE). AH protokolu verilənlərin tamlığına və autentikliyinə zəmanət verir. O, paketin tərkibindəki verilənləri imza ilə əlaqələndirir, imza həm göndərənin həqiqiliyini, həm də qəbul edilmiş informasiyanın tamlığını təsdiqləməyə imkan verir.

Aircrack-ng – 802.11 standartlı simsiz lokal şəbəkələri üçün detektor, paket dinləyicisi, WEP və WPA/WPA2-PSK analiz alətlərindən ibarət olan şəbəkə proqram təminatı paketi.

Air-gapped network
Hava boşluqlu şəbəkə – İnternet daxil olmaqla, heç bir başqa şəbəkəyə qoşulmayan və verilənlərin yalnız daxildə ötürülməsinə icazə verən şəbəkə.

Alert
Həyəcan siqnalı – informasiya təhlükəsizliyi hadisəsinin baş verməsi barədə informasiya təhlükəsizliyi vasitələrinin (IDS) generasiya etdiyi xəbərdarlıq (bildiriş).

American National Standards Institute (ANSI)
Amerika Milli Standartlar İnstitutu – sənaye dairələrinin maliyyələşdirdiyi bu təşkilat 1918-ci ildə ABŞ-da yaradılmışdır, məqsədi milli sənaye standartlarının yaradılması və onların ISO standartları ilə uzlaşdırılmasıdır.

Analytical attack
Analitik hücum – analitik metodlardan istifadə etməklə açarı tapmaq və ya kodu sındırmaq cəhdi.

Anti-jam
Anticam – məqsədyönlü maneələr yaradılması cəhdlərinə baxmayaraq, ötürülən informasiyanın qəbul edilməsini təmin edən tədbirlər.

Anti-Malware Testing Standards Organization (AMTSO) http://www.amtso.org/
Zərərli Proqramları Testetmə Standartları Təşkilatı – zərərli proqramların test edilməsi metodologiyalarının keyfiyyətini, relevantlığını və obyektivliyini yüksəltmək məqsədilə 2008-ci ildə yaradılmış beynəlxalq qeyri-kommersiya təşkilatı.

Antispoofing
Antispufinq – filtrasiya və bloklamanın xüsusi halı. Bu mexanizm əsasən interfeyslərdə və məntiqi baxımdan mümkün olmayan istiqamətlərdə meydana çıxan paketləri bloklamaqla saxta və ya saxtalaşdırılmış IP ünvanların fəaliyyətinin qarşısını alır.

Anti-virus program
Antivirus proqramı – zərərli proqramları aşkarlamaq və mümkün olduqca lazımi tədbirlər görmək üçün nəzərdə tutulan proqram təminatı.

Archive file
Arxiv faylı – təhlükəsizlik və ya hər hansı başqa məqsədlərlə sonradan araşdırmaq və ya yoxlamaq üçün saxlanılan fayl.

Asset
Aktiv – təşkilat üçün dəyəri olan və buna görə də mühafizəsi tələb olunan hər hansı bir şeydir. İlkin aktivlər (biznes prosesləri və informasiya) və köməkçi aktivlər (texniki təminat, proqram təminatı, şəbəkə, personal və s.) fərqləndirilə bilər.

Assurance
Etibar − təhlükəsizlik siyasətinin həyata keçirilməsinin korrektliyi və səliqəliyi baxımından sistemin təhlükəsizliyinin təmin edilməsi arxitekturasına və vasitələrinə inamın arxitekturası.

Asymmetric keys
Asimmetrik açarlar – şifrləmə və deşifrləmə, rəqəmsal imzanın yaradılması və yoxlanılması kimi əməliyyatları yerinə yetirmək üçün istifadə edilən əlaqəli iki açar (açıq açar və gizli açar).

AJAX (Asynchronous JavaScript and XML**)**
Asinxron Cava skripti və XML – asinxron tətbiqi veb proqramları yaratmaq üçün kliyent tərəfdə istifadə olunan qarşılıqlı əlaqəli veb texnologiyaları qrupu.

Attack
Hücum − müdafiə sistemindən keçmək cəhdləri. Hücum verilənlərin dəyişdirilməsinə gətirməklə aktiv və ya passiv ola bilər. Hücumun həyata keçirilməsi faktı hələ onun uğurlu olması demək deyil. Hücumun uğur dərəcəsi sistemin zəifliyindən və təhlükəsizlik mexanizmlərinin effektivliyindən asılıdır.

Attack graph
Hücum qrafı – düşmənin sistemi sındırmaq üçün boşluqları istismar edə biləcəyi ardıcıllığı təsvir edir.

Attack Sensing and Warning (ASW)
Hücumun aşkarlanması və xəbər xerilməsi – icazəsiz qəsdli fəaliyyətin aşkarlanması, identifikasiyası, analizi və müvafiq reaksiyanın hazırlanması üçün qərar qəbul edən şəxslərə bildirilməsi.

Attack signature
Hücum siqnaturası – icazəsiz giriş cəhdini göstərən hadisələrin spesifik ardıcıllığı.

Attack surface
Hücum səthi – proqram təminatı mühitində avtorizasiya edilməmiş istifadəçinin verilənləri mühitə daxil etməyə və mühitdən çıxarmağa cəhd edə bildiyi müxtəlif nöqtələrin ("hücum vektorlarının") toplusu.

Audit
1. **Audit** – sistem mexanizmlərinin adekvatlığını qiymətləndirmək, təsbit edilmiş siyasətlərə və istismar prosedurlarına uyğunluğu təmin etmək və mexanizmlərə, siyasətlərə və prosedurlara zəruri dəyişikliklər tövsiyə etmək üçün fəaliyyətin (hərəkətlərin) müstəqil araşdırılması və yoxlanılması.
2. ***Audit*** – sistemdə baş verən hadisələr haqqında toplanan informasiyanın (log-faylların) analizidir. Audit operativ (təxminən real vaxtda) və ya dövri (məsələn, gündə bir dəfə) aparıla bilər.

Audit reduction tools
Auditi azaltmaq alətləri – insan tərəfindən analizi asanlaşdırmaq məqsədilə audit yazılarının həcmini azaltmaq üçün nəzərdə tutulmuş ilkin emal prosesləri.

Audit trail
Audit jurnalı − sistemin subyektlərinin fəaliyyəti barəsində xronoloji nizamlanmış yazıların son nəticənin təftişi məqsədi ilə

əməliyyatların, prosedurların yerinə yetirilməsinə və ya tranzaksiyalar zamanı hadisələrin baş verməsinə səbəb olan və ya şərait yaradan hərəkətlər ardıcıllığının bərpası, baxılması və analizi üçün yetərli olan verilənlər.

Authentication
Autentifikasiya – subyektin doğrudan da özünü təqdim etdiyi şəxs olmasının yoxlanması prosesidir. Autentifikasiya sözünün sinonimi kimi çox vaxt "həqiqiliyin yoxlanması" işlədilir.

- İstifadəçinin, qurğunun və ya sistemin digər komponentinin identifikatorunun yoxlanmasıdır; adətən sistemin resurslarına girişə icazə qərarının qəbul edilməsi üçün istifadə edilir;
- Saxlanılan və ya ötürülən verilənlərin icazəsiz dəyişdirilməsini aşkarlamaq üçün tamlığının yoxlanılması.

Autentification exchange
Autentifikasiya mübadiləsi – informasiya mübadiləsi vasitəsilə obyektin autentifikasiyasını təmin etmək üçün nəzərdə tutulmuş mexanizm.

Authentication information
Autentifikasiya məlumatı − obyektin bəyan edilmiş kimliyinin həqiqiliyini müəyyən etmək üçün istifadə edilən məlumatlar.

Authentication token
Autentifikasiya tokeni – autentifikasiya mübadiləsi zamanı ötürülən autentifikasiya məlumatları.

Automated information system (AIS)
Avtomatlaşdırılmış informasiya sistemi **(*AİS*)** − verilənlərin və informasiyanın yaradılması, ötürülməsi, emalı, yayılması, saxlanması və/və ya idarə edilməsi və hesablamaların aparılması üçün nəzərdə tutulmuş proqram və aparat vasitələrinin çoxluğu.

Automated information system security
Avtomatlaşdırılmış informasiya sisteminin təhlükəsizliyi − AIS-i xidmətdən imtinadan və AİS və verilənləri icazəsiz (bilərəkdən və ya təsadüfi) aşkarlanmaqdan, modifikasiyadan və ya məhv edilməkdən mühafizə edən idarəetmə və nəzarət tədbirlərinin məcmusu.

Authorization
Avtorizasiya − istifadəçiyə, proqrama və ya prosesə *giriş hüquqları*na əsaslanan girişin verilməsi də daxil olmaqla hüquqların verilməsi.

Authorization boundary
Avtorizasiya sərhədi – informasiya sisteminin səlahiyyətli şəxs tərəfindən əməliyyat üçün avtorizasiya edilməli olan bütün komponentləri; informasiya sisteminin qoşulduğu və ayrıca avtorizasiya edilən sistemlər bura daxil edilmir.

Automatic remote rekeying
Açarın məsafədən avtomatik dəyişdirilməsi – qəbuledici terminalın operatoru tərəfindən xüsusi əməliyyatlar edilmədən məsafədəki kriptoqrafik avadanlıqda açarın elektron şəkildə dəyişdirilməsi proseduru.

Availability of data
Verilənlərin əlyetərliyi − verilənlərin istifadəçiyə lazım olan şəkildə; lazım olan yerdə və lazım olan zamanda olması vəziyyəti.

B

Back door
Arxa qapı – təhlükəsizlik mexanizmlərini aldatmaq üçün istifadə edilən avtorizə olunmamış gizli proqram və ya aparat təminatı.

Back Orifice
Sistem administratorlarına kompüteri məsafədən (adətən, İnternetdən) idarə etməyə icazə verən alət. "Cult of the Dead Cow" (cDc) adlı haker klubu tərəfindən 1998-ci ildə yaradılmışdı, iki ildən sonra qrup BO2K və ya Back Orifice 2000 adlandırılan daha yeni versiyanı buraxmışdı. Back Orifice krekerlər tərəfindən troyan vasitəsilə yayıla bilər. Quraşdırılandan sonra hədəf kompüteri məsafədən tam idarə etməyə imkan verir.

Backtracking resistance
İzlənmə müqaviməti – təsadüfi bitlər generatorunun (ing. Random Bit Generator, RBG) çıxış ardıcıllığının gələcəkdə generator sındırıldıqda da iddia olunan təhlükəsizlik səviyyəsində ideal, təsadüfi ardıcıllıqdan fərqlənməyəcək şəkildə qalacağının təminatı.

Backup file
Ehtiyat nüsxə faylı – verilənlərin sonradan bərpasını mümkün etmək üçün yaradılan fayl.

Backup procedure
Ehtiyat nüsxə proseduru – uğursuzluq və ya nasazlıq halında verilənlərin bərpasını nəzərdə tutan prosedur.

Backward recovery
Köhnə versiyanın bərpası – jurnalda qeydə alınmış verilənlərdən və sonrakı versiyalardan istifadə etməklə verilənlərin əvvəlki versiyasının yenidən yaradılması.

Bacterium
Bakteriya – özünü e-poçt vasitəsilə hər bir abonentin ünvan siyahısında olan bütün şəxslərə göndərən proqram.

Bad sectoring
Zədəli sektorların yazılması – zədəli sektorları bilərəkdən diskə yazmaqla surətçıxarmadan qorunma üsulu.

Banner grabbing
Bayraq toplanması – məsafədəki kompüterdə işləyən servislər haqqında məlumat toplamaq üçün istifadə edilən fəaliyyət.

Baseline security
Baza təhlükəsizlik səviyyəsi – informasiya sisteminin konfidensiallıq, tamlıq və əlyetərlik üçün müəyyən edilmiş tələbləri əsasında tələb edilən minimal təhlükəsizlik mexanizmləri.

Bastion host
İstehkam-host – xüsusi təşkil edilmiş və hücuma dayanıqlıq üçün möhkəmləndirilmiş əməliyyat sisteminin əsasında reallaşdırılan şəbəkələrarası ekran.

Bell-LaPadula model
Bell-LaPadula modeli − təhlükəsizlik siyasətinin formal avtomat modelidir, girişin idarə edilməsi qaydaları çoxluğunu təsvir edir. Bu modeldə sistemin komponentləri təhlükəsizlik obyektlərinə və subyektlərinə bölünür. Təhlükəsiz vəziyyət anlayışı daxil edilir və isbat edilir ki, əgər hər bir keçid təhlükəsiz vəziyyəti saxlayırsa (yəni sistemi bir təhlükəsiz vəziyyətdən digər təhlükəsiz vəziyyətə keçirirsə), onda induksiya prinsipinə görə sistem təhlükəsizdir.

Between-the-lines entry
Xəttə qoşulma – kommunikasiya kanalına qoşulmuş qanuni istifadəçinin ani qeyri-aktiv olan terminalının icazəsiz istifadəçi tərəfindən aktiv dinlənilməsi.

Biometrics
Biometriya – şəxsin həqiqiliyini avtomatik yoxlamaq üçün barmaq izi, gözün qüzehli qişası, səs və s. kimi fərdi xarakteristikaları əks

etdirən spesifik atributların istifadəsi ilə bağlı olan identifikasiya texnologiyaları.

Biometric template
Biometrik şablon – biometrik informasiyanın xüsusiyyətləri (məsələn, barmaq izində xırda nöqtələr).

Birthday attack
Ad günü hücumu – heş-funksiyaların kriptoqrafik analizi metodu. Hücum öz adını "ad günü paradoksu"ndan almışdır; müəyyən qrupda iki və ya daha çox insanın ad gününün eyni günə düşməsi ehtimalını hesablamaqdan ibarətdir. Heş-funksiyanın üst-üstə düşən qiymətlərinin hesablanması üçün istifadə edilir.

BISO (Business Information Security Officer)
İnformasiya təhlükəsizliyi xidmətinin mütəxəssisi/meneceri – informasiya təhlükəsizliyi siyasətinin bölmə, məsələn, iqtisadiyyat şöbəsi və ya marketinq xidməti səviyyəsində praktiki həyata keçirilməsi ilə məşğul olur.

Black Hat Briefings
Qara Şlyapa Brifinqləri – rəqəmsal özünümüdafiə ilə əlaqəli mövzular haqqında biliklərini bölüşmək üçün hüquq, texnologiya və akademiya ekspertləri Qara şlyapa brifinqləri konfransı üçün hər il Las Veqasda, Avropada və Asiyada toplaşırlar. Konfransın təşkilatçısı və prezidenti Jeff Mossdur (The Dark Tanget kimi də tanınır). Daha ətraflı məlumatı http:/www.blackhat.com saytında tapmaq olar.

Black Hats
Qara Şlyapalar – haker cəmiyyətinin zərərli və ya kriminal təbəqəsi. Qara şlyapaların arsenalına dağıdıcı kompüter eksploytları daxildir, onlar krakerlərin qisas, sabotaj, şantaj və ya tamahkarlıq motivasiyaları səbəbindən baş verir. Kiber-təbiətli olmayan cinayətlərdə olduğu kimi, Qara şlyapaların eksploytları da

mülkiyyətə və ya adamlara zərər vurmaqla nəticələnə bilər. Yeraltı kompüter dünyasında Qara şlyapaların müxtəlif tipləri mövcuddur, "krekerlər" daha geniş yayılıblar.

Blackout of 2003
2003-cü il elektrik kəsintisi – Şimali Amerika tarixində ən böyük elektrik kəsilməsi 14 avqust 2003-cü ildə ABŞ-ın şimal-şərq və Böyük Göl ərazilərində, Kanadanın Ontario əyalətində baş vermişdi. 2003-cü il elektrik kəsintisi baş ofisi Ohayo ştatının Akron şəhərində olan FirstEnergy korporasiyasının işlətdiyi qurğularda başlamışdı.

Blended attack
Qarışıq hücum – yayılmaq üçün bir çox metoddan istifadə edən zərərli proqram kodu. Məşhur Nimda soxulcanı qarışıq hücumun bir nümunəsidir.

Blinding
Kölgələmə – agentin real girişi və ya real çıxışı bilmədən müştəriyə xidməti (məsələn, funksiyanın qiymətinin hesablanması) kodlaşdırılmış formada təmin etməsi metodu

Block cipher
Blok şifri – kriptoqrafik açardan istifadə etməklə bir dəfəyə informasiya blokunu çevirən simmetrik açarlı kriptoqrafik alqoritm. Blok şifrində giriş blokunun uzunluğu çıxış blokunun uzunluğuna bərabərdir.

Bluejackers
Mavi yeləklər – Bluetooth texnologiyasından istifadə edərək əlaqə saxlayan şəxslərə verilən addır. "Bluejacking" o zaman baş verir ki, bədniyyətli Bluetooth simsiz şəbəkəsindən istifadə edərək başqa bir şəxsin mobil telefonuna anonim mesaj göndərir. Haker cəmiyyətində çoxları onları "*şən zarafatcıllar*" kimi qəbul edirlər –

onları Ağ şlyapaların və Qara şlyapaların arasındakı *boz zona*da yerləşdirirlər.

Blue team
Mavi komanda – Çin Xalq Respublikasının ABŞ-ın təhlükəsizliyinə qarşı ciddi təhlükə olması fikri əsasında birləşən ABŞ siyasətçiləri və jurnalistləri qrupuna verilən qeyri-rəsmi addır.

Boot sector virus
Yükləmə sektoru virusu – özünü sistemin yükləmə sektoruna yazan və əsas yükləmə yazısını yoluxduran virus.

Bootkit (ing. boot – yükləmə və kit – alətlər dəsti)
Butkit – öz kodunu tərpənməz diskdə əsas yükləmə yazısına (Master Boot Record) yazan zərərli proqramdır. Nəticədə diskə ilk müraciət zamanı idarəetmə butkitə verilir, butkit yaddaşa yüklənir və o, tərpənməz diskə müraciətləri ələ keçirərək və onları dəyişərək öz iştirakını maskalayır.

Bot
Bot − istifadəçinin kompüterində onun xəbəri olmadan gizli quraşdırılan və bədniyyətliyə yoluxmuş kompüterin resurslarından istifadə etməklə müəyyən əməlləri yerinə yetirməyə, o cümlədən kompüteri məsafədən idarə etməyə imkan verən zərərli proqramdır.

Botnet (ro**bot** və **net**work sözlərindən yaranmışdır)
Botnet − botlarla yoluxmuş kompüterlərdən ibarət şəbəkədir. Botnetlər adətən, spam göndərilməsi, konfidensial informasiyanın toplanması, xidmətdən imtina hücumları, fişinq üçün istifadə edilir.

Breach
Zədə – kompüter təhlükəsizliyinin bəzi elementlərinin yararsızlığı və ya yararsız vəziyyətə gəlməsidir ki, aşkarlandıqda və ya aşkarlanmadan verilənlərin emalı sisteminə soxulma ilə nəticələnə bilər.

BREACH (Browser Reconnaissance and Exfiltration via Adaptive Compression of Hypertext)
Hipermətnin adaptiv sıxılması vasitəsilə brauzerin izlənməsi və verilənlərin köçürülməsi – HTTP kompressiya (sıxılma) istifadə edilən zaman HTTPS-ə qarşı təhlükəsizlik eksploytu.

Brute force password attack
Kobud güclə parol hücumu – ədədi və ya simvol-rəqəm parolların çoxsaylı kombinasiyalarını sınamaqla giriş əldə etmək metodu.

Buffer overflow
Buferin daşması – buferə və ya verilənləri saxlama sahəsinə ayrılmış həcmdən çox informasiya yerləşdirilməsi. Hücum edənlər sistemi dayandırmağa və ya sistemin idarə edilməsini ələ keçirməyə imkan verən xüsusi hazırlanmış kodu buferə yerləşdirmək üçün bu üsuldan faydalanırlar.

Bug
Baq – proqram təminatında səhv; ehtimala görə bu termin ilk kompüter sistemlərində əməliyyatların pozulmasına səbəb olmuş taxtabiti ilə bağlı real hadisə ilə əlaqədardır.

BUGTRAQ
BUGTRAQ – boşluqlar, onların istismar metodları və boşluqların aradan qaldırılması daxil olmaqla kompüter təhlükəsizliyi problemlərinə həsr edilmiş e-poçt göndərişi siyahısı. 1993-cü il noyabrın 5-də Skott Çasin tərəfindən yaradılmışdır, poçt göndərişi hazırda Symantec Response tərəfindən idarə edilir və http://www.securityfocus.com/archive/1 veb-saytında arxivləşdirilir.

Business Continuity Plan (BCP)
Fəaliyyətin fasiləsizliyi planı – əhəmiyyətli pozuntu zamanı və ondan sonra təşkilatın biznes funksiyalarının necə təmin ediləcəyini təsvir edən təlimatların və ya proseduraların qabaqcadan müəyyən edilmiş toplusu.

Business Impact Analysis (BIA)
Fəaliyyətə təsirin analizi – informasiya texnologiyaları sisteminin tələblərinin, proseslərin və qarşılıqlı asılılıqların analizi; əhəmiyyətli pozuntu halında prioritetləri və sistemin gözlənilməz tələblərini müəyyənləşdirmək üçün istifadə edilir.

Business Recovery-Resumption Plan (BRP)
Fəaliyyətin bərpası planı – əhəmiyyətli pozuntu baş verdikdən sonra biznes-proseslərin necə bərpa ediləcəyini təsvir edən təlimatların və ya proseduraların qabaqcadan müəyyən edilmiş toplusu.

C

Cache cramming
Keş tıxacı – kompüteri normal halda işlədilməyən Java kodunu işə salmağa məcbur edən metod.

Cache poisoning
Keşin zəhərlənməsi (DNS-in zəhərlənməsi və ya DNS keşinin zəhərlənməsi də adlanır) – İnternet ünvanını başqa saxta ünvanla dəyişməklə İnternet serverinin domen adları sisteminin bazasını korlayır.

Call-back
Geri çağırış – elə bir prosedurdur ki, verilənlərin emalı sistemi çağırış terminalını identifikasiya edir, çağırışı ayırır və çağırış terminalını autentifikasiya etmək üçün çağırış terminalına zəng edir.

CAN-SPAM Act of 2003
2003-cü il CAN-SPAM Qanunu – 25 noyabr 2003-cü ildə ABŞ Senatı tərəfindən qəbul edilib (Controlling the Assault of Non-Solicited Pornography and Marketing Act) və İnternet ilə soruşulmayan e-poçtu (spam) göndərən şəxslərə cəzalar nəzərdə tutmaqla dövlət daxilində ticarəti tənzimləyir. Qanun 1 yanvar 2004-cü ildən qüvvəyə minmişdir. Cəzalara 1 milyon dollara kimi yüksək cərimələr və beş ildən çox olmamaqla həbs cəzası daxildir.

Canister
Kanister – ştamplanan və ya çap olunan lent formasında açar materialını saxlamaq və paylamaq üçün istifadə edilən qoruyucu paket növü.

Capability
Mandat – identifikatorun bir növüdür, obyektə giriş yolunu və obyekt üzərində icazə verilən əməliyyatları müəyyən edir.

Capability list
Mandat siyahısı – subyektlərin bütün obyektlərə giriş növlərinin hamısını identifikasiya edən siyahı.

Capstone
Açıq açarlı kriptoqrafiya üçün standartlar toplusunun işlənməsi üçün ABŞ hökumətinin uzunmüddətli layihəsi. Layihə haqqında açıq məlumatlar azdır, layihə 4 hissədən ibarət idi:
- Clipper mikrosxemində realizə edilmiş şifrləmə alqoritmi Skipjack;
- rəqəmsal imza alqoritmi DSA;
- heş-funksiya alqoritmi SHA-1;
- açarların mübadiləsi protokolu (Diffi-Helman sxeminə əsaslandığı güman edilir).

Cascading
Kaskadlama – video-konfrans sistemlərində kaskadlama konfransa bir çox-nöqtəli nəzarət nöqtəsinin (multipoint control unit, MCU) dəstəkləyə bildiyindən daha çox iştirakçının daxil olmasına imkan verən metod.

Certificate
Sertifikat – ən azı aşağıdakıları təmin edən informasiyanın rəqəmsal təqdimatı:
1) onu verən sertifikat mərkəzini identifikasiya edir,
2) onun abunəçisini adlandırır və ya identifikasiya edir,
3) abunəçinin açıq açarını özündə saxlayır,
4) onun istismar dövrünü identifikasiya edir,
5) onu verən sertifikat mərkəzi tərəfindən rəqəmsal imzalanır.

Certificate Policy (CP)
Sertifikat siyasəti – sertifikatın idarə edilməsi ərzində yerinə yetirilən elektron tranzaksiyalara köklənmiş inzibati siyasətin xüsusi formasıdır. Sertifikat siyasəti rəqəmsal sertifikatların yaradılması, istehsalı, paylanması, uçotu, nüfuzdan düşmüşlərin ləğvi ilə

əlaqədar bütün aspektləri nəzərə alır. Sertifikat siyasəti həmçinin sertifikatlara əsaslanan təhlükəsizlik sistemi vasitəsilə qorunan kommunikasiya sistemindən istifadə edən tranzaksiyaları da idarə edə bilər. Kritik sertifikat genişlənmələrinə nəzarət etməklə belə siyasətlər və əlaqədar məcburiyyət texnologiyaları xüsusi tətbiqlər üçün tələb edilən təhlükəsizlik servislərinin təmin edilməsini dəstəkləyə bilərlər.

Certification
Sertifikatlaşdırma – verilənlərin emalı sisteminin bütövlükdə və ya qismən təhlükəsizlik tələblərinə uyğun gəlməsi haqqında üçüncü tərəfin zəmanət verməsi proseduru.

Certification Authority (CA)
Sertifikat Mərkəzi – açıq açar sertifikatlarını verən və ləğv edən etibarlı subyekt.

Certification Practice Statement (CPS)
Sertifikat qaydaları bəyannaməsi – spesifik tələblərə (məsələn, sertifikat siyasətində və ya servis üçün müqavilədə müəyyən edilmiş tələblərə) uyğun olaraq sertifikatların verilməsi, dayandırılması, ləğvi, yenilənməsi və onlara müraciətlərin təmin edilməsi zamanı Sertifikat Mərkəzinin istifadə etdiyi qaydaların bəyan edilməsi.

Certified Ethical Hacker (CEH)
Sertifikatlı etik haker – mütəxəssislərə *EC-Council* tərəfindən informasiya təhlükəsizliyi üzrə verilən sertifikatdır. ABŞ Müdafiə Nazirliyi tərəfindən tanınır. Şəbəkə təhlükəsizliyi sahəsində müvafiq səviyyədə biliklərin olmasını təsdiq edir. Etik hakerlər, adətən təşkilatlar tərəfindən istifadə olunurlar, informasiya təhlükəsizliyi boşluqlarını aşkar etmək və aradan qaldırmaq məqsədilə hakerlərin istifadə etdikləri eyni metodlardan istifadə edərək şəbəkələrə və ya kompüter sistemlərinə daxil olmağa cəhdlər edirlər.

CEH sertifikat imtahanı şəbəkə protokollarının, əməliyyat sistemlərinin və tətbiqi proqramların boşluqları, troyanlar, viruslar, rutkitlər, informasiyanın toplanması, şəbəkənin daranması və resursların inventarlaşdırılması, veb-serverlərin və simsiz şəbəkələrin sındırılması, informasiya təhlükəsizliyi vasitələrinin aldadılması, nüfuzetmə testləri, DoS hücumların, SQL-inyeksiya hücumlarının həyata keçirilməsi, seansların ələ keçirilməsi və s. kimi sahələri əhatə edir.

Chain of custody (CoC)
Mühafizə zənciri – fiziki və ya elektron sübutların toplanmasını, qorunmasını, saxlanmasını, ötürülməsini, analizini və məhv edilməsini göstərən xronoloji sənəd və ya kağız jurnal.

Challenge-response protocol
Sorğu-cavab protokolu – autentifikasiya protokoludur, verifikator iddiaçıya sorğu göndərir (adətən, təsadüfi qiymət), iddiaçı onu ortaq sirlə birləşdirir və cavab generasiya edir, onu verifikatora göndərir. Verifikator ortaq sirri bilir, buna görə cavabı müstəqil hesablaya və onu iddiaçının göndərdiyi cavabla müqayisə edə bilər. Əgər onlar eyni olsalar, iddiaçı autentifikasiya edilmiş sayılır.

CHAP (Challenge Handshake Authentication Protocol)
Çağırış-əlsıxma autentifikasiya protokolu – aşağıdakı kimi işləyir: Məsafədən giriş serveri kliyentə təsadüfi simvollar ardıcıllığından və öz adından ibarət sorğu (challenge) göndərir. Məsafədən giriş kliyenti MD5 alqoritmi ilə sorğu və istifadəçinin parolundan hesablanmış heşin əsasında yeni heş hesablayır. Kliyent hesablanmış MD5 heşini öz adı ilə birlikdə məsafədən giriş serverinə göndərir. Məsafədən giriş serveri istifadəçinin parolu əsasında heşi hesablayır və istifadəçidən alınmış heşlə müqayisə edir. Üst-üstə düşmə halında məsafədən giriş kliyentinin uçot verilələri həqiqi hesab olunur. Beləliklə, parol açıq şəkildə göndərilmir, lakin məsafədəki tərəf istifadəçinin parolunu açıq şəkildə saxlayır.

Checking code
Yoxlama kodu – icazəsiz nüsxə olub-olmadığını təyin etmək üçün diskin bir hissəsini oxuyan maşın əmrləri.

Checksum
Nəzarət cəmi – tamlığa nəzarət mexanizmidir, əsasən verilənlərin saxlanması və şəbəkə protokollarında istifadə edilir. Nəzarət cəmi müəyyən alqoritmlə hesablanır, verilənlərə əlavə edilir və yadda saxlanır. Nəzarət cəmini bilən şəxs həmin verilənlər üçün nəzarət cəmini hesablayıb müqayisə etməklə məlumatın dəyişdirilmədiyinə əmin ola bilər. Bəzi səhvlər – məlumatda baytların yenidən nizamlanması, sıfırlardan ibarət baytların daxil edilməsi və ya çıxarılması, nəzarət cəmini əks istiqamətlərdə atıran və azaldan səhvlər – nəzarət cəmində aşkarlana bilmir. Bu problemdən yaxa qurtarmaq üçün ***kriptoqrafik nəzarət cəmləri*** – kriptoqrafik heş funksiyalar daxil edilir.

Chief Information Officer (CIO)
İnformasiya direktoru – təşkilatın aşağıdakılar üçün məsul rəsmi şəxsi:
1) İnformaiya texnologiyalarının əldə edilməsinin və informasiya resurslarının idarə edilməsinin qanunvericiliyə, sərəncamlara, göstərişlərə, siyasətlərə, qaydalara və rəhbərliyin müəyyən etdiyi prioritetlərə uyğun tərzdə həyata keçirilməsini təmin etmək üçün təşkilatın icra rəhbərliyinə və digər yuxarı idarəetmə heyətinə məsləhət və digər köməyin təmin edilməsi;
2) Təşkilat üçün nöqsansız və inteqrativ informasiya texnologiyaları arxitekturasının işlənməsi, gerçəkləşdirilməsi, saxlanması və inkişaf etdirilməsi;
3) İş proseslərinin təkmilləşdirilməsi də daxil olmaqla təşkilat üçün bütün əsas informasiya resurslarının idarə edilməsi proseslərinin effektiv və səmərəli layihə və istismarını təkmilləşdirmək.

Chief Information Security Officer (CISO)
İnformasiya təhlükəsizliyi üzrə direktor – təşkilatda baş verən biznes proseslərinə adekvat informasiya təhlükəsizliyi siyasətinin işlənməsinə və həyata keçirilməsinə cavabdehdir.

Chosen-plaintext attack
Seçmə açıq mətn hücumu – kriptoanalitikin qeyri-məhdud sayda açıq mətn məlumatlarını əldə edə və uyğun gələn şifrlənmiş mətni nəzərdən keçirə bildiyi analitik hücum.

Common Intrusion Detection Framework (CIDF)
Müdaxilələrin aşkarlanması üzrə vahid arxitektura – aşağıdakıları müəyyən edir:

- hücumlar, boşluqlar, hadisələr və hadisələrə reaksiya üsulları haqqında informasiyanı təsvir etmək üçün verilənlər modeli;
- IDS komponentlərinin qarşılıqlı əlaqəsi modeli;
- IDS komponentlərinin qarşılıqlı əlaqəsinin protokolları və interfeysləri.

Ciphony
Sifon – informasiyanın düşmən və ya rəqib tərəfindən ələ keçirilməsinin qarşısını almaq üçün telekommunikasiya siqnallarının şifrlənməsi prosesi.

Ciphertext
Şifrlənmiş mətn – kriptoqrafik vasitələrdə şifrləmə nəticəsində alınan verilənlər.

Ciphertext-only attack
Yalnız şifrlənmiş mətnlə hücum – kriptoanalitikin əlində yalnız şifrlənmiş mətnin olduğu analitik hücum.

Classified information
Məxfi informasiya – Hökumət sərəncamı 13292-yə və ya onun istənilən əvvəlki sələfinə müvafiq olması müəyyən edilən

informasiya, icazəsiz açıqlanmaya qarşı mühafizə tələb edir və sənəd formasında olduqda onun məxfi statusunu göstərmək üçün nişanlanır.

Clearance
Şəffaflıq səviyyəsi − verilən subyektə Bell-LaPadula modelinin qaydaları ilə girişə icazə verilən təhlükəsizliyin maksimal səviyyəsi. Subyektin cari səviyyəsi (baxılan anda onun əməliyyatları yerinə yetirdiyi səviyyə) minimaldan şəffaflıq səviyyəsinə qədər dəyişə bilər.

Clearing
Təmizləmə – təsnif edilmiş verilənlərin ayrıca təhlükəsizlik təsnifatı və təhlükəsizlik kateqoriyası olan verilənlər daşıyıcısına yenidən yazılmalıdır ki, nəticədə həmin verilənlər daşıyıcısı eyni təhlükəsizlik təsnifatında və təhlükəsizlik kateqoriyasında yazı üçün yenidən istifadə edilə bilsin.

Click fraud
Klik dələduzluğu – klik sayına görə ödəniş edilən onlayn reklamda baş verən dələduzluqdur, şəxs, skript və ya kompüter proqramı brauzerin qanuni istifadəçisini imitasiya edərək klik sayına görə ödəniş məqsədi ilə reklama klik edir.

Clickjacking attacks (User Interface redress attack)
Klik qaçırma hücumları (İstifadəçi interfeysinin əvvəlki vəziyyətə qaytarılması hücumu) – istifadəçilərin fərqində olmadan istədiklərinin əvəzinə başqa bir linkə klikləməsi üçün veb-istifadəçilərinin aldadılması üsuludur. İstifadəçi zərərsiz görünən veb-səhifələri kliklədikdə bədniyyətlinin konfidensial informasiya götürməsinə və ya istifadəçinin kompüterinə nəzarəti ələ keçirməsinə səbəb olur.

Clipper – Skipjack şifrləmə alqoritmini realizə edən mikrosxem. Capstone layihəsinin tərkib hissəsidir. Clipper-in yaradılması 1993-cü ilin aprelində rəsmən elan olunmuşdu.

Clonebot, Clonies, or Bot
Klonbot, Klonlar və ya Bot – özünü şəbəkədə kritik həcmdə replikasiya etmək üçün nəzərdə tutulur. Klonbot şəbəkədə bir neçə agent kimi meydana çıxır və sonra şəbəkədə digər istifadəçiyə qarşı daşqın [**flooding]** eksploytunu yerinə yetirir.

Closed-security environment
Qapalı təhlükəsizlik mühiti – verilənləri və resursları təsadüfi və ya bədniyyətli əməllərdən qorumaq üçün (səlahiyyət vermək formalarında, təhlükəsizlik hüquqlarında, konfiqurasiya idarə elementlərində) xüsusi diqqət verilən mühit.

Clone phishing
Klon fişinqi – fişinq yayanlar həqiqi mənbələrdən göndərilən məktublara tam oxşayan elektron məktub yaradırlar.

Code
Kod: 1. Açıq mətn elementlərinin (hərflər, hərf birləşmələri, sözlər və s.) qrup şəklində simvola çevrilmələri çoxluğu. Şifrin xüsusi növüdür.
2. Məlumat itkisi olmadan bir əlifbada olan məlumatın digər əlifbadakı məlumata çevrilməsi qaydası.

Code Red I and II Worm
I və II Qırmızı kod soxulcanları – 16 iyul 2001-ci ildə Windows IIS Serverindəki boşluqlardan istifadə edərək I Qırmızı Kod və sonra II Qırmızı Kod soxulcanları saatlar ərzində çoxalaraq və İnternetdəki hər bir müdafiəsiz kompüteri yoluxduraraq İnternetdə sürətlə yayılmışdı.

Coding
Kodlaşdırma – ilkin əlifbadakı məlumatın digər əlifbadakı məlumata çevrilməsi.

Cold site
Soyuq sayt – verilənlərin ehtiyat emalı sisteminin quraşdırılmasını və fəaliyyətini təmin etmək üçün nəzərdə tutulan zəruri avadanlığı olan vasitə.

Collision
Kolliziya – müxtəlif məlumatların heş-qiymətlərinin üst-üstə düşməsi hadisəsi.

Common Attack Pattern Enumeration and Classification (CAPEC)
Hücum şablonlarının ümumi siyahısı və təsnifatı – hücum şablonlarının, hücum sxemlərinin və hücum siniflərinin açıq kataloqu. MITRE korporasiyası tərəfindən ABŞ Milli Təhlükəsizlik Nazirliyi (Department of Homeland Security, DHS) üçün işlənmişdir.

Common Platform Enumeration (CPE)
Platformaların ümumi siyahısı – təşkilatın hesablama texnikası vasitələrində təmsil olunmuş əməliyyat sistemlərinin, tətbiqi proqramların və aparat qurğularının siniflərinin identifikasiyası və təsviri üçün strukturlaşdırılmış metod. CPE bu vasitələr barəsində məsələn, informasiya təhlükəsizliyi siyasətinin yerinə yetirilməsini yoxlamaq məqsədilə informasiya mənbəyi kimi istifadə edilə bilər.

Common Vulnerabilities and Exposures (CVE)
Boşluqların ümumi tezaurusu – bütün məlum informasiya təhlükəsizliyi boşluqları üçün vahid tezaurus təqdim edir və boşluqların adlandırılmasının vahid qaydalarını müəyyən edir.

Common Weakness Enumeration (CWE)
Boşluqların ümumi siyahısı – proqram təminatı məhsullarının məlum boşluqlarının siyahısı.

Communications security
Kommunikasiya təhlükəsizliyi – verilənlərin ötürülməsinə tətbiq edilən kompüter təhlükəsizliyi

COMP 128
Girişi 256 bit və çıxışı 128 bit olan heş-funksiya. GSM standartlı mobil rabitə şəbəkələrində A3/A8-in realizəsi üçün istifadə edilir. Tam sındırılmışdır, müəyyən girişlər üçün generasiya edilən heş-qiymətlərdən girişin bir hissəsini bərpa etmək mümkündür.

Compartmentalization
Parselləmə – riski azaltmaq məqsədilə ayrı-ayrı təhlükəsizlik elementləri ilə verilənlərin təcrid olunmuş bloklara bölünməsi.

Compromise
Nüfuzdansalma – informasiya təhlükəsizliyinin proqramların və ya verilənlərin modifikasiyası, məhv edilməsi və ya səlahiyyətsiz subyektlər tərəfindən istifadəsinin mümkün edilməsi yolu ilə pozulması.

Compromising emanation
Nüfuzdansalma emanasiyası – qeyri-ixtiyari olaraq buraxılan və ələ keçirilib analiz edilərsə, emal edilən və ya ötürülən mühüm informasiyanı aşkarlaya bilən siqnallar.

Computer crime
Kompüter cinayətkarlığı – verilənlərin emalı sisteminin və ya kompüter şəbəkəsinin köməyilə və ya onların birbaşa cəlb edilməsi ilə törədilən cinayət.

Computer Emergency Response Team/Coordinating Center (CERT/CC)
Kompüter Təhlükəsizliyi İnsidentlərini Operativ Cavablandırma Qrupu/Əlaqələndirmə Mərkəzi – Karnegi-Mellon Universitetinin Proqram Mühəndisliyi İnstitutunda (PMİ) 1988-ci ildə yaradılmışdı.

CERT/CC PMİ-də işlənən Networked Systems Survivability (NSS) proqramının bir hissəsidir. Bu proqramın əsas məqsədi müvafiq texnologiyaların və sistemin idarə edilməsi metodlarının qurulmasını elə şəkildə təmin etməkdir ki, hücumların maksimal səmərəli qarşısı alınsın, ziyan minimumlaşdırılsın və hətta hücumların həyata keçirilməsi uğurlu halında da sistemin fasiləsiz işi təmin edilsin.
CERT/CC əlaqələndirmə mərkəzinin vəzifələri aşağıdakı məsələlərin həll edilməsidir:
CERT/CC laboratoriyalarında (tədqiqat) proqram və aparat təminatının aşkarlanmış boşluqları haqqında istifadəçiləri məlumatlandırmaq üçün veb-serverdə (http://www.cert.org), ftp-serverdə (ftp://ftp.cert.org/pub/cert_advisories), Usenet telekonfransında (comp.security.announce) və göndəriş siyahılarında boşluqların təsviri və onların aradan qaldırılması üsulları – Advisories nəşr olunur. Təhlükəsizlik problemləri və onların həlli haqqında istehsalçı firmalardan alınmış məlumatlar xüsusi informasiya bülletenlərində (Vendor-Initiated Bulletins) nəşr olunur, onlar da Advisories kimi həmin kanallarla yayılır.

Computer forensics
Kompüter kriminalistikası – təhqiqat məqsədləri üçün verilənlərin tamlığını saxlamaqla kompüterlə əlaqədar verilənlərin toplanması, saxlanması və analizi praktikası.

Computer fraud
Kompüter dələduzluğu – verilənlərin emalı sisteminin və ya kompüter şəbəkəsinin köməyilə və ya onların birbaşa cəlb edilməsi ilə edilən dələduzluq.

Computer Incident Advicory Capability (CIAC)
Kompüter İnsidentləri üzrə Məsləhət Mərkəzi – ABŞ Energetika Nazirliyi yanında 1989-cu ildə yaradılmışdı və Lawrence Livermore Milli Laboratoriyasında yerləşir. Mərkəzin əsas məqsədi Energetika

Nazirliyi əməkdaşlarının və podratçılarının kompüter təhlükəsizliyinin təmin edilməsidir. FIRST-in təşkilatçılarından biridir.
Internet istifadəçilərinin boşluqlar haqqında dövri məlumatlandırılması üçün CIAC mərkəzi də CERT/CC-yə analoji olaraq öz veb serverində (http://llnl.ciac.gov) və göndəriş siyahılarında informasiya bülletenləri (Advisories) nəşr edir.

Computer security
Kompüter təhlükəsizliyi – verilənlərin və resursların adətən müvafiq tədbirlərin görülməsi yolu ilə təsadüfi və ya bədniyyətli əməllərdən qorunması.

Computer security incident
Kompüter təhlükəsizliyi insidenti – kompüter təhlükəsizliyi siyasətlərinin, yolverilən istifadə siyasətlərinin və ya standart kompüter təhlükəsizliyi qaydalarının pozulması və ya labüd pozulma təhdidi.

Computer Security Incident Response Team (CSIRT)
Kompüter təhlükəsizliyi insidentinə cavab komandası – kompüter təhlükəsizlik ilə əlaqədar insidentlərə cavab verməkdə kömək məqsədilə qurulur; Kompüter insidentinə cavab komandası (Computer Incident Response Team, CIRT) və ya kompüter insidentinə cavab mərkəzi (CIRC Computer Incident Response Center, Computer Incident Response Capability, CIRC) də adlanır.

Computer-system audit
Kompüter sisteminin auditi – verilənlərin emalı sistemində istifadə edilən prosedurların onların effektivliyini və düzgünlüyünü dəyərləndirmək və təkmilləşdirmələr tövsiyə etmək üçün yoxlanılması.

Confidentiality
Konfidensiallıq − kritik informasiyanın gizli saxlanması, ona giriş istifadəçilərin (ayrıca şəxslərin və ya təşkilatların) qapalı dairəsi ilə məhdudlanır.

Contamination
Kontaminasiya – bir təhlükəsizlik təsnifatının və ya təhlükəsizlik kateqoriyasının verilənlərinin daha aşağı təhlükəsizlik təsnifatının və ya müxtəlif təhlükəsizlik kateqoriyasının verilənlərinə daxil edilməsi.

Contingency plan (backup plan, recovery plan)
Fasiləsiz işin təmini planı (fəaliyyətin bərpası planı) − təhlükəli şəraitə reaksiya, ehtiyat surətçıxarma və sonrakı bərpaetmə prosedurlarının planı, mühafizə proqramının bir hissəsidir, sistemin əsas resurslarının əlyetərliyini təmin edir və böhran hallarında fəaliyyətin fasiləsizliyini təmin edir.

Contingency procedure
Gözlənilməz vəziyyət proseduru – qeyri-adi, lakin gözlənilən situasiya baş verdikdə prosesin normal gedişinə alternativ prosedur.

Controlled access system
Nəzarət edilən giriş sistemi – fiziki girişə nəzarətin avtomatlaşdırılması vasitəsi.

Cookie
Kuki – müvəqqəti saxlamaq və istənilən sonrakı müraciətlərdə və ya sorğularda serverə qaytarmaq üçün veb-server tərəfindən veb-resursla birlikdə brauzerə göndərilən informasiya bloku.

Copy protection
Surətçıxarmadan qorunma – səlahiyyət olmadan verilənlərin, proqram təminatının və ya sistem proqramlarının surətinin

çıxarılmasını aşkarlamaq və ya əngəlləmək üçün xüsusi üsullardan istifadə edilməsi.

Countermeasure
Əks-tədbir – boşluğu minimuma endirmək üçün nəzərdə tutulan əməliyyat, vasitə, prosedur, texnologiya və ya başqa tədbir.
Covert channel
Gizli kanal − informasiyanın ötürülməsi yolu, qarşılıqlı təsirdə olan iki prosesə informasiyanı elə üsulla mübadilə etməyə imkan verir ki, sistemin təhlükəsizlik siyasətini pozsun.

Covert storage channel
Gizli yaddaş kanalı − informasiyanın yaddaş sahəsinə birbaşa və ya dolayısı ilə bir proses tərəfindən yazılmasını və bu informasiyanın başqa proses tərəfindən oxunmasını təmin edən gizli kanal. Yaddaşa malik gizli kanal adətən müxtəlif təhlükəsizlik səviyyəsinə malik iki subyektə ortaq olan məhdud həcmli resursların (məsələn, diskdə sektorların) istifadəsi ilə əlaqədardır.

Covert timing channel
Gizli zaman kanalı – informasiya sistemin davranışının müəyyən aspekti (məsələn, mərkəzi prosessorun məşğulluq zamanı) müəyyən müddət modulyasiya edilməklə elə tərzdə ötürülürr ki, bu informasiyanı alan proqram sistemin davranışını müşahidə edə və qorunan informasiyanı məntiqi çıxarışla əldə edə bilər.

Cold start
Soyuq start – kompüterə əsaslanan informasiya sistemlərində potensial problemdir, verilənlərin avtomatlaşdırılmış modelləşdirilməsi müəyyən dərəcədə daxildir.

Common Configuration Scoring System (CCSS)
Konfiqurasiyanı ümumi qiymətləndirmə sistemi – proqram təminatında təhlükəsizliyin konfiqurasiyası məsələlərinin ciddiliyini ölçmək üçün vasitələr çoxluğu.

Common Misuse Scoring System (CMSS)
Sui-istifadəni ümumi qiymətləndirmə sistemi – proqram təminatı xüsusiyyətlərindən sui-istifadə boşluqlarının ciddiliyini ölçmək üçün vasitələr çoxluğu.

Computer forensics
Kompüter məhkəmə ekspertizası – kompüterlərdə və rəqəmsal yaddaş qurğularında tapılan hüquqi sübutlar ilə əlaqəli rəqəmsal ekspertiza elminin bir qolu.

Cracker
Kreker – başqasının kompüter sistemini sındıran, kompüter programlarında parollardan və lisenziyalardan yan keçən və ya başqa yollarla kompüter təhlükəsizliyini qəsdən pozan şəxs.

CRAMM (CCTA Risk Analysis and Managment Method)
Riskin analizi və idarə edilməsi metodu CRAMM – 1985-ci ildə Böyük Britaniya Mərkəzi Kompüter və Telekommunikasiya Agentliyi (Central Computer and Telecommunications Agency, CCTA) tərəfindən işlənmişdi. CRAMM proqram təminatı müxtəlif növ təşkilatlar üçün nəzərdə tutulmuşdur, onlar öz biliklər bazası – profillərlə fərqlənirlər.

Credentials
İdentifikasiya verilənləri, səlahiyyətlər – obyektin elan edilmiş kimliyini müəyyənləşdirmək üçün ötürülən verilənlər.

Critical Infrastructures
Kritik infrastrukturlar − 2001-ci ildə ABŞ-da qəbul edilmiş Vətənpərvərlik Qanununda "kritik infrastruktur" anlayışı aşağıdakı kritik infrastruktur sektorlarını və resurslarını əhatə edir: kimya sənayesi; fövqəladə xidmətlər; informasiya texnologiyaları; poçt; telekommunikasiya; nəqliyyat sistemləri (avtobus, təyyarə, gəmi, avtomobil sistemləri, dəmiryolu sistemləri və boru kəməri sistemləri daxil olmaqla).

Cross-certificate
Çarpaz sertifikat – iki sertifikat xidməti mərkəzi arasında etimad əlaqəsi qurmaq üçün istifadə edilən sertifikat.

Cryptanalysis
Kriptoanaliz – açıq mətn kimi mühüm məlumatı əldə etmək üçün kriptoqrafik sistemin, onun giriş və çıxış məlumatlarının, yaxud hər ikisinin analizi.

Cryptographic hash function
Kriptoqrafik heş funksiya − ixtiyari uzunluqda məlumatı sabit uzunluqda heş-koda çevirən kriptoqrafik çevirmə. Kriptoqrafik heş funksiyaların iki mühüm növü var.

1. *Açarlı heş funksiyalar* – məlumatın autentifikasiya kodları (Message Authentication Code, MAC) adlanır. Məlumatın autentifikasiya kodları simmetrik açarlı sistemlərdə tətbiq edilir və onlar əlavə vastələr cəlb etmədən, istifadəçiləri bir-birinə etibar edən sistemlərdə həm verilənlərin mənbəyinin həqiqiliyinə, həm də verilənlərin tamlığına zəmanət verməyə imkan verir.
2. *Açarız heş funksiyalar* – səhvlərin aşkarlanması kodları (Modification Detection Code və ya Manipulation detection Code, MDC) adlandırırlar. Onlar əlavə vastələrlə (məsələn, şifrləmə, mühafizəli kanaldan istifadə və ya rəqəmsal imza) verilənlərin tamlığına zəmanət verməyə imkan verir. Bu heş funksiyalardan həm istifadəçiləri bir-birinə etibar edən sistemlərdə, həm də istifadəçiləri bir-birinə etibar etməyən sistemlərdə istifadə etmək olar.

Cryptographic key
Kriptoqrafik açar − şifrləmə, deşifrləmə, rəqəmsal imza yaratmaq və imzanı yoxlamaq kimi kriptoqrafik əməliyyatların idarə edilməsi üçün istifadə edilən parametr.

Cryptographic system
Kriptoqrafik sistem – şifrləmə və deşifrləmə vasitəsini təmin etmək üçün birgə istifadə edilən sənədlər, qurğular, avadanlıq və əlaqədar texniki vasitələr.

Cryptography
Kriptoqrafiya − informasiyanın anlaşılmaz şəklə çevrilməsinin, həmçinin informasiyanın qavrayış üçün yararlı şəklə bərpa edilməsinin prinsipləri, vasitələri və metodları. "Kriptoqrafiya" sözü *kryptos* ("gizli") və *graphos* ("yazı") yunan sözlərindən yaranmışdır. Şifrləmə proseduru adətən müəyyən kriptoqrafik alqoritmdən və açardan istifadəni nəzərdə tutur.

CSI/FBI Survey
Kompüter cinayətləri və təhlükəsizlik üzrə icmal – Kompüter Təhlükəsizliyi İnstitutu (Computer Security Institute, CSI) və Federal Təhqiqat Bürosu (FTB) tərəfindən nəşr olunur. Kompüter Təhlükəsizliyi İnstitutu FTB-nin San-Fransiskodakı Kompüter müdaxilələri bölməsi (ing. Computer Intrusion Squad) ilə birlikdə on illər ərzində tədqiqatlar aparır və hər il "Kompüter cinayətləri və təhlükəsizlik" icmalları buraxır; məqsəd biznes, təhsil, səhiyyə müəssisələrində və dövlət orqanlarında məlumatlandırma səviyyəsini yüksəltməkdir. İcmalın əsas hədəfi ABŞ-da illik kompüter cinayətlərinin növlərini və miqyasını aydınlaşdırmaq və kibercinayətkarlıq meyllərini əvvəlki illərlə müqayisə etməkdir.

Cross-site scripting (XSS)
Saytlararası skript – veb sistemlərinə hücum növlərindən biri. Veb-səhifəyə zərərli kodun yerləşdirilməsinə və bu kodun bədniyyətlinin veb-serveri ilə qarşılıqlı əlaqəsindən ibarətdir (zərərli kod veb-səhifəni açan istifadəçinin kompüterində yerinə yetirilir). Zərərli kodu veb-serverdə olan boşluqdan və ya istifadəçinin kompüterindəki boşluqdan istifadə etməklə veb-səhifəyə yerləşdirmək olar.

XSS hücumlarının dəqiq təsnifatı yoxdur, lakin ekspertlərin çoxu XSS-in ən azı iki növünü fərqləndirirlər*: "əks olunmuş XSS*" ("*reflected XSS*") və "*saxlanılan XSS*" ("*stored XSS*").
Termin üçün "XSS" qısaltması kaskad stil cədvəlləri üçün istifadə edilən "CSS" (Cascading Style Sheets) qısaltması ilə səhv salmamaq üçün istifadə edilir.

Crypto(graphic) ignition key (CIK)
Kripto(qrafik) kontakt açarı – kriptoqrafik açarları və aktivləşdirmə verilənlərini saxlamaq, ötürmək və qorumaq üçün isitfadə olunan fiziki token (daşıyıcı).

Cryptographic randomization
Kriptoqrafik randomizasiya – kriptoqrafik sxemin ötürmə vəziyyətini təsadüfi şəkildə müəyyən edən funksiya.

CTF (Capture The Flag)
"***Bayrağı ələ keçir***" – informasiya təhlükəsizliyi üzrə komanda yarışlarıdır. Bu yarışların məqsədi informasiya təhlükəsizliyi üzrə mütəxəssislərin real şəraitə yaxın şərtlərdə təlimi və təcrübə qazanmasıdır. CTF öyrədici xarakter daşıyır, iştirakçılara kompüter sistemlərinin müdafiəsi və hücum sahəsində praktiki təcrübə qazanmağa imkan verir. Bir qayda olaraq, yarışlarda proqramın maşın kodunun analizi (*reverse engineering*) biliklərini tətbiq etmək, şəbəkələri və protokolları analiz etmək, şəbəkələri idarə etmək, proqramlaşdırmaq, kriptoanaliz etmək bacarıqları tələb olunur.
İnformasiya təhlükəsizliyi üzrə CTF tipli yarışlar – DEF CON CTF ilk dəfə DEFCON haker konfransında keçirilib (1996-cı il, 4-cü DEFCON). Ali məktəblər arasında beynəlxalq distant UCSB iCTF yarışları ilk dəfə 2004-cü ildə Santa-Barbaradakı Kaliforniya Universiteti (University of California at Santa Barbara, UCSB) tərəfindən keçirilib. Rusiyada CTF yarışları 2008-ci ildə Ural Dövlət Universiteti, HackerDom komandası (http://hackerdom.ru) tərəfindən təşkil edilib. 2009-cu ildən tələblər arasında beynəlxalq distant RuCTF yarışları da keçirilir.

CyberAngels
Kiber Mələklər – ən yaşlı və ən böyük onlayn təhlükəsizlik təşkilatı. Haker cəmiyyətinin cinayətlərə qarşı mübarizə aparan qoludur, 1995-ci ildən onlayn fəaliyyət göstərir.

Cyber Apocalypse
Kiber Qiyamət – kritik informasiya infrastrukturlarını çökdürməklə dövlətdə xaos yarada bilən kiber hücum. Hazırda əsasən kritik infrastrukturu – magistral telekommunikasiya xətlərini, elektrik xətlərini, neft və qaz kəmərlərini və s. idarə edən kompüter sistemlərində proqram təminatının təhlükəsizliyi məsələlərini əhatə edir.

Cyber attack
Kiber-hücum – kiber-insident yaratmaq üçün informasiya sistemlərinə qarşı kiber-silahın və ya kiber-silah kimi istifadə edilə bilən sistemin qəsdən istifadəsidir.

Cyber conflict
Kibermünaqişə – siyasi məqsədlərə nail olmaq üçün kiberhücumların istifadəsi (hədəf sistemlərin tamlığına və əlyetərliyinə qarşı yönəlmiş hücumlar daxil olmalıdır).

Cyber crook
Kiberdələduz **(çəngəl)** – kompüter sisteminə qeyri-qanuni giriş əldə edən və ya maliyyə transferlərini öz şəxsi hesabına yönləndirən şəxs.

Cyber incident
Kiber-insident – informasiya sisteminin (və ya informasiya, aparat və proqram təminatı daxil olmaqla onun komponentlərinin) strukturunda və əməliyyatlarında yol verilməyən kənaraçıxmalara səbəb olan və ya səbəb ola biləcək hadisələrdir. Kiber-insidentlər qəsdən və ya təsadüfən törədilə bilər.

Cyber espionage
Kiber-casusluq – hədəf sistemin konfidensiallığını pozmaq üçün kiber-hücumun istifadəsi.

Cyber hoodlums
Kiber-xuliqanlar – hesabların sındırılması, kimliyin saxtalaşdırılması üçün parollardan istifadə edən və ya həmin parolları qara bazarda pul qarşılığında digər cinayətkarlara satanlar.

Cyber Observable eXpression (CybOX)
Kiberdomendə müşahidələrin təsviri – kiberdomendə müşahidə edilə bilən hadisələr və vəziyyət xarakteristikaları haqqında informasiyanın kodlaşdırılması, toplanması və ötürülməsi üçün standartlaşdırılmış dil. MITRE korporasiyası tərəfindən işlənmişdir.

Cyber weapon
Kiber-silah – informasiya texnologiyalarına əsaslanan digər sistemlərin strukturuna və əməliyyatlarına ziyan vurmaq üçün yaradılmış, informasiya texnologiyalarına əsaslanan sistem (aparat təminatı, proqram təminatı və kommunikasiya mühitindən ibarət olur).

Cyclical Redundancy Check (CRC)
Tsiklik izafi kod − məlumatın kommunikasiya kanalı ilə göndərilməsi zamanı tamlığına nəzarət etmək üçün metoddur. Bax. *Checksum.*

Cybercrime
Kibercinayət – kompüterlərlə və ya onların vasitəsilə edilən cinayətlərdir. Kibercinayətlərə kompüter verilənləri və sistemlərinin konfidensiallığı, tamlığı və əlyetərliyinə qarşı cinayətlər; kompüter texnologiyalarından istifadə etməklə saxtalaşdırma və dələduzluq, məlumatların məzmunu ilə (uşaq pornoqrafiyası ilə) bağlı cinayətlər; müəllif hüquqlarının və əlaqəli hüquqların pozulması ilə bağlı cinayətlər daxildir.

Cyberbullying
Kiberzorakılıq – başqa insanlara düşünülmüş şəkildə dəfələrlə zərər vurmaq və ya təqib etmək üçün informasiya texnologiyalarından istifadə edilməsi.

Cyberpunk
Kiberpank – hərfən "*cyber*" və "*punk*" sözlərinin birləşməsindən əmələ gəlmişdir, ilk dəfə Bruce Bethke-nin "Cyberpunk" adlı qısa hekayəsinin adında meydana çıxmışdı. Hekayə 1983-ci ildə "Amazing" fantastik hekayələr jurnalında nəşr edilmişdi. Bu qısa hekayə etik qüsurları olan bir qrup yeniyetmə kreker haqqında yüksək texnologiyalar sahəsində elmi-fantastik hekayə idi. Bethke bildirir ki, bu sözü "pank münasibətləri" və "yüksək texnologiya" anlayışlarını birləşdirən söz axtararkən tapmışdı.

Cyberocracy
Kiberokratiya – informasiyanın effektiv istifadəsi ilə idarə edilən hökumət və ya hökumət elementinin formasını təsvir edir.

Cyberstalking
Kiber-təqib – fərdi, qrupu və ya təşkilatı izləmək və narahat etmək üçün İnternet və ya başqa elektron vasitələrdən istifadə edilməsi.

Cyberwar
Kibermüharibə – ölkələr arasında kibermünaqişə; fiziki vasitələrlə deyil, daha çox elektron vasitələrlə kompüter və İnternetdə baş verən müharibə formasıdır.

D

Daemons
Demonlar – başqa kompüter proqramları üçün bəzi xidmətləri yerinə yetirən fon prosesi kimi işləyən kompüter proqramı. Tipik demonlar e-poçt, FTP, çap, telnet və veb xidmətlərini təmin edir. Bu termin əsasən UNİX və Linux sistemlərində istifadə edilir. Windows sistemlərində demonları "servislər" adlandırırlar.

Daisy chain
Zəncirvari şəbəkə – kompüter qurğularının, periferiya qurğularının və ya şəbəkə qovşaqlarının bir-birinin ardınca qarşılıqlı qoşulmasıdır.

Data authentication
Verilənlərin autentifikasiyası – verilənlərin tamlığını yoxlamaq üçün istifadə edilən proses.

Data corruption
Verilənlərin korlanması – verilənlərin tamlığının təsadüfi və ya bilərəkdən pozulması.

Data custodian
Verilənlərin qoruyucusu – təşkilatın təhlükəsizlik siyasəti və yaxud standart İT təcrübələri ilə müəyyən olunmuş məlumatların qorunduğu halda, təşkilatın sənədlərinə və ya elektron fayllarına çıxış verən məsuliyyətli şəxs və yaxud inzibati nəzarətə malik şəxs.

Data diddling
Verilənlərin təhrifi – kompüter sisteminə girişdən əvvəl və ya giriş zamanı verilənlərin şifrlənməsi.

Data Encryption Standard (DES)
Verilənləri şifrləmə standartı – ABŞ hökuməti tərəfindən 1977-ci ildə qəbul edilmiş simmetrik şifrləmə standartı; kommersiya və

mülki hökumət təşkilatları tərəfindən istifadə üçün nəzərdə tutulmuşdu. 2000-ci ildə AES standartı ilə əvəzlənmişdir.

Data exfiltration
Verilənlərin eks-filtrasiyası – verilənlərin kompüter və serverdə icazəsiz axtarılması, kopyalanması və ya ötürülməsidir. Kibercinayətkarlar tərəfindən Internet və ya digər şəbəkə üzərindən müxtəlif üsullarla yerinə yetirilən bədniyyətli fəaliyyətdir. Verilənlərin eks-filtrasiyası üçün ingilis dilində "data extrusion", "data exportation" or "data theft" terminləri də işlədilir.

Data Integrity
Verilənlərin tamlığı − verilənlərin əvvəlcədən müəyyən edilmiş şəkil və keyfiyyətini saxlaması xassəsi.

Data protection
Verilənlərin qorunması – verilənlərə icazəsiz girişlərin qarşısını almaq üçün inzibati, texniki və ya fiziki tədbirlərin gerçəkləşdirilməsi.

Data reconstitution
Verilənlərin bərpası – alternativ mənbələrin istifadəsi mümkün olan komponentlərindən verilənlərin toplanması yolu ilə verilənlərin bərpası.

Data restoration
Verilənlərin bərpası – itirilmiş və ya yoluxmuş verilənlərin yenidən yaradılması.

Data security
Verilənlərin təhlükəsizliy − verilənlərin icazəsiz (təsadüfi və ya bilərəkdən) modifikasiyalardan, məhv edilmək və açıqlanmaqdan mühafizəsi.

Data validation
Verilənlərin doğrulanması – verilənlərin doğru və tam olduğunun və ya göstərilən meyarlara cavab verdiyinin müəyyənləşdirilməsi prosesi.

DDoS (Distributed Denial of Service) attack
Xidmətdən paylanmış imtina hücumu – çox sayda kompüterdən eyni anda həyata keçirilən *xidmətdən imtina* (*DoS*) *hücumu*.

Deep Packet Inspection (**DPI**, **complete packet inspection** və ya **Information eXtraction** (**IX**) də adlanır)
Dərin Paket Təftişi (**paketin tam təftişi** və **informasiyanın çıxarılması** da adlanır) – şəbəkə paketlərinin süzülməsinin bir formasıdır; təftiş nöqtəsinə keçdikdə paketin məlumat hissəsini (və ehtimal ki, onun başlığını) paketin keçib-keçməyəcəyinə və yaxud başqa məntəqəyə yönləndirilməli olduğuna qərar vermək, yaxud statistik məlumatlar toplamaq üçün protokollara uyğunsuzluq, viruslar, spam, müdaxilələr və yaxud müəyyən olunmuş kriteriyalar yoxlanır.

Deep Web (**Deepnet**, **Invisible Web** və ya **Hidden Web** də adlanır)
Dərin veb – World Wide Web-in standart axtarış maşınları tərəfindən indekslənən hissəsinə (ing. Surface Web) daxil olmayan kontentidir.

Defense-in-breadth
Eninə müdafiə – sistem, şəbəkə və ya altkomponentin həyat dövrünün hər bir mərhələsində (sistemin, şəbəkənin və yaxud məhsulun dizaynı və hazırlanması; istehsalı; qablaşdırılması; yığılması; sistemlərin inteqrasiyası; distribusiya; əməliyyatlar; texniki dəstək və demontaj edilməsi) boşluqların müəyyən edilməsinə, idarə edilməsinə və mövcud risklərin azaldılmasına xidmət edən planlaşdırılmış, sistemli, multi-disiplinar fəaliyyətlər toplusudur.

Defence in depth (**deep** və ya **elastic defence** kimi də işlədilir)
Dərin müdafiə (**dərin** və **yaxud elastik müdafiə** kimi də işlədilir) – hücumun yayılmasının qarşısını almaqdansa, daha çox onu gecikdirməyə, məsafə buraxmaqla vaxt qazanmağa çalışan və əlavə itkilərə səbəb olan hərbi strategiyadır.

DMZ (Demilitarized zone)
Demilitarizasiya zonası − hərbçilərdən alınmış termindir, döyüş əməliyyatlarının hazırlanması və aparılması qadağan edilmiş əraziləri bildirmək üçün istifadə edilir. İnformasiya texnologiyaları sahəsində DMZ termini əsasən şəbəkə ekranının xarici seqmenti ilə xarici marşrutizatorun daxili interfeysi arasında qalan şəbəkə seqmentini bildirir. DMZ-nin təyinatı müxtəlif servislər təqdim etmək imkanı saxlamaqla, konfidensial informasiya olan daxili şəbəkəni bütün digər şəbəkələrdən təcrid etməkdir. DMZ zonada, bir qayda olaraq, İnternetdən müraciət olunan informasiya resursları yerləşdirilir.

Denial of service
Xidmətin imtinası − sistemin öz funksiyalarını yerinə yetirməyi dayandırmağına səbəb olan istənilən hissəsinin sıradan çıxmasına gətirən istənilən hərəkət və ya hərəkətlər ardıcıllığı. Səbəb icazəsiz giriş, xidmətdə gecikmə və s. ola bilər.

Deutsches Advisory Format (DAF)
Təhlükəsizlik bülleteni formatı – CSIRT-lər tərəfindən təhlükəsizlik bülletenlərinin yaradılması və müxtəlif komandalar arasında mübadiləsi üçün standart. CERT-Verbund tərəfindən təklif edilib (Almaniya).

Dialer
Nömrə yığan – telefon nömrələrinəavtomatik zəng etmək üçün nəzərdə tutulmuş proqram.Avtomatlaşdırılmış nömrə yığanlar adları və telefon nömrələrini yadda saxlayırlar,insanlara telefon nömrələrini əzbərləmədənasan əlaqə qurmağa imkan yaradırlar.

Differensial cryptanalysis
Diferensial kriptoanaliz – iterariv blok şifrləri üçün tətbiq edilə bilən kriptoanaliz metodudur. İlk dəfə 1990-cı ildə Merfi tərəfindən FEAL-4 şifrinə hücum üçün istifadə edilmişdir. 1991-ci ildə E.Biham və A.Şamir tərəfindən DES şifrinə hücum üçün təkmilləşdirilmişdir. Diferensial kriptoanaliz seçilmiş açıq mətnlə kriptoanaliz metoduna əsaslanır və eyni açarla şifrlənmiş iki açıq mətn arasındakı fərqi analiz edir. Mümkün açarlardan hər birinə onun "düzgünlüyü" ehtimalı təyin edilir və nəticədə istifadə edilən açar hesablanır.

Differential Power Analysis (DPA)
Enerjinin diferensial analizi − kriptoqrafik alqoritmlərdə istifadə edilən kriptoqrafik açarlarla hər hansı bir əlaqəsi olan informasiyanın çıxarılması üçün qabaqcıl statistik metodlardan və ya başqa üsullardan istifadə etməklə kriptoqrafik modulun elektrik enerjisi istehlakının dəyişmələrinin analizi.

Diffie-Hellman (DH) algorithm
Diffi-Helman alqoritmi **–** 1976–cı ildə "Kriptoqrafiyada yeni istiqamətlər" adlı məqalədə nəşr edilib. Kriptoqrafik açarların mühafizə olunmayan rabitə kanalları ilə göndərilməsi üçün istifadə edilir. Diffi-Helman sxeminin nöqsanı – istifadəçilərin açıq açarlarının autentifikasiya edilməməsidir, yəni açarların həqiqi istifadəçilər tərəfindən yaradılmasının yoxlanmamasıdır.

Digital envelope
Rəqəmsal zərf – məlumata əlavə olunan və məlumatı alan şəxsə məlumatın kontentinin tamlığını yoxlamağa imkan verən verilənlər.

Digital signature
Rəqəmsal imza – sənədə əlavə olunan və sənədi alan şəxsə sənədi imzalayanın həqiqiliyini və imzalandıqdan sonra sənəddə dəyişikliyin edilmədiyini yoxlamağa imkan verən verilənlər.

Disaster Recovery Plan (DRP)
Qəzadan sonra bərpa planı − ciddi aparat və ya proqram təminatı vasitələrində səhvlər və ya bu vasitələrin sıradan çıxması (məhvi) halında kritik tətbiqi proqramların emalı üçün yazılmış plan.

Disclosure
Açıqlama – verilənlərin səlahiyyətsiz obyektlər tərəfindən istifadəsi mümkün edilməsi yolu ilə kompüter təhlükəsizliyinin pozulması.

Discretionary access control (DAC)
Girişin diskresion idarə edilməsi − sistemin subyektlərinin obyektlərinə girişini istifadəçinin, prosesin və/və ya onun mənsub olduğu qrupun identifikasiyasına və tanınmasına əsaslanan idarəetmə metodu.

DNS Amplification
DNS gücləndirmə − bədniyyətli boşluq olan DNS-serverə sorğu göndərir (adətən qısa), server isə sorğuya uzunluğu xeyli böyük olan paketlə cavab verir. Əgər ilkin IP-ünvan kimi hədəf kompüterin ünvanı göstərilsə (IP-spoofing), DNS-server hədəf-kompüterə onun işini tamamilə iflic edənədək böyük miqdarda lazımsız paketlər göndərəcək.

DNS cache poisoning
DNS keşinin zəhərlənməsi – verilənlərin nüfuzlu DNS-dən (Domain Name System – Domen adları sistemi) qaynaqlanmayan keş ad serverinə ötürüldüyü qəsdən yaradılmış və ya istənməyən situasiya.

DNSSEC (Domain Name System Security Extensions)
DNS təhlükəsizlik genişlənməsi (“di-en-es-sek” kimi oxunur) – DNS protokolunun təkmilləşdirilməsidir, domen adlarının müəyyənləşdirilməsi zamanı DNS-ünvanların saxtalaşdırılması ilə əlaqəli hücumları minimallaşdırmağa imkan yaratmaq üçün işlənmişdir. DNS-kliyentlərə (ing. resolver) DNS-sorğulara autentik

cavablar verməyə (və ya məlumatın olmaması haqqında autentik cavab) və onların tamlığını təmin etməyə yönəlib. Bu zaman açıq açarlı kriptoqrafiya istifadə edilir, bütün DNSSEC cavablarında rəqəmsal imza olur. Verilənlərin əlyetərliyi və sorğuların konfidensiallığı təmin edilmir.

DNS sinkhole (**sinkhole server**, **internet sinkhole** və ya **BlackholeDNS** kimi də tanınır)
DNS qıfı – təmsil etdiyi domen adlarının istifadə edilməsinin qarşısını almaq üçün yalan informasiya verən DNS server. Hədəfdən asılı olaraq DNS qıfı həm konstruktiv, həm də destruktiv istifadə edilə bilər. İstifadələrdən biri botnetin koordinasiya üçün istifadə etdiyi DNS adlarını kəsməklə botneti dayandırmaqdır. Kompüter DNS serverlərdən əvvəl *hosts* faylına müraciət edir, bu fayldan da saytlara müraciəti bloklamaq üçün istifadə etmək olar. Məsələn, *hosts* faylına əsaslanan qıf reklam saytlarını bloklamaq üçün geniş istifadə edilir.

Domain
Domen − unikal kontekst (məsələn, girişə nəzarət parametrləri) subyektin girişə malik olduğu obyektlər çoxluğunun, proqramların yerinə yetirilməsinin unikal konteksti. İyerarxik struktura malikdir.

DoS (Denial) attack
Xidmətdən imtina hücumu ("Dos-hücum") – sistemi göstərdiyi xidmətdən imtinaya məcbur etməyə yönəlmiş haker hücumlarının geniş yayılmış növüdür; elə şərait yaradılır ki, qanuni istifadəçilərin sistemin müəyyən resurslarına girişi (tamamilə) bağlanır, ya da giriş çətinləşir.

Downgrade-attack
Zəiflətmə hücumu – şifrlənmiş bağlantını açıq mətn kimi asan istismar edilə bilən bir vəziyyətə gətirməyə çalışan mürəkkəb hücum.

Doxing (“doxxing”-in tələffüz variantı)
Doksinq – sənədlərin izlənilməsi, bir şəxs haqqında İnternet vasitəsilə özəl məlumatların araşdırılması və dərc edilməsi təcrübəsini əks etdirən qısaltma.

Droneware (ing. **drone** – idarə edilən mərmi və soft**ware** – proqram təminatı) – kompüterə məsafədən nəzarəti ələ keçirməyə imkan verən istənilən zərərli proqram nəzərdə tutulur. Adətən, droneware spamın göndərilməsi, DDoS-hücumlar və digər qanunsuz əməllər üçün istifadə edilir.

Dropper
Paraşüt – hədəf sistemdə müəyyən növ zərərli proqramı (virus, arxa qapı və s.) yükləmək üçün hazırlanmış bədniyyətli proqram. İlk dəfə 2 fevral 2000-ci ildə aşkar edilmiş və “Dropper” adlandırılmışdı, çünki yoluxdurulan kompüterlərə troyanları və ya “arxa qapı”troyanlarını yükləyirdi.

Due care
Müvafiq münasibət – menecerlərin və onların təşkilatlarının informasiya təhlükəsizliyi tədbirlərinin tipinin, qiymətinin və tətbiqinin idarə edilən sistemə müvafiq olan şəkildə təmin edilməsi məsulliyyətidir.

Due diligence
Müvafiq cəhd – təhdidlərin və risklərin identifikasiyası; müəyyən öhdəlik standartı olan sözləşməni və ya aktı imzalamadan öncə biznes və ya şəxsin araşdırılmasıdır.

E

Easter Egg
Pasxa yumurtası – tətbiqi proqram daxilində gizlədilmiş funksiya, sənədləşdirilməmiş və çox vaxt gizli komandalar və klaviatura kombinasiyası daxil edildikdə işə düşür. Pasxa yumurtalarından adətən proqram təminatı komandası haqqında informasiya göstərmək üçün istifadə edilir və təhlükəli olmaması ehtimal edilir.

Eavesdropping
Passiv dinləmə – ötürülən informasiyanın icazəsiz ələ keçirilməsi (iştirakçısı olmadığı söhbətə qulaq asılması).

Eccrowed Encryption Standart (EES)
Açarların deponə edilməsi ilə şifrləmə standartı – 1994-cü ilin fevralında ABŞ-da qəbul edilmişdi. Standart Skipjack alqoritmini və xüsusi giriş sahəsinin (Law Enforcement Access Field, LEAF) hesablanması metodunu müəyyən edir. LEAF qanunvericiliyə riayət edilməsinə nəzarət məqsədilə məxfi açarı açmağa imkan verir.

EC-Council (**International Council of Electronic Commerce Consultants**)
Elektron Kommersiya üzrə Məsləhətçilərin Beynəlxalq Şurası (**EK-Şurası**) – üzvləri tərəfindən dəstəklənən təşkilatdır. EK-Şurasının baş qərargahı Nyu-Meksiko ştatı, Albukerkede yerləşir.

ECHELON
Eşelon – elektron kəşfiyyatı üçün avtomomatlaşdırılmış sistem. ABŞ və Böyük Britaniya tərəfindən Kanada, Avstraliya və Yeni Zelandiyanın dəstəyi ilə yaradılmışdır. ABŞ Milli Təhlükəsizlik Agentliyi ECHELON sisteminin işini koordinasiya edir. ECHELON-un konkret vəzifələri və texniki xarakteristikaları olduqca məxfidir, lakin məlumdur ki, sistem ümumdünya informasiya trafikinin 95%-ə qədərini avtomatik rejimdə "ələməyə" qadirdir (peyk, radio və mikrodalğalı rabitə xətləri üzrə trafik daxil

olmaqla), açar sözləri və frazaları aşkarlayır, ilkin müqayisə, analiz aparır və kəşfiyyat məlumatları hazırlayır.

Egress Filtering
Çıxış süzülməsi − daxili şəbəkənin mənbə ünvanları kimi saxta IP-ünvanlardan istifadə edərək şəbəkədən çıxan paketləri bloklama prosesi.

Elevation of privilege
İmtiyazın artırılması **–** hücum edənə ilkin nəzərdə tutulan imtiyazlardan üstün hüquqlar verilməsi.

End-to-end encryption
Abonent şifrləməsi − telekommunikasiya vasitələri ilə ötürülən informasiyanın kriptoqrafik metodlarla bilavasitə göndərənlə alan arasında mühafizəsi.

Enigma
Eniqma – İkinci Dünya müharibəsi zamanı istifadə edilən alman rotorlu şifratoru.

ENISA (European Network and Information Security Agency)
Avropa Şəbəkə və İnformasiya Təhlükəsizliyi Agentliyi – məqsədi şəbəkə və informasiya təhlükəsizliyi sahəsində mədəniyyətin formalaşdırılması yolu ilə Avropa İttifaqında şəbəkə və informasiya təhlükəsizliyinin səviyyəsini yüksəltməkdir. ENISA 2004-cü ilin yanvarında Avropa Nazirlər Şurası və Avropa Parlamenti tərəfindən "yüksək texnologiya" cinayətlərinə cavab vermək üçün yaradılmışdı.

ESP (Encapsulating Security Payload)
Şifrlənmiş verilənlərin inkapsulyasiyası protokolu – IPSec-in nüvəsini təşkil edən üç protokoldan biri (digərləri AH və IKE). Ötürülən verilənləri şifrləməklə konfidensiallığı təmin edir, verilənlərin autentifikasiyasını və tamlığını da dəstəkləyə bilər.

Entrapment
Tələqurma – cəhd edilən müdaxilələrin aşkarlanması məqsədilə və ya hücum edənin hansı boşluqlardan istifadə edə bilməsini çaşdırmaq üçün verilənlərin emalı sistemindəki aşkar boşluqların qəsdən "gizlədilməsi".

Enumeration
İnventarlaşdırma – hücum obyektində şəbəkə resursları, o cümlədən birgə istifadə edilən resurslar, istifadəçilər və istifadəçi qrupları, tətbiqi proqramlar barəsində məlumatların toplanması.

Ephemeral keys
Birgünlük açarlar – açar qurma prosesinin hər icrası zamanı statistik unikal olan və və açar növünün başqa tələblərini ödəyən (məsələn, hər bir məlumat və ya sessiya üçün unikallıq) qısaömürlü kriptoqrafik açarlar.

Escrow
Şərti depozitə qoyma − yalnız müəyyən şərti yerinə yetirməsi halında depozit qoyana vermək üçün üçüncü şəxsə verilmiş nəsə (məsələn, sənəd, şifrləmə açarları).

Evaluated Products List (EPL)
Aprobasiya olunmuş məhsulların siyahısı − qiymətləndirilən və TCSEC (Trusted Computer System Evaluation Criteria) standartına − Narıncı kitaba müvafiq olaraq müəyyən sinfə uyğunluğu təsdiqlənən avadanlığın, aparatların və proqram təminatının siyahısı. EPL siyahısı ABŞ Milli Təhlükəsizlik Agentliyinin nəşr etdirdiyi "Information System Security Products and Services Catalogue" kataloquna daxil edilib.

Event
Hadisə –- sistemdə və ya şəbəkədə müşahidə edilə bilən istənilən hadisə.

Exhaustive attack
Tükədici hücum – parolları və ya açarları bütün mümkün qiymətlərini yoxlamaqla tapmaq cəhdi.

Exhaustive key search
Tükədici açar axtarışı – açarın bütün mümkün qiymətlərini yoxlamaqla kriptoqrafik açarı tapmaq cəhdi.

Exploitable channel
İstismara yararlı kanal – informasiya sisteminin informasiya təhlükəsizliyi siyasətinin pozulmasına imkan verən və informasiya sisteminə nəzərən xarici olan subyekt tərəfindən aşkarlana və istifadə edilə bilən kanal.

Exploit Code
Əməliyyat kodu – bədniyyətliyə sistemə avtomatik girməyə imkan verən proqram.

Exposure
İstismar – konkret hücumun verilənlərin emalı sisteminin ayrı-ayrı boşluqlarından istifadə edə bilməsinin mümkünlüyü.

Extra sector
Əlavə sektor – kopyalama əleyhinə qorunma metodunun bir hissəsi kimi cığıra sektorların standart miqdarından artıq yazılan sektor.

Extra track
Əlavə cığır – surətçıxarma əleyhinə qorunma metodunun bir hissəsi kimi diskə cığırların standart miqdarından artıq yazılan cığır.

F

Fail-safe
İmtinaya dayanıqlı sistem – komponentinin müəyyən funksiyanı yerinə yetirməkdən imtinası zamanı etibarlılığı saxlayan sistem.

Failover
İmtinaya dayanıqlılıq – işləyən tətbiqi proqramın, serverin, sistemin, aparat komponentinin və ya şəbəkənin sıradan çıxması və ya dayanması baş verdikdə ehtiyat serverə, sistemə, aparat komponentinə və ya şəbəkəyə avtomatik qoşulması.

Fail-secure və ya **Fail-safe**
İmtinaya dayanıqlı qurğu – qəza baş verdikdə başqa qurğulara zərər vurulmayacaq və ya minimal zərər vurulacaq şəkildə və insanlara təhlükə yaratmayacaq tərzdə hərəkət edən qurğu.

Fail-soft operation
İmtinaya dayanıqlı əməliyyat – sistemin qəza baş verdikdə mümkün qədər çox funksiyanı və verilənləri qoruyub saxlamaq qabiliyyəti.

Failure access
Səhv səbəbindən giriş – verilənlərin emalı sistemində verilənlərə avadanlıq və ya proqram təminatının nasazlığından irəli gələn, səlahiyyət olmadan və adətən, təsadüfən baş verən giriş.

Fake sector
Saxta sektor – icazəsiz kopyalama proqramının diskdə kopya yaratmasının qarşısını almaq üçün diskə böyük sayda istifadə edilən, verilənlər olmadan yalnız başlıqdan ibarət olan sektor.

False Acceptance Rate (FAR)
Səhv qəbul əmsalı – biometrik sistemin qanuni istifadəçini səhv tanıması və ya basqasının adını mənimsəyən şəxsi sistemə

buraxması ehtimalı. Bu əmsal hesablanarkən güman edilir ki, basqasının adını mənimsəyən şəxs passiv cəhdlər edir.

False negative
Yalan mənfi – IDS-in bədniyyətli fəaliyyət baş verdiyi halda həyəcan siqnalı verməməsi halı.

False positive
Yalan müsbət – IDS-in bədniyyətli fəaliyyətin baş vermədiyi halda səhvən həyəcan siqnalı verməsi.

False Rejection Rate (FRR)
Səhv imtina əmsalı – biometrik sistemin istifadəçinin kimliyini müəyyən edə bilməməsi və ya qanuni istifadəçinin kimliyini yoxlayanda səhv etməsi ehtimalı.

Fault tolerance
İmtinalara dayanıqlıq – səhvlər və ya imtinalar olduqda sistemin və ya proqramın düzgün işləməsini saxlaması xassəsi.

Fast flux
Sürətli axın – proksi kimi çıxış edən yoluxmuş hostların daim dəyişən şəbəkəsidir, botnetlər tərəfindən fişinq və zərərli proqram təminatı yayan saytları gizlətmək üçün istifadə edilən üsuldur.

FedCIRC (Federal Computer Incident Response Capability)
FedCIRC – 1996-cı ildə ABŞ-da NIST, CERT/CC və CIAC-ın iştirakı ilə yaradılmış təşkilat. Bu mərkəz qeyri-hərbi federal hakimiyyət orqanlarını müvafiq informasiya ilə təmin edir. FedCIRC-in ünvanı http://csrc.nist.gov/fedcirc/.

Federal Information Processing Standard (FIPS)
Federal informasiya emalı standartı – ABŞ federal agentlikləri tərəfindən istifadə üçün qəbul olunmuş standart. ABŞ Ticarət

Nazirliyinə tabe olan Milli Texnologiyalar və Standartlar İnstitutu tərəfindən nəşr edilir.

File Integrity Checker
Faylın tamlığına nəzarətçi – fayllarda dəyişiklikləri aşkarlamaq üçün onların heş kodlarını hesablayan, saxlayan və müqayisə edən proqram təminatı.

FIREFLY
FIREFLY – açıq açarlı kriptoqrafiya əsasında açarların idarə edilməsi protokolu.

Firewall
Şəbəkələrarası ekran və ya ***şəbəkə ekranı*** – verilmiş qaydalara uyğun olaraq OSI modelinin müxtəlif səviyyələrində şəbəkə paketlərinə nəzarəti həyata keçirən aparat və/və ya proqram vasitələri kompleksidir.
Şəbəkələrarası ekranın əsas vəzifəsi kompüter şəbəkələrinin və ya ayrıca qovşaqların icazəsiz girişlərdən qorunmasıdır. Şəbəkələrarası ekranları çox vaxt *süzgəc* də adlandırırlar, çünki onların əsas vəzifəsi – konfiqurasiyada müəyyən edilmiş meyarlara uyğun gəlməyən paketləri buraxmamaqdır (süzməkdir).
Şəbəkələrarası ekranlar həm də xarici mühitə yönələn informasiya axınına nəzarət edir və beləliklə, daxildə konfidensiallığı təmin edir.

Firmware
Proqramlaşdırılan avadanlıq – kriptoqrafik modulun aparat təminatında saxlanan və icra zamanı dinamik yazmaq və ya dəyişdirmək mümkün olmayan proqramlar və məlumat komponentləri.

FIRST (Forum of Incident Response and Security Teams)
İnsidentlərin emalı və təhlükəsizlik komandalarının beynəlxalq forumu (http: //www.first.org). 1990-cı ildə 11 iştirakçının dəstəyi ilə (CERT/CC, CIAC və s.) yaradılmışdı. Hazırda FIRST tərkibinə

dünyanın müxtəlif ölkələrindən 200-dən çox CERT-komandası daxildir.
FIRST illik Computer Security Incident Handling Workshop simpoziumunun təşkilatçısıdır. Bu simpoziumda təkcə FIRST iştirakçıları deyil, bütün arzu edənlər iştirak edə bilər. FIRST yalnız öz iştirakçıları üçün ildə 2-3 dəfə qapalı kollokviumlar təşkil edir.
CERT-komandalarının əlaqələndiricisi olan FIRST forumu kompüter sistemlərində boşluqlar və onlara hücumlar haqqında məlumat nəşr etmir.

Flaw
Defekt – informasiya sistemində təhlükəsizlik mexanizmlərindən yan keçməyə və ya onların söndürülməsinə imkan verən səhv, gözdən qaçırma və ya səhlənkarlıq.

Flooding
Daşqın – 1) daxil olan hər bir paketi öz ünvanı istisna olmaqla bütün çıxış ünvanlarına göndərən sadə marşrutlaşdırma alqoritmi.
2) xidmətdən imtina ilə nəticələnən, böyük həcmdə verilənlərin təsadüfi və ya bilərəkdən daxil edilməsi.

Footprinting
Ayaq izinin alınması – kompüter sistemləri və onların mənsub olduqları təşkilatlar və ya şəxslər haqqında məlumatların toplanması. Müxtəlif kompüter təhlükəsizliyi üsulları tətbiq etməklə həyata keçirilir.

Formal security policy model
Təhlükəsizlik siyasətinin formal modeli − təhlükəsizlik siyasətinin ciddi riyazi təsviri. Sistemin başlanğıc vəziyyətinin təsvirini, sistemin bir vəziyyətdən digərinə keçid üsullarını, həmçinin təhlükəsiz vəziyyətin müəyyən edilməsini nəzərdə tutur. Etibarlı hesablama bazasının əsası kimi qəbul edilməsi üçün modeldə aşağıdakı müddəaların formal isbatı olmalıdır:

- sistemin başlanğıc vəziyyəti təhlükəsizdir;

- əgər modelin müəyyən etdiyi bütün təhlükəsizlik şərtləri ödənirsə, onda sistemin bütün sonrakı vəziyyətləri təhlükəsiz olacaqdır.

Formal modelə misal Bell-LaPadula modelidir.

Fortezza

Capstone layihəsindəki alqoritmlərin reallaşdırılması üçün PCMCIA-kart, ABŞ Milli Təhlükəsizlik Agentliyi tərəfindən yaradılmışdır, əvvəllər "Tessera" adlanırdı.

Forward recovery

İrəliyə bərpa – jurnalda qeydə alınmış verilənlərdən və əvvəlki versiyadan istifadə edilməklə verilənlərin sonrakı versiyasına aid verilənlərin yenidən yaradılması.

Fuzzing

Fazzinq – proqram təminatının test edilməsinin qara qutu üsulu; səhv formalaşdırılmış verilənləri avtomatik rejimdə daxil etməklə reallaşdırma xətalarının aşkarlanmasından ibarətdir.

G

G-DES
G-DES – 1983-cü ildə Şaumüller-Bihl (Schaumuller-Bichl) tərəfindən DES alqoritmini sürətləndirmək və gücləndirmək üçün təklif edilmiş variant. Daha böyük bloklarla işləyir. 1993-cü ildə E.Biham və A.Şamir bu alqoritmin dözümünün DES alqoritmindən aşağı olmasını göstərmişdilər.

Greedy algorithm
"Acgöz" alqoritm – yerinə yetirilmə zamanı sistem resurslarını inhisara almağa çalışan və digərlərinə onlardan istifadə etməyə imkan verməyən proqram. Bu növ proqramlar xidmətdən imtina hücumlarına səbəb ola bilər.

Green Book
Yaşıl kitab – Almaniyanın "Narıncı kitab"a cavabıdır. Bu sənəd 1990-cu ildə Ümumavropa "Ağ kitabı" üçün əsas kimi təklif edilmişdi. "Yaşıl kitab" Böyük Britaniya, Almaniya, Fransa və Hollandiya hökümətləri tərəfindən bəyənilmişdi.
"Narıncı kitab"dan fərqli olaraq "Yaşıl kitab" konfidensiallıqdan əlavə, informasiyanın tamlığına və əlyetərliyinə də baxır. Bu sənəd hərbi sahə ilə yanaşı, biznes sektoru üçün də nəzərdə tutulmuşdu.

Group signature
Qrup imzası – 1990-cı ildə Şaum və Van Heyst tərəfindən təklif edilmiş rəqəmsal imza sxemidir. Qrupun istənilən üzvünə məlumatı elə imzalamağa imkan verir ki, yoxlama zamanı məlumatın qrupun üzvlərindən biri tərəfindən imzalandığını müəyyən etmək olar, lakin kimin imzalamasını müəyyən etmək mümkün deyil.

Guard
Mühafizə – müxtəlif təhlükəsizlik səviyyələrində fəaliyyət göstərən verilənlərin iki emalı sistemi arasında və ya istifadəçi terminalı və verilənlər bazası arasında istifadəçinin müraciət etməyə səlahiyyəti

olmadığı verilənləri süzgəcdən keçirmək üçün təhlükəsizlik filtrasiyasını təmin edən funksional vahid.

Guessed plaintext attack
Gümanlı açıq mətnlə hücum – gümana gələn açıq mətn üzrə kriptoanaliz metodu. Kriptoanalitikin əlində şifrmətn var, açıq mətni fərz edərək onu şifrmətni alanın açıq açarı ilə şifrləyir. Alınmış şifrmətni əldə olan şifrmətnlə tutuşdurmaqla gümanının doğru olub-olmadığını yoxlayır.

H

Hacker

Haker – 1) proqram təminatının və verilənlərin icazəsiz istifadəsinə yönəlmiş əməlləri həyata keçirən texniki cəhətdən səriştəli istifadəçi.

2) informasiya texnologiyaları sahəsində öz üstün bilik və bacarıqlarından istifadə edərək proqram və aparat təminatında boşluqlar tapan və bu boşluqları istismar etmək üçün orijinal yanaşmalar və proqramlar işləyən kompüter mütəxəssisi.

Hacktivist

Haktivist (*hack* və *aktivizm* sözlərindən yaranmışdır) **–** söz azadlığı, insan hüquqları, informasiya etikası kimi siyasi hədəfləri təbliğ etmək üçün kompüterlərdən və kompüter şəbəkələrindən istifadə edilməsi.

Hash-based Message Authentication Code (HMAC)

Məlumatın heş əsasında autentifikasiya kodu – heş funksiyalardan istifadə edən simmetrik açarlı autentifikasiya metodu.

HIDS (Host-based IDS)

Host-əsasl IDS – bir kompüter sistemi çərçivəsində hadisələri analiz edən IDS.

Hijacker (ing. hijacker ['haɪˌdʒækə] – təyyarə qaçıran)

"Brauzer qaçıran"– əsas məqsədi veb-brauzerin parametrlərini və davranışını dəyişmək olan zərərli proqramlardır. Brauzer qaçıranlar brauzerin ev-səhifəsini dəyişirlər və onu geri dəyişməyə imkan vermirlər; axtarış nəticələrini dəyişirlər, istifadəçini başqa saytlara yönəldirlər. Onlar casus kimi də işləyə və informasiyanı bədniyyətliyə göndərə bilərlər.

HoneyMonkey

HoneyMonkey (Strider Honey Monkey eksployt aşkarlanması sistemi) – Microsoft-un tədqiqat məqsədli bal küpəsidir. HoneyMonkey kompüter şəbəkəsindən istifadə edir, bu şəbəkə

HoneyMonkey kompüterində brauzer eksploytlarından istifadə edərək zərərli proqram təminatı quraşdıran veb-saytları axtarır.

Honeynet
Honeynet – bal küpələrinin şəbəkəsi.

Honeypot
Bal küpəsi – şübhəli aktivlik haqqında məlumat toplamaq üçün nəzərdə tutulmuş host; administratorundan başqa heç bir icazəli istifadəçisi yoxdur.

Hot site
"Qaynar" sayt – verilənlərin alternativ emalının mümkünlüyünü təmin edən tam təchiz edilmiş kompüter mərkəzi.

HTTPS (HyperText Transfer Protocol Secure və ya **HTTP with SSL/TLS)**
Şifrlənmiş HTTP – HTTP protokolunun genişləndirilmiş variantı, veb-serverlə veb-brauzer arasında ötürülən verilənlərin şifrlənməsini təmin edir. HTTPS protokolu ilə ötürülən verilənlər SSL və ya TLS kriptoqrafik protokoluna "qablaşdırılır". HTTP-dən fərqli olaraq, HTTPS üçün 443-cü TCP-portu istifadə edilir.
Protokol 1994-cü ildə Netscape Navigator brauzeri üçün Netscape Communications şirkəti tərəfindən işlənmişdi. HTTPS veb-də geniş istifadə edilir və populyar brauzerlərin hamısı tərəfindən dəstəklənir.

Hyper-V
Hiper-V – x86-64 sistemlərində virtual maşınların yaradılmnası və idarə edilməsi üçün proqram təminatıdır – hipervizordur (kod adı Viridian-dır, əvvəllər Windows Server Virtualization kimi tanınırdı).

I

IDEA (International Data Encryption Algorithm)
Verilənlərin şifrlənməsi üçün beynəlxalq alqoritm − blokun uzunluğu 64 bit, açarı 128 bit və raundların sayı 8 olan iterativ blok şifridir. Feyştel şifrlərinə aid deyil, lakin bu alqoritmdə də əsas açardan hesablanan əlavə açarlar istifadə edilir. IDEA həm proqram, həm də aparat təminatında realizə üçün yaradılmışdı. Sürəti DES-dəki kimidir. IDEA şifri xətti və diferensial kriptoanalizə qarşı dözümlüdür. 2^{51} zəif açarı var.

Identification
İdentifikasiya − sistemin müəyyən komponentlərinin tanınması prosesi; unikal, sistem tərəfindən qavranılan identifikatorların (adların) köməyi ilə aparılır və identifikasiya istifadəçiyə (və ya istifadəçinin adından fəaliyyət göstərən prosesə) öz adını sistemə bildirməyə imkan verir.

Identifier
İdentifikator – şəxsin adını və onunla bağlı atributlarını adlandırmaq üçün biometrik sistemdə açar kimi istifadə edilən unikal verilənlər sətri.

Identity
Kimlik identifikatoru – şəxsin unikal adı. Şəxslərin hüquqi adları həmişə unikal olmur, buna görə kimlik identifikatorunu unikal etmək üçün ona kifayət qədər əlavə informasiya qoşulmalıdır.

Identity theft
İdentifikator oğurluğu – bir şəxsin özünü başqa bir şəxs kimi təqdim etməsi; adətən, nəzərdə tutulur ki, təqlid edilən şəxsin identifikatoru şəxsin adından resurslara giriş əldə etmək, kredit və ya digər faydalar əldə etmək üçün istifadə edilir.

IEEE P1363
IEEE-nin işçi qrupu, RSA, Diffi-Helman və digər alqoritmlərə əsaslanan açıq açarlı kriptoqrafiya üçün standartların işlənməsi ilə məşğul olur.

IFrame (Inline Frame)
Sətirdaxili freym – veb-səhifədə başqa bir HTML sənədin içərisində yerləşdirilmiş HTML sənəd.

IKE (Internet Key Exchange)
Açarları idarəetmə protokolu – IPSec-in nüvəsini təşkil edən üç protokoldan biri (digərləri AH və IKE). Təhlükəsiz bağlantının parametrlərini avtomatik razılaşdırmağa və onun üçün açar informasiyası formalaşdırmağa (gələcəkdə isə onu təzələməyə) imkan verir. Razılaşdırma prosesində həm də bağlantı tərəflərinin autentifikasiyası baş verir.

Impact
Təsir – informasiyanın icazəsiz açıqlanması, dəyişdirilməsi, məhv edilməsi və ya informasiyanın və ya informasiya sisteminin əlyetərliyinin pozulması nəticəsində gözlənilən ziyanın həcmi.

Incident Response Plan
İnsidentə reaksiya planı – təşkilatın informasiya sistem(lər)inə qarşı bədniyyətli kiberhücumları aşkarlamaq, cavab vermək və nəticələrini məhdudlaşdırmaq üçün sənədləşdirilmiş təlimatların və ya prosedurların qabaqcadan müəyyən edilmiş çoxluğu.

Indicator of compromise (IOC)
Müdaxilə indikatoru – kompüter kriminilastikasında şəbəkə və ya əməliyyat sistemində müşahidə edilən və kompüterə edilən müdaxiləni yüksək ehtimalla göstərən artefakt.

Inference Attack
Məntiqi hücum – subyekt və ya verilənlər bazası haqqında qeyri-qanuni yolla məlumat əldə etmək üçün verilənlərin intellektual analizi ilə həyata keçirilən analiz üsuludur.

Information Assurance
İnformasiya təhlükəsizliyinə zəmanət – əlyetərliyi, tamlığı, autentifikasiyanı, konfidensiallığı və boyun qaçırmamanı təmin etməklə informasiya və informasiya sistemlərinin təhlükəsizliyini təmin edən tədbirlər.

Information flow control
İnformasiya axınının idarə edilməsi − informasiyanın yuxarı təhlükəsizlik səviyyələrindən aşağı səviyyələrə keçə bilmədiyini təsdiqləyən idarəetmə prosedurları (Bell-Lapadula modelinin müddəalarına müvafiq olaraq). İnformasiya axınlarına nəzarətin daha ümumi tərifi informasiyanın gizli kanallarla ötürülə bilmədiyini (yəni təhlükəsizlik siyasətindən yan keçərək) təsdiqləyən idarəetmə prosedurlarını nəzərdə tutur.

Information resources
İnformasiya resursları – şəxsi heyət, təchizat, fondlar və informasiya texnologiyaları kimi informasiya və bir-biri ilə əlaqəli resurslar.

Information security
İnformasiya təhlükəsizliyi – konfidensiallığı, tamlığı və əlyetərliyi təmin etmək üçün informasiyanın və informasiya sistemlərinin icazəsiz girişlərdən, istifadədən, açıqlanmaqdan, modifikasiyadan və ya məhv edilmədən mühafizəsi.

Information security policy
İnformasiya təhlükəsizliyi siyasəti – təşkilatda informasiyanın idarə edilməsi, mühafizə edilməsi və mübadiləsi qaydalarını müəyyən edən sərəncamlar, təlimatlar, reqlamentlər, qaydalar toplusu.

Information system
İnformasiya sistemi – informasiyanı toplamaq, emal etmək, istismar etmək, istifadə etmək, paylaşmaq, yaymaq və ya yerləşdirmək üçün təşkil edilmiş informasiya resurslarının toplusu.

Information System Security Officer (ISSO)
İnformasiya sistemi təhlükəsizlik mütəxəssisi – informasiya sistemi üçün müəyyən edilmiş informasiya təhlükəsizliyi səviyyəsini təmin etmək üçün məsul təyin edilmiş şəxs.

Information warfare (IW)
İnformasiya müharibəsi – rəqib üzərində üstünlüyü saxlamaq üçün üçün informasiya və kommunikasiya texnologiyalarının cəlb edilməsi və idarə edilməsi.

Ingress filtering
Giriş süzülməsi – ehtiyat IP-ünvanlardan daxil olan paketlərin bloklanması prosesi.

Initialization vector (IV)
Başlanğıc vektor – kriptoqrafik alqoritmdə şifrləmə prosesinin başlanğıc nöqtəsini müəyyən etmək üçün istifadə edilən parametr.

Input validation
Verilənlərin təsdiqlənməsi – giriş sahələrinə daxil edilən ilkin verilənlərin yoxlanması prosedurları; tətbiqi veb proqramlarda ilk müdafiə xətti kimi çıxış edir.

Inside threat
Daxili təhdid – məhvetmə, açıqlama, verilənlərin modifikasiyası və ya xidmətdən imtina vasitəsilə informasiya sisteminə zərər vurmaq potensialına malik giriş icazəsi olan obyekt.

Institute of Electrical and Electronics Engineers (IEEE)
Elektrik və Elektronika Mühəndisləri İnstitutu – tərkibində dünyanın 175 ölkəsindən 360 000 üzvü var. Dünya səviyyəsində müxtəlif texnologiyaların standartlaşdırılması məsələləri ilə məşğuldur. Kompüter şəbəkələri ilə bağlı müxtəlif standartları işləmək üçün 1980-ci ilin fevralında **802** saylı komissiya yaradılmışdı. Bu komissiyanın simsiz şəbəkələr üçün yaratdığı 802.11 standartlar ailəsi daha çox yayılıb.

In-the-Wild (ItW)
Aktiv viruslar – yalnız laboratoriyada testetmə mühitində mövcud olan zərərli proqramların əksinə olaraq, aktiv dövriyyədə olan və ya istifadəçi kompüterlərini aktiv şəkildə yoluxduran virusları və digər zərərli proqramları bildirir.

Integrity
Tamlıq − bax. data integrity və system integrity.

Intellectual property
İntellektual mülkiyyət – faydalı bədii, texniki və ya sənaye informasiyası, bilik və ya ideyalar, real nəzarət və ya virtual istifadə təqdimatı.

Interception
Ələ keçirmə – passiv dinləmədən fərqli olaraq bu aktiv hücumdur. Bədniyyətli təyinat yerinə çatdırılma prosesində informasiyanı tutur. Onu analiz etdikdən sonra informasiyanın irəli ötürülməsinə icazə verilməsi/qadağan edilməsi haqqında qərar qəbul edilir.

International Organization for Standardization (ISO)
Beynəlxalq Standartlaşdırma Təşkilatı – standartlaşdırma üzrə beynəlxalq təşkilatdır, ən müxtəlif sahələrdə, o cümlədən, informasiya təhlükəsizliyi sahəsində beynəlxalq standartların işlənib qəbul edilməsi ilə məşğul olur. 1946-ci ildə yaradılıb, standartlaşdırma üzrə milli təşkilatlar üzv kimi daxildir.

Internet Engineering Task Force (IETF)
Internet mühəndisliyi işçi qrupu– Internet-standartları və protokolları RFC sənədlərində təsvir edən fərdi mütəxəssislərin beynəlxalq təşkilatı.

Internet Keyed Payments Protocol
İnternet açarlı ödəniş protokolu – 3 və daha çox tərəf arasında təhlükəsiz ödəniş tranzaksiyalarının aparılması üçün protokol. IBM tədqiqat mərkəzində və Sürix elmi-tədqiqat laboratoriyasında işlənmişdir. Protokol açıq açarlı kriptoqrafiyaya əsaslanır.

Internet Storm Center (ISC)
İnternet Monitorinq Mərkəzi – SANS İnstitutunun İnternetdə zərərli fəaliyyətin səviyyəsini, xüsusilə də genişmiqyaslı infrastruktur hadisələrini monitorinq etmək üçün həyata keçirdiyi proqram.

Intrusion Detection System (IDS)
Müdaxilənin aşkarlanması sistemi – kompüter sisteminə və ya şəbəkəyə icazəsiz giriş faktlarını aşkarlamaq üçün nəzərdə tutulmuş proqram və ya aparat vasitəsi. Adətən, IDS arxitekturasına aşağıdakılar daxildir: **sensor altsistemi** – təhlükəsizliklə əlaqəli hadisələr haqqında verilənləri toplayır; **analiz altsistemi** – sensor məlumatları əsasında hücumları və şübhəli hərəkətləri aşkarlayır, **saxlanc** – ilkin hadisələrin və analizin nəticələrinin toplanmasını təmin edir; **idarəetmə konsolu** – IDS-lə qorunan sistemin və IDS-in öz vəziyyətini müşahidə etməyə, analiz altsisteminin aşkarladığı insidentləri nəzərdən keçirməyə, IDS-i konfiqurasiya etməyə imkan verir.

Intrusion Prevention Systems (IPS)
Müdaxilənin qarşısının alınması sistemləri – kompüter sisteminə və ya şəbəkəyə icazəsiz giriş faktlarını aşkarlayan və öz hədəflərinə çatmazdan əvvəl bu hərəkətləri dayandırmağa cəhd edən sistemlər. IPS sistemlərinə IDS-lərin genişlənməsi kimi baxmaq olar, çünki

hücumların aşkarlanması məsələsi eynidir. Fərq ondadır ki, IPS fəaliyyəti real zamanda izləməli və hücumların qarşısının alınması hərəkətlərini tez həyata keçirməlidir.

Intrusion deterrence
Müdaxilədən çəkindirmə – bədniyyətlinin qarşısında mümkün maneələr yaradılır, bu sistem administratoruna əlavə müdafiə vasitələrini qısa zamanda işə salmaq üçün vaxt qazandırır və bədniyyətlini hücumu davam etdirməkdən çəkindirir.

Intrusion deflection
Müdaxilənin sapdırılması – bədniyyətlini hücumun uğurlu olmasına və sistem resurslarına giriş əldə etdiyinə inanmağa məcbur edir. Həqiqətdə isə, bədniyyətli xüsusi yaradılmış qapalı mühitə ("qum saatı" və ya "akvarium") düşür.

Intrusion preemption
Müdaxilənin boğulması – aşkarlanan, lakin hələ tam həyata keçirilməyən müdaxilələrlə fəal mübarizə edir və onların uğurla başa çatmasına imkan vermir.

Intrusion prevention
Müdaxilənin qarşısının alınması – müdaxilənin qarşısını alır və ya onun uğurlu olmasını əhəmiyyətli dərəcədə çətinləşdirir. Honeypot, ildırımötürmə sistemləri – lighting rod systems, karantin sistemləri – quarantined faux systems, aldatma sistemləri – deception toolkits, tənha hücrə – padded cell (ing. psixiatriya xəstəxanasında keçə ilə üzlənmiş palatanı bildirir) kimi vasitələrlə həyata keçirilə bilər.

IP address
IP-ünvan ("ay-pi" kimi oxunur) – IP protokolu əsasında qurulmuş şəbəkədə qovşağın (kompüterin) unikal şəbəkə ünvanı. IPv4 versiyasında IP-ünvanın uzunluğu 4 bayt, IPv6 versiyasında isə 16 baytdır. IPv4-də IP-ünvan 32-bitlik ədəddir, onu nöqtələrlə ayrılmış 0-dan 255-ə dörd onluq ədəd şəklində göstərirlər, məsələn,

192.168.0.3. IP-ünvan iki hissədən ibarətdir: şəbəkənin nömrəsi və qovşağın nömrəsi. Windows əməliyyat sistemində IP-ünvanı komanda sətrində *ipconfig* yazmaqla bilmək olar.

IPSec (IP Security)

***IPSec (IP təhlükəsizliyi*)** – IP protokolu ilə ötürülən verilənlərin təhlükəsizliyini təmin etmək üçün protokollar toplusu. IP-paketlərin autentifikasiyasını, tamlığının yoxlanmasını və/və ya şifrlənməsini həyata keçirməyə imkan verir. IPSec-ə İnternet şəbəkəsində açarların təhlükəsiz mübadiləsi üçün protokollar da daxildir. Əsasən VPN-lərin yaradılması üçün istifadə edilir.

ISAKMP (Internet Security Association and Key Management Protocol)

İnternet təhlükəsizlik parametrlərini və açarı idarəetmə protokolu – IPSec daxilində uc qovşaqlar arasında təhlükəsizlik parametrlərinin və açarların mübadiləsini idarə edən açar mübadiləsi arxitekturasıdır. ISAKMP protokolu daha çox IKE (Internet key exchange – Internet açar mübadiləsi) və ya ISAKMP/Oakley kimi də tanınır.

J

Jailbreaking
Qaladan qaçış – Apple iOS əməliyyat sistemi işlədən qurğularda mövcud məhdudiyyətlərin proqram və aparat təminatı eksploytları vasitəsilə aradan qaldırılması prosesi. Belə qurğulara iPhone, iPod sensor, iPad və ikinci nəsil Apple TV daxildir.

Jamming
Əngəlləmə – xüsusi avadanlıq istifadə edərək simsiz şəbəkə tezliyində elektromaqnit enerjisi şüalandırmaqla şəbəkəni istifadəyə yararsız edən hücum.

Java
Cava – paralel, obyekt-yönümlü, siniflərə əsaslanan və mümkün qədər az realizə asılılığının olması xüsusi olaraq nəzərdə tutulmuş proqramlaşdırma dili.

Jitter
Titrəmə – elektronika və telekommunikasiyada periodik siqnalın nəzərdə tutulmuş həqiqi periodundan yayınması; çox zaman sinxronlaşdırma mənbəyinə nəzərən müəyyən edilir.

JSON (JavaScript Object Notation)
Java Skript Obyekt İşarələri – atribut-qiymət cütlərindən ibarət məlumat obyektlərinin ötürülməsi üçün insan tərəfindən başa düşülən mətnlərdən istifadə edən açıq standart formatı.

Jump bug
Keçid xətası – hamar, üfüqi və şaquli hərəkət etməni daxil etmək üçün ilk platforma oyunu.

K

Kerberos
Kerberos – geniş istifadə edilən autentifikasiya protokolu. “Klassik” Kerberos-da istifadəçilər Açar Paylaşma Mərkəzi (Key Distribution Center, KDC) ilə məxfi parolu bölüşürlər. Massaçusest Texnologiya İnstitutunda yaradılmışdı.

Kerckoffs principle
Kerxof prinsipi – şifrin dözümü yalnız açarın məxfiliyi ilə müəyyən edilir.

Key
Açar – şifrləmə, deşifrləmə, imza yaratma və ya imza yoxlama kimi kriptoqrafik əməliyyatları idarə etmək üçün istifadə edilən parametrlər.

Key crunching
Açar xırdalama – hər hansı prosedurun, məsələn, heş funksiyaların köməyi ilə asan yaddaqalan və mənalı sözlərdən (ifadələrdən) psevdotəsadüfi açarların yaradılması metodu.

Key escrow
Açar depoziti – açarların depozitə qoyulması prosesi: kriptoqrafik açar iki hissəyə bölünür, hər iki hissə şifrlənir və depozit xidmətinə saxlamağa verilir. Depozit xidməti açar hissələrinin qüvvədə olma müddətində etibarlı saxlanmasını təmin edən hökumət orqanıdır.
Açarlar yalnız müvafiq sorğu ABŞ Federal Məhkəməsi tərəfindən təsdiqləndikdə milli təhlükəsizlik orqanlarına verilir. Əldə edilmiş komponentlər unikal açarı bərpa etməyə və məlumatı deşifrləməyə imkan verir.

Key establishment
Açar paylanması – kriptoqrafik açarların kriptoqrafik modullar arasında təhlükəsiz paylanması prosesi.

Key exchange
Açar mübadiləsi – təhlükəsiz kommunikasiyaların qurulması üçün açıq açarların mübadiləsi prosesi.

Keylogger
Klaviatura casusu – istifadəçinin basdığı hər bir klaviatura düyməsini loq-faylda qeydə alan casus proqramının bir növü.

Key management
Açarların idarə edilməsi – bütün həyat dövrü ərzində kriptoqrafik açarların və başqa əlaqəli təhlükəsizlik parametrlərinin (məsələn, parolların) yaradılması, saxlanması, mübadiləsi, işə salınması, dayandırılması, məhv edilməsi daxil olmaqla emalını əhatə edən fəaliyyətlər.

Keystroke monitoring
Klaviatura monitorinqi – istifadəçinin basdığı klaviatura düymələrinə və ya interaktiv sessiya zamanı kompüterin cavablarına baxmaq və ya yazmaq üçün istifadə edilən proses.

Keystroke verification
Klaviatura verifikasiyası – klaviatura ilə eyni verilənlərin yenidən daxil edilməsi yolu ilə verilənlərin daxil edilməsinin doğruluğunun yoxlanması.

Known-plaintext attack
Məlum açıq mətnlə hücum – xeyli miqdarda açıq mətnin və uyğun şifrlənmiş mətnin olduğu kriptoanaliz üsulu.

L

Layer 2 Tunneling Protocol (L2TP)
İkinci səviyyədə tunel protokolu – virtual xüsusi şəbəkələrin yaradılması üçün istifadə edilən protokol. PPTP və L2F protokollarının nöqsanlarını aradan qaldırmaq üçün IETF tərəfindən işlənmişdi. Autentifikasiya üçün PAP protokolundan istifadə edir. Kriptoqrafik mühafizəni gücləndirmək üçün IPSec protokolunun elementlərindən istifadə edir.

Layer 2 Forwarding Protocol (L2F)
İkinci səviyyədə ötürmə protokolu – virtual xüsusi şəbəkələrin yaradılması üçün istifadə edilən protokol. Cisco Systems şirkətinin fəal iştirakı ilə yaradılmışdı. PPTP protokolundan əsas fərqi – IP protokolu ilə işləyən şəbəkələrdən istifadənin məcburi olmamasıdır. L2F protokolu Frame Relay və ATM şəbəkələrində mühfizəli tunellər yaratmağa imkan verir. PPTP protokolundan digər fərqi eyni zamanda bir neçə birləşməni dəstəkləməsidir. Autentifikasiya üçün PAP, TACACS+ və RADIUS protokolları istifadə edilir.

Least privilege
Minimum imtiyaz − subyektin giriş hüquqlarının yalnız səlahiyyət verilmiş tapşırıqların icrası üçün lazım olan giriş hüquqları ilə məhdudlaşdırılması. İnformasiya təhlükəsizliyi sisteminin təşkilinin əsas prinsiplərindən biridir. Hər bir subyekt onun qarşısında qoyulmuş məsələlərin həlli üçün minimal mümkün imtiyazlar çoxluğuna malik olmalıdır. Bu prinsipə əməl edilməsi bəd niyyət, səhv və imtiyazların icazəsiz istifadəsi nəticəsində mümkün pozuntulardan qoruyur.

Linear cryptanalysis
Xətti kriptoanaliz – blok şifrləri üçün məlum açıq mətn üzrə kriptoanaliz metodu. İlk dəfə 1992-ci ildə M. Matsui və A. Yamaqişi tərəfindən FEAL şifrinə hücüm üçün təklif edilmişdi. 1993-cü ildə Matsui bu metodu DES şifrinə hücum üçün

təkmilləşdirdi. 1994-cü ildə S. Lenqford və M. Helman diferensial xətti kriptoanaliz metodunu təklif etdilər.

Linear Feedback Shift Register (LFSR)
Əks əlaqəli xətti sürüşmə registri – psevdotəsadüfi bitlər ardıcllığı yaratmağa imkan verən riyazi model. Zəruri xassələrə malik açar ardıcıllıqlarının yaradılması üçün bir çox axın şifrində istifadə edilir.

Linkage
Birləşmə – mühafizə olunan informasiyanı almaq üçün verilənlərin emalı sistemindəki verilənlərin və ya informasiyanın digər sistemdəki verilənlərlə və ya informasiya ilə məntiqi birləşdirilməsi.

Link encryption
Kanal şifrləməsi − telekommunikasiya vasitələri ilə ötürülən informasiyanın kriptoqrafik metodlarla mühafizəsi. Şifrləmə iki qovşaq arasındakı rabitə kanalında həyata keçirilir (onlar göndərəndən alana gedən yolda aralıq qovşaqlar ola bilərlər).

Local area network (LAN)
***Lokal şəbəkə* (*LŞ*)** – məhdud coğrafi ərazi çərçivəsində istifadəçinin sərəncamında olan kompüter şəbəkəsi.

Log clipping
Loqun qayçılanması – sistemə girildiyini gizlətmək üçün sistem loq-faylından yazıların seçilərək silinməsi.

Logic bomb
Məntiqi bomba – müəyyən spesifik sistem şərti ilə başladıldıqda verilənlərin emalı sisteminin korlanmasına səbəb olan bədniyyətli məntiqi proqram. Ancaq müəyyən şərtlər ödənildikdə “patlayaraq”, yəni işə düşərək sistemə ziyan vururlar.

Loss
İtki – informasiya təhlükəsizliyinin pozulmasının səbəb olduğu ziyanın kəmiyyət ölçüsü.

M

Macro virus
Macro virus – sənədlərə qoşulan virusdur və sənədlərin yaradılması üçün istifadə edilən tətbiqi proqramların makro proqramlaşdırma imkanlarından istifadə edərək işə duşur və yayılır.

Maintenance book
Xidmət kitabı – proqram təminatında rahat müşaiyətə və əlavə xüsusiyyətlərin inkişaf etdirilməsinə imkan verən, qeyri-adi nöqtələrdə və ya adi yoxlamalar olmadan proqrama qeydlər etməyə şərait yaradan "arxa qapı".

Malicious code
Zərərli kod – informasiya sistemlərinin konfidensiallığına, tamlığına və ya əlyetərliyinə ziyan vura bilən icazəsiz proseslərin yerinə yetirilməsi üçün nəzərdə tutulmuş proqram.

Malicious logic
Bədniyyətli məntiq – avadanlıqda, proqram-aparat vasitəsində, proqram təminatında tətbiq edilən və məqsədi icazə verilməyən və ya zərərli əməliyyatları icra etmək olan proqram.

Malvertising ("**mal**icious ad**vertising**")
Zərərli proqram reklamçılığı – zərərli proqramları yaymaq üçün onlayn reklamdan istifadə edilməsi.

Malware (malicious soft**ware** üçün qısaltma**)**
Zərərli proqram təminatı – kompüterin əməliyyatlarını pozmaq, konfidensial məlumatları toplamaq, məlumatların tamlığını və ya əlyetərliyini pozmaq və s. məqsədilə sistemə adətən gizli daxil edilən hər hansı proqram təminatı.

Malware Attribute Enumeration and Characterization (MAEC)
Zərərli proqram təminatı atributlarının siyahısı və xarakteristikaları – zərərli proqram təminatının unikal atributları haqqında strukturlaşdırılmış informasiya toplamaq üçün dil (qrammatika, lüğət və toplama formatı). MITRE korporasiyası tərəfindən işlənmişdir.

Mandatory access control (MAC)
Girişi mandatlı idarə edilməsi − obyektlərə girişin idarə edilməsi üsulu. Obyektdə olan informasiyanın məxfilik dərəcəsinə və kritikliyinə, verilən kritiklik səviyyəsinə (xüsusi nişanlarla təsvir olunmuş) malik informasiyaya giriş zamanı subyektin səlahiyyətlərinin və hüquqlarının formal yoxlanılmasına əsaslanır.

Man-in-the-middle Attack (MitM)
Ortada adam hücumü – autentifikasiya protokolunun əsasında yerinə yetirilən hücumdur, hücum edən autentifikasiya olunan və autentifikasiya edən tərəflər arasında yerləşərək onlar arasında ötürülən verilənləri ələ keçirə və dəyişə bilər.

Manipulation detection
Manipulyasiyanın aşkarlanması – verilənlərin təsadüfən və ya bilərəkdən dəyişdirilib-dəyişdirilmədiyini aşkarlamaq üçün istifadə edilən prosedur.

Manipulation detection code
Manipulyasiyanın aşkarlanması kodu – manipulyasiyaların aşkarlanmasına imkan vermək üçün əlavə edilən verilənlər funksiyası olan bit sətri.

Masquerading
Maskarad − başqa istifadəçinin və ya sistemin adından əməliyyatların yerinə yetirilməsi cəhdləri. Maskarad hücumları maliyyə əməliyyatları zamanı və ya informasiya bir sistemdən digərinə ötürüldükdə həyata keçirilə bilər.

Media sanitization
Daşıyıcının təmizlənməsi – yaddaş daşıyıcısında yazılmış verilənlərin bərpa olunmamaları üçün adi və qeyri-adi üsullarla çevrilməsi əməliyyatlarını bildirən ümumi termin.

Message authentication code
Məlumatın autentifikasiya kodu – həm verilənlərin (açıq mətn və ya şifrlənmiş mətn), həm də məxfi açarın funksiyası olan və verilənlərin autentifikasiyasına imkan vermək məqsədilə verilənlərə əlavə edilən bit sətri.

Message digest
Məlumatın daycesti – adətən fayl üçün generasiya edilir və fayla edilən dəyişiklikləri aşkar etmək üçün istifadə edilən kriptoqrafik heş kodudur; SHA-1 məlumatın daycesti alqoritminə misaldır.

Multi-hop problem
Çoxaddımlılıq problemi – müxtəlif platformalara müraciət edən mobil agent proqramlarının yaratdığı təhlükəsizlik riskləri.

Multilevel cryptography
Çoxsəviyyəli kriptoqrafiya – simmetrik kriptosistemlər üçün kriptoqrafik açarların xüsusi metodla seçilməsinə əsaslanır, R.Rayvest tərəfindən təklif edilib. Bu mexanizmdən istifadə edən kriptosistem elə qurulur ki, ilk kriptoqrafik açar ixtiyari seçilə bilər, sonrakı açarların seçilməsi isə müəyyən qanuna tabe olmalıdır. Belə kriptosistemlərin yaradılması zərurəti ABŞ-da "güclü kriptoqrafiya"nın ixracına məhdudiyyətlərin qoyulması ilə meydana çıxmışdı.

Multilevel security
Çoxsəviyyəli təhlükəsizlik − müxtəlif şəffaflıq səviyyələrinə malik subyektlərin obyektlərə eyni zamanda girişinə icazə verən və bu zaman icazəsiz girişi qadağan edən müxtəlif kritiklik səviyyəli infortmasiyaya malik sistemlər sinfi.

Mutual suspicion

Qarşılıqlı inamsızlıq – qarşılıqlı əlaqədə olan obyektlər arasında heç bir obyektin müəyyən mülkiyyətə münasibətdə digər obyektin düzgün və ya təhlükəsiz olaraq fəaliyyət göstərəcəyinə inam ifadə etməməsini göstərən qarşılıqlı əlaqə.

N

National Computer Security Center (NCSC)
Milli Kompüter Təhlükəsizliyi Mərkəzi – ABŞ Federal hökumət təşkilatlarında təhlükəsiz sistemlərin yayılmasını dəstəkləyən və stimullaşdıran təşkilat. Zəmanətli təhlükəsizlik sistemlərinin yaradılması və analizi sahəsində əlaqələndirici orqandır. İlkin adı − ABŞ Müdafiə Nazirliyinin Kompüter Təhlükəsizliyi Mərkəzi idi (DoD Computer Security Center).

National Security Agency (NSA)
Milli Təhlükəsizlik Agentliyi (MTA) – ABŞ-da 1952-ci ildə yaradılmışdır. Bir çox kriptoqrafik standartın işlənməsində iştirak etmişdir.

Need-to-know
Zəruri bilik prinsipi – istifadəçi yalnız ona konkret funksiyanı yerinə yetirmək üçün mütləq lazım olan verilənlərə giriş əldə edir.

Network weaving
Şəbəkə toru – verilənlərin emalı sisteminə müraciət etməyə nail olmaq, aşkarlamanı və izləməni əngəlləmək məqsədilə müxtəlif kommunikasiya şəbəkələrinin istifadə edildiyi sızma texnologiyası.

NIDS (Network-based IDS)
Şəbəkə əsaslı IDS – bədniyyətlinin sistemə keçmək və ya DoS hücumu reallaşdırmaq cəhdlərini aşkarlamaq üçün bütün şəbəkə trafikini izləyir.

NIST (National Institute of Standards and Technology)
Milli Standartlar və Texnologiyalar İnstitutu – ABŞ Ticarət Nazirliyinin tabeliyində olan bu institut informasiya təhlükəsizliyinin müxtəlif məsələlərinə aid bir sıra standartlar işləyib hazırlayır.

Non-repudiation
İmtinanın qeyri-mümkünlüyü **–** informasiyanı göndərəninin çatdırmanın sübutu ilə təmin etdiyi zəmanət və qəbul edən göndərənin eyniliyinin (şəxsiyyəti) sübutu ilə təmin edilir, beləliklə sonra heç biri inkar edə bilməz ki, informasiyanı o emal edib.

Notarization
Əslliyin təsdiqi – sonradan verilənlərin kontenti, mənşəyi, vaxtı və ya çatdırılması kimi xarakteristikalarının dürüstlüyünün təminatına imkan verən etibarlı üçüncü tərəf vasitəsilə verilənlərin qeydiyyatı.

National Vulnerability Database (NVD)
İnformasiya təhlükəsizliyi boşluqları üzrə vahid baza – boşluqlar üzrə əlyetər bütün resursları vahid bazada birləşdirir, CVE standartına əsaslanır və ona tam uyğundur. NVD veb-saytında axtarış, statistika, NVD məlumatlarının bazadan XML formatında yüklənməsi xidmətləri var, onlardan qeydiyyatdan keçmədən və pulsuz istifadə etmək olar. 2005-ci ildə Milli Standartlar və Texnologiyalar İnstitutu tərəfindən istifadəyə verilib. NVD saytında (http://nvd.nist.gov/) US-CERT məlumatları, o cümlədən boşluqlar haqqında qeydlər və texniki həyəcan siqnalları da yerləşdirilir.

O

Oakley
Diffi-Helman alqoritminə əsaslanan açarların mübadiləsi protokoludur. Bir qayda olaraq ISAKMP ilə birlikdə istifadə edilir.

Obfuscation
Obfuskasiya – ilkin kodun və ya yerinə yetirilən kodun proqramın funksionallığı saxlanılmaqla kodun analizini, iş alqoritmlərinin anlaşılmasını və dekompilyasiya zamanı modifikasiyanı çətinləşdirən şəklə salınması. Obfuskasiyanı yerinə yetirmək üçün xüsusi proqram təminatı (ing. *obfuscator*) da mövcuddur.

Object
Obyekt − sistemin informasiyanı saxlayan, qəbul edən və ötürən passiv komponenti. Obyektə giriş onda olan informasiyaya girişi nəzərdə tutur. Obyektlərə misallar: yazılar, bloklar, səhifələr, seqmentlər, fayllar, direktoriyalar və proqramlar, həmçinin ayrıca bitlər, baytlar, sözlər, sahələr; müxtəlif qurğular (terminallar, printerlər, disk qurğuları vəs.); müxtəlif şəbəkə qurğuları (ayrıca qovşaqlar, kabellər və s.).

Object reuse
Obyektin təkrar istifadəsi − əvvəl bir və ya bir neçə obyektin yerləşdiyi yaddaş sahəsinin (məsələn, səhifənin, freymin, diskin, maqnit lenti sektorunun) yeni obyekt üçün ayrılması və təkrar istifadəsi. Təhlükəsizliyi təmin etmək üçün yaddaş sahəsinin yeni obyekt üçün ayrılması zamanı orada köhnə obyektlərin məlumatları olmamalıdır.

OCTAVE (**Operationally Critical Threat, Asset, and Vulnerability Evolution**) – təşkilatda informasiya təhlükəsizliyi risklərinin idarə edilməsi metodologiyasıdır. Karnegi-Mellon Universitetinin Proqram Mühəndisliyi İnstitutu tərəfindən

yaradılmışdır. Metodologiyanın tam təsviri www.cert.org/octave saytında var.

Offset track
Kompensasiya cığırı – surətçıxarma əleyhinə qorunma metodunun bir hissəsi kimi diskə qeyri-standart mövqeyə yazılan cığır.

One-time pad
Birdəfəlik bloknot – Vernam şifri də adlanan kriptosistem, tam təsadüfi generasiya olunan bitlər sətrindən istifadə edir. Açar axının uzunluğu açıqmətnin uzunluğuna bərabərdir. Şifrmətni almaq üçün açıq mətn və açar axını bitləri XOR əməlindən istifadə etməklə toplanır. Belə sistem mütləq düzümə malikdir. Əsasən hərbi və diplomatik məqsədlər üçün istifadə edilir. Əsas nöqsanı – açarların idarə edilməsindəki çətinliklərdir.

One-time signature
Birdəfəlik imza – istənilən məlumat üçün rəqəmsal imzanın yalnız bir dəfə istifadə edilə biləcəyi rəqəmsal imza sxemi, hər yeni məlumat üçün yeni açar cütü istifadə edilir. Belə sxemin üstünlüyü – yüksək sürət, nöqsanı – böyük həcmdə informasiya (açıq açarlar) nəşr etmək zərurətidir, çünki açar cütü yalnız bir dəfə istifadə edilir.

One-way function
Biristiqamətli funksiyalar – biristiqamətli funksiyaların varlığı indiyədək isbat edilməyib. Məlumatın şifrlənməsi üçün biristiqamətli funksiyalar istifadə edilmir, çünki onların köməyilə şifrlənmiş mətni hətta şifrləyən şəxs belə açа bilmir. Şifrləmə üçün məxfi girişli biristiqamətli funksiyalar istifadə edilir.

One-way trapdoor function
Məxfi girişli biristiqamətli funksiyalar– əsasında məxfi açarların mübadiləsi və açıq açarlı kriptosistemlər təklif edilmişdir. Belə funksiyaların tədqiqi əsasən aşağıdakı istiqamətlər üzrə aparılır:
– diskret loqarifm məsələsi – Diffi-Helman sxemi, DSA və s.

– tam ədədlərin vuruqlara ayrılması məsələsi – RSA və s.
– səhv düzəldən kodlar – Mak-Ellis sxemi, Niderrayter sxemi və s.
– NP-tam məsələlər – "çanta" məsələsi və s.
– elliptik əyrilərdə diskret loqarifm məsələsi – ECDSA və s.

On-Line Certificate Status Protocol (OCSP)
Onlayn sertifikat statusu protokolu – açıq açar sertifikatının statusunu onlayn müəyyən etmək üçün istifadə edilən protokol.

Online predators
Onlayn yırtıcılar – İnternet üzərindən uşaqların cinsi istismarıyla məşğul olan insanlar.

Open-source intelligence (**OSINT**)
Açıq mənbə kəşfiyyatı – açıq mənbələrdən toplanmış kəşfiyyat məlumatları.

OSSIM (**Open Source Security Information Management**
İnformasiya təhlükəsizliyinin açıq kodlu təminat əsasında idarə edilməsi – vahid açıq arxitektura çərçivəsində müxtəliv tipli utilitlərin mümkün olduqca geniş inteqrasiyası. Nəticədə verilənləri toplamaq və toplanmış verilənlərdə qanunauyğunluqları tapmaq və izləmək imkanı yaranır. Verilənlərin mənbəsi kimi real zamanda sistem və şəbəkə verilənlərini analiz edən istənilən utilit çıxış edə bilər. Hazırda OSSIM çərçivəsində inteqrsiya olunmuş alətlərin siyahısı kifayət qədər genişdir: Arpwatch, P0f, pads, Nessus/OpenVAS, Ntop, Snort, tcptrack, tcpdump, Nmap, Spade, Nagios, Osiris, OCSInventory-NG, OSSEC, RRDTool (əlavə olaraq, preludeIDS, NTsyslog, Snare, Cisco Secure IDS tərəfindən toplanan verilənlərin analizi də mümkündür).

Open Source Vulnerability DataBase (OSVDB)
Boşluqlar üzrə açıq verilənlər bazası – proqram və aparat təminatındakı boşluqlar haqqında məlumatlar yayımlayan müstəqil və açıq mənbə. Yaradılması 2002-ci ildə Black Hat və Defcon

konfranslarında qərara alınıb. Hazırda OSVDB layihəsi çərçivəsində 200-ə yaxın könüllü mütəxəssis tərəfindən boşluqlar üzrə mərkəzləşdirilmiş verilənlər bazası yaradılıb, bazaya giriş açıqdır və axtarış vasitələri var. Verilənlər bazasında hər bir boşluğa unikal OSVBD ID nömrəsi verilir.

Open Web Application Security Project (OWASP)
Tətbiqi veb proqramların təhlükəsizliyi üzrə açıq layihə – tətbiqi veb proqramların təhlükəsizliyi ilə məşğul olan onlayn cəmiyyət.

P

Packet sniffer
Paket snifferi – şəbəkə trafikini müşahidə edən və qeydiyyata alan proqram təminatı.

Padlocking
Kilidləmə – verilənləri və ya proqram təminatını icazəsiz kopyalamaqdan qorumaq üçün xüsusi üsullardan istifadə edilməsi.

Passive attack
Passiv hücum – autentifikasiya protokoluna qarşı hücum; bu zaman hücum edən autentifikasiya edilən və autentifikasiya edən arasında şəbəkədə gedən məlumatları ələ keçirir, lakin məlumatları dəyişdirmir.

Passive threat
Passiv təhdid – verilənlərin emalı sisteminin vəziyyətini dəyişdirmədən informasiyanın açıqlanması təhlükəsi.

Passive wiretapping
Passiv dinləmə – verilənləri əldə etmək məqsədilə telefon məlumatlarının gizli dinlənilməsi.

Pass the hash
Heş keçidi – hakerə parol əvəzinə parolun NTLM və ya LanMan heş-kodundan istifadə edərək məsafədəki sereverdə/servisdə autentifikasiya olunmağa imkan verən hakinq üsulu.

Password
Parol – autentifikasiya məlumatı kimi istifadə edilən *simvol sətri*.

Password Authentication Protokol (PAP)
Parolun autentifikasiyası protokolu – kommutasiya edilən xətlərlə qoşulma protokolu (Point-to-Point Protocol, PPP) üçün autentifikasiya protokolu. Protokol istifadəçi identifikatorunun və

parolun şifrələnmiş şəkildə göndərilməsini nəzərdə tutur. Autentifikasiya prosesinə təşəbbüs edən kompüter identifikator və parolun göndərilməsini autentifikasiya sistemi istifadəçinin həqiqiliyini təsdiq edənə və qoşulmanı kəsənə kimi davam etdirir.

Patch
Yamaq **-** kompüter proqramını və ya onu dəstəkləyən verilənləri yeniləmək və onlarda düzəlişlər etmək üçün nəzərdə tutulmuş proqram təminatı.

PDCA (Plan-Do-Check-Act)
PHYT (***Planlaşdırma-Həyata keçirmə-Yoxlama-Təkmilləşdirmə***) – proseslərin fasiləsiz yaxşılaşdırılması üzrə məşhur modeldir, informasiya təhlükəsizliyinin idarə edilməsi üzrə ISO/IEC 27001 standartının və digər standartların əsasında dayanır. PHYT tsiklinin mərhələlərini İnformasiya Təhlükəsizliyinin İdarə edilməsi Sistemi (İTİS) üçün qısaca aşağıdakı kimi ifadə etmək olar:
1. *Planlaşdırma*. İTİS-i yaradın.
2. *Həyata keçirmə*. İTİS-i həyata keçirin və istismar edin.
3. *Yoxlama*. İTİS-in monitorinqi və yoxlanması.
4. *Təkmilləşdirmə*. İTİS-i işlək vəziyyətdə saxlayın və təkmilləş-dirin.
PDCA tsikli Şuhart-Deminq tsikli kimi də tanınır.

Penetration
Nüfuzetmə − təhlükəsizlik mexanizmlərindən uğurla keçilməsi.

Penetration testing (qısa formada **pentest**)
Nüfuzetmə testi – təşkilatın sifariş əsasında informasiya təhlükəsizliyi mexanizmlərinin yoxlanması üzrə göstərilən xidmət. Ekspertlər belə testləri yerinə yetirməklə potensial bədniyyətli kimi istifadə edilən təhlükəsizlik mexanizmlərindən yan keçməyə, sifarişçinin daxili şəbəkəsinə sızmağa və infrastrukturun kritik vacib komponentlərinə giriş əldə etməyə cəhd edirlər. Nüfuzetmə testlərinin köməyi ilə təhlükəsizlik sisteminin nöqsanları aşkarlanır və onların istismarının mümkün nəticələri qiymətləndirilir.

Perfect Forward Secrecy (PFS)
Birbaşa mükəmməl məxfilik – bəzi açar razılaşdırma (ing. key-agreement) protokollarının xassəsi. Zəmanət verilir ki, uzunmüddətli açarlar toplusunun köməyi ilə generasiya edilmiş sessiya açarları uzunmüddətli açarlardan biri ələ keçdikdə sındırılmayacaq.

Perl – yüksək səviyyəli, ümumi təyinatlı, interpretatorla işləyən, dinamik proqramlaşdırma dilləri ailəsi.

Personnel security
Şəxsi heyətin təhlükəsizliyi − kritik informasiyaya girişi olan bütün şəxslərin zəruri icazə və müvafiq səlahiyyətlər almasını təsdiqləyən prosedurlar.

PGP (Pretty Good Privacy) − şifrləmə və rəqəmsal imza əməliyyatlarını yerinə yetirməyə imkan verən kriptoqrafik funksiyalar kitabxanası. İlkin versiyası 1991-ci ildə Filip Zimmerman tərəfindən işlənmişdi. OpenPGP (RFC 4880) standartı sayəsində PGP-nin funksional imkanları müxtəlif, lakin öz aralarında və digər proqramlarla (GnuPG, FileCrypt və s.) uyuşan bir sıra realizələri var. Geniş yayılmış əməliyyat sistemlərinin hamısı üçün realizələri mövcuddur. Pulsuz yayılan realizələri ilə yanaşı, kommersiya realizələri də vardır.

Pharming
Farminq – veb-saytın trafikini saxta sayta (adətən, fişinq saytına) yönləndirən kiberhücum. Farminq hücumunu hədəf kompüterdəki "hosts" faylını dəyişməklə və ya DNS serverin proqram təminatında boşluğu istismar etməklə həyata keçirmək olar. DNS serverlər veb-sayt adlarını real IP-ünvanlara çevirir. Korlanmış DNS serverləri bəzən "zəhərlənmiş" adlandırırlar.

Phishing
Fişinq ("***balıq ovu***") – aldadıcı kompüter vasitələrinin köməyi ilə istifadəçilərin konfidensial fərdi məlumatları açıqlamağa məcbur edilməsi.

PHP (*PHP: Hypertext Preprocessor*; əvvəllər *Personal Home Page Tools*; "*pi-eyç-pi*" *kimi tələffüz edilir*) – server tərəfdə veb proqramlaşdırma üçün yaradılmış proqramlaşdırma dili; ümumi təyinatlı proqramlaşdırma dili kimi də istifadə edilir.

Phreaking
Frikinq – telefon şəbəkələrinə qoşulmuş cihazlar və avadanlıqlar kimi telekommunikasiya sistemlərini araşdıran, eksperimentlər aparan, öyrənən insanların fəaliyyətini təsvir edir.

Physical security
Fiziki təhlükəsizlik − sistemin resurslarına və kritik informasiyaya fiziki təhdidlərə (sındırma, oğurluq, terror aktı, həmçinin yanğın, daşqın və s.) qarşı tədbirlərin və ya fiziki maneələrin və yoxlama prosedurlarının həyata keçirilməsi.

Piggyback entry
"Donuz belində" giriş – səlahiyyətli istifadəçinin qanuni bağlantısı vasitəsilə verilənlərin emalı sisteminə səlahiyyət olmadan giriş.

Ping of Death Attack
Ölümcül pinq hücumu – 1990-cı illərdə Unix, Linux, Mac, Windows, şəbəkə printerləriu və marşrutizatorlar daxil olmaqla müxtəlif əməliyyat sistemlərində və şəbəkə qurğularında yayılmış DoS hücum növüdür, hazırda əksər sistemlərdə bu problem aradan qaldırılıb. Uzunluğu 65 535 baytdan böyük ICMP-paketin göndərilməsi kompüterin şəbəkə stekini dolduraraq kompüteri çökdürmək mümkündür. Bu uzunluqda paketi şəbəkədə bir dəfəyə göndərmək olmur, ona görə onu hissələrə (fraqmentlərə) bölüb göndərirlər. Windows-da olan *pinq* proqramı paketləri asanlıqla fraqmentləşdirdiyi üçün bu hücum növü belə adlandırılmışdı.

Point-To-Point Tunneling Protocol (PPTP)
Nöqtə-nöqtə tunel protokolu – virtual xüsusi şəbəkələrin yaradılması üçün protokol. Ascend Communications, Microsoft və

bir sıra digər şirkətlər tərəfindən işlənmişdi. Əsasən, şəbəkə resurslarına məsafədən girişin təşkili üçün nəzərdə tutulmuşdu (məsələn, mobil istifadəçilər üçün). Bu protokol Microsoft şirkətinin məhsullarına, o cümlədən Windows NT və Windows 98 əməliyyat sistemlərinə daxil edilmişdi. PPTP protokolu parol generatorlarının köməyi ilə istifadəçilərin autentifikasiyası sxemləri və şifrəmə üçün güclü vasitələri dəstəkləmir. Autentifikasiya üçün PAP istifadə edilir.

Polyinstantiation
Çoxnüsxəlilik – birdən çox müstəqil nüsxədə (obyektlər, nüsxələr) kimi reallaşdırılan növ konsepsiyası (kateqoriya, verilənlər bazası sətri və s.).

Port
Port – IP-paketin hansı tətbiqi proqram üçün nəzərdə tutulduğunu göstərən 1-dən 65535-ə kimi şərti ədəd. Portlardan istifadə edilməsi bir kompüterdə bir neçə tətbiqi proqramın eyni vaxtda TCP protokolundan istifadə etməsinə imkan verir. Məsələn, HTTP protokolu 80, SMTP isə 25 nömrəli TCP portundan istifadə edir.

Port scanning
Portların skanlanması – xüsusi proqramlardan istifadə etməklə sistemdə hansı portların açıq olmasının məsafədən müəyyən edilməsi.

Precursor
Prekursor – hücum edənin insidentə səbəb olmağa hazırlaşmasını göstərən əlamət.

Preferred Products List (PPL)
Üstün məhsulların siyahısı − TEMPEST proqramı üzrə sınaqlardan keçən və ABŞ Milli Təhlükəsizlik Agentliyinin (MTA) digər tələblərinə cavab verən kommersiya məhsullarının (aparatlar və avadanlıq) siyahısı. Üstün məhsullar siyahısı MTA tərəfindən nəşr

edilən “Information System Security Products and Services Catalogue” kataloquna daxildir.

Privacy
Məxfilik – istifadəçinin və ya etibarlı tərəfin məlumatlarına girişin qanunvericilik və informasiya təhlükəsizliyi siyasəti əsasında məhdudlaşdırılması.

Privacy Enhandced Mail (PEM)
E-poçt məlumatlarının mühafizəsi standartı – məlumatların şifrlənməsini və rəqəmsal imzalanmasını təmin edir. Bu standart RFC 1421-1424 sənədlərində təsvir olunur.
PEM-də aşağıdakı təhlükəsizlik mexanizmləri reallaşdırılır:
- məlumatın imzalanması;
- məlumatın şifrlənməsi və imzalanması.

Hər bir PEM-məlumatda göndərənin rəqəmsal imzası olur.

Privacy protection
Məxfiliyin qorunması – məxfiliyi təmin etmək üçün görülən tədbirlər.

Private Key
Gizli açar – adətən rəqəmsal imza və ya məlumatın şifrlənməsi üçün istifadə edilən asimmetrik açar cütünün məxfi hissəsi.

Privileged Accounts
***İmtiyazlı hesablar* – v**erilən sistemdə digər istifadəçilərə “giriş hüquqları” vermək hüququna malik olan istifadəçilərə məxsus hesablar.

Profiling
***Profilləmə (profaylinq)* –** verilənlərin analizi sistemi tərəfindən generasiya edilən profillərin hazırlanması və istifadə edilməsi prosesi.

Prosess
Proses − yerinə yetirilən proqramlar.

Protection key
Yaddaşın mühafizə açarı – proqrama ayrılmış yaddaş blokuna verilən və yaddaşın müraciətləri üçün istifadə edilən kod. Mühafizə açarı ilə üst-üstə düşməlidir, əks halda proqramın işi qəza kodu ilə dayandırılır.

Protocol
Protokol − sistemin müxtəlif komponentlərinə (məsələn, şəbəkənin qovşaqlarına) informasiyanı mübadilə etməyə imkan verən semantik və sintaksis qaydalar və formatlar toplusu.

Proxy
Proksi – kliyentlə server arasında əlaqə "quran" tətbiqi proqram.

Proxy Agent
Proksi agent – şəbəkələrarası ekranda və ya xüsusi serverdə qurulan tətbiqi proqram təminatıdır; protokolları filtrasiya etmək və onları qurğunun interfeysləri arasında yönəltmək imkanı var.

Proxy server
Proksi server – kliyent tətbiqi proqramı, məsələn, veb-brauzer və real server arasında yerləşən server.

Public key
Açıq açar – rəqəmsal imzaları yoxlamaq üçün və ya verilənləri şifrləmək üçün istifadə edilən asimmetrik açar cütünün açıq hissəsi.

Public key certificate
Açiq açar sertifikatı – istifadəçinin adını və açıq açarını əlaqələndirən, sertifikat xidməti mərkəzinin gizli açarı ilə imzalanmış rəqəmsal sənəd.

Public Key (Asymmetric) Cryptographic Algorithm
Açıq açarlı (asimmetrik) şifrləmə alqoritmi – əlaqəli iki açardan – açıq açardan və gizli açardan istifadə edən kriptoqrafik alqoritm.

Public Key Cryptography Standards (PKCS)
Açıq açarlı kriptoqrafiya standartları – RSA Data Security şirkəti tərəfindən qeyri-formal konsorsiumla birlikdə yaradılmışdı. Konsorsiuma ilk vaxtlar Apple, Microsoft, DEC, Lotus, Sun və MIT daxil idi. Hazırda PKCS#1, PKCS#3, PKCS#5, PKCS#6, PKCS#7, PKCS#8, PKCS#9, PKCS#10, PKCS#11 standartları nəşr edilib.
PKCS həm alqoritmdən asılı, həm də alqoritmdən asılı olmayan realizələri müəyyən edir. Bir çox alqoritm dəstəklənir, lakin yalnız Diffi-Helman və RSA alqoritmləri ətraflı təsvir olunur. PKCS standartları vaxtaşırı nəzərdən keçirilir və kriptoqrafiya sahəsində son nailiyyətlər nəzərə alınmaqla əlavələr edilir.

Public Key Infrastructure (PKI)
Açiq açar infrastrukturu – açıq açar sertifikatlarının verilməsi, dəstəklənməsi və ləğv edilməsi imkanı olmaqla, sertifikatların və açıq açar-gizli açar cütlərinin idarə olunması üçün istifadə edilən siyasətlər, server platformaları, proqram və aparat təminatı çoxluğudur.

Python
Payfon – geniş istifadə edilən ümumi təyinatlı, yüksək səviyyəli proqramlaşdırma dili. Onun dizayn fəlsəfəsi kodun oxunaqlığını xüsusi vurğulayır, sintaksisi isə proqramçılara ideyanı C++ və ya Java dillərində olduğundan daha az sətirdə ifadə etməyə imkan verir.

Q

Quantum Key Distribution (QKD)
Açarların kvant paylanması – açar materialının optik lifli rabitə xətti ilə ötürülməsi metodu. Açar bitləri impuls lazeri tərəfindən buraxılan işıq fotonlarının paylanması ilə kodlaşdırılır. Kvant fizikasının fundamental qanunlarına görə (Heyzenberqin qeyri-müəyyənlik prinsipi) kvant sisteminin xassələrini pozmadan onun ölçülməsini aparmaq olmaz. Bunun sayəsində açar materialının gizli ələ keçirilməsini və ya aktiv müdaxiləni istisna edən etibarlı kanal formalaşdırılır.

Quantum Cryptography
Kvant kriptoqrafiyası – 1984-cü ildə *açarların kvant paylanması* sistemi ilə meydana çıxıb. Hazırda açarların kvant paylanması ilə yanaşı təhlükəsiz birbaşa kvant rabitəsi, kvant axın şifrləməsi, kvant steqanoqrafiyası, kvant açarlar infrastrukturu, kvant rəqəmsal imzası mövzularında da tədqiqatlar aparılır.

R

Rainbow series
Göy qurşağı seriyası – ABŞ Müdafiə Nazirliyi tərəfindən informasiya təhlükəsizliyi üzrə nəşr edilmiş standartlar seriyası.

Random Number Generator (RNG)
Təsadüfi ədədlər generatoru – ədədlərin əvvəlcədən bilinməyən ardıcıllığını yaratmaq üçün istifadə edilən proses. Əgər qiymətlərin tam toplusunda hər bir qiymətin seçilməsi bərabər ehtimallıdırsa, onda belə qiymətlər təsadüfi hesab edilir.

Ransomware
Verilənlərin girov götürülməsi aləti – verilənlərin girov götürülməsi üçün zərəli proqram təminatı; bu eksploytda bədniyyətli hədəf kompüterdə verilənləri şifrləyir və deşifrləmə açarını vermək üçün ödəniş tələb edir.

Recovery procedures
Bərpaetmə prosedurları − sistemin qəzadan sonra normal fəaliyyətə qaytarılması üçün əməliyyatlar ardıcıllığı.

Red team
Qırmızı komanda – şirkətin strategiyasını, məhsullarını və qəbul edilmiş anlayışlarını icazəli şəkildə sındırmağa çalışan daxili qrup.

Reference monitor concept
Müraciətlər monitoru konsepsiyası − subyektlərin obyektlərə bütün giriş cəhdlərini ayıran abstrakt maşın anlayışına əsaslanan girişə nəzarət konsepsiyası. Praktikada təhlükəsizlik nüvəsi şəklində realizə edilir.

Registration Authority (RA)
Qeydiyyat Mərkəzi (QM) – abunəçinin şəxsiyyətini müəyyən edən və Sertifikat Xidmətləri Mərkəzinə (SXM) bu haqda zəmanət verən

etibarlı subyekt. Qeydiyyat Mərkəzi SXM-in tərkib hissəsi və ya SXM-dən müstəqil ola bilər.

Remediation
Düzəliş – boşluğun və ya təhdidin aradan qaldırılması.

Remote access
Məsafədən giriş – informasiya sisteminin təhlükəsizlik perimetrinin xaricindəki istifadəçilər (və ya informasiya sistemləri) tərəfindən giriş.

Remote Access Trojan (RAT)
Məsafədən giriş troyanı – bədniyyətliyə məsafədəki serverdə proqram kodlarını icra etməyə imkan verən təklükəsizlik boşluğu.

Remote Administration Tool (RAT)
Məsafədən administrator aləti – hücum edənə hədəf kompüterdə administrator hüququ verən zərərli proqram təminatı.

Replay attack
Təkrarlama hücumu – əvvəlcədən yazılmış və ya ələ keçirilmiş məlumat kompüter sisteminə və ya şəbəkəyə hücum etmək və ya icazəsiz giriş əldə etmək üçün istifadə edilir. Məsələn, bədniyyətli səlahiyyətli şəxsin səsini yaza və sistemə girmək üçün onu təkrar səsləndirə bilər.

Repudiation
İmtina – məlumatın alınması və ya göndərilməsi faktından boyun qaçırma.

Residual data
Qalıq verilənlər – faylın və ya faylın müəyyən hissəsinin silinməsindən sonra yaddaş daşıyıcısında qalan verilənlər.

Residual risk
Qalıq risk – bütün informasiya təhlükəsizliyi tədbirləri həyata keçirildikdən sonra qalan potensial risk.

Reverse engineering
Tərs mühəndislik (rivers mühəndislik) – iş prinsipini başa düşmək məqsədilə hazır qurğunun və ya proqramın, həmçinin onlara aid olan sənədlərinin tədqiq olunmasıdır. Sənədləşdirilməmiş imkanları aşkarlamaq (o cümlədən, proqram əlfəcinlərini), dəyişiklik etmək və ya analoji funksiyalarla həmin qurğunu, proqramı və ya digər obyekti kopyalamadan təkrar yaratmaq üçün istifadə edilir.

Revoke a Certificate
Serlifikatın ləğvi – müəyyən tarixdə və vaxtda qüvvədə olan sertifikatın istismar dövrünün vaxtından əvvəl sona çatması.

Risk
Risk – konkret təhlükənin sistemin konkret boşluqlarından istifadə edə bilməsinin mümkünlüyü.

Risk analysis
Risk analizi − sistemin və onun ayrı-ayrı komponentlərinin təhlükəsizliyinə olan təhdidlərin identifikasiyası, onların xarakteristikalarının və potensial ziyanın müəyyən edilməsi və əks-tədbirlərin seçilməsi prosesi.

Root Certification Authority
Kök Sertifikat Mərkəzi – Açıq Açar İnfrastrukturunda təhlükəsizlik domeni üçün ən etibarlı məlumat mənbəyi (yəni, etibarlı yolların başlanğıcı) kimi xidmət edən Sertifikat Xidməti Mərkəzi.

Rootkit
Rutkit – zərərli proqramların sistemdə fəaliyyətini maskalamaq üçün istifadə edilən proqram və ya proqramlar toplusu. Bu topluya sistemə müdaxilənin “izlərinin silinməsi” üçün müxtəlif utilitlər,

snifferlər, skanerlər, klaviatura casusları, əməliyyat sisteminin əsas utilitlərini əvəzləyən troyan proqramları daxildir. Rutkit hakerə sındırılmış sistemdə möhkəmlənməyə və faylları, prosesləri, rutkitlərin sistemdə olmasını gizləmək yolu ilə fəaliyyətinin izlərini ört-basdır etməyə imkan verir.

RSA – həm şifrləmə, həm də rəqəmsal imza üçün istifadə edilən açıq açarlı kriptosistemdir. 1977-ci ildə Ron Rayvest (Ron Rivest), Adi Şamir (Adi Shamir) və Leonard Adleman (Leonard Adleman) tərəfindən təklif edilmişdir və müəlliflərin soyadlarının baş hərfləri ilə adlanır. RSA kriptosistemi bir neçə yüz onluq rəqəmi olan ədədlərin vuruqlara ayrılması məsələsinin hesablamaların həcmi baxımından çətinliyinə əsaslanır.

Reconnaissance

Kəşfiyyat – sonradan analiz etmək və paylaşmaq üçün düşmən qüvvələri və coğrafi mövqe xüsusiyyətləri barədə həyati əhəmiyyətli məlumatları əldə etmək məqsədilə dost qüvvələr tərəfindən tutulmuş ərazilər xaricində aparılan kəşfiyyatı bildirən hərbi termindir.

S

S^n DES
DES-in Cənubi Koreya tədqiqatçılar qrupu tərəfindən təklif edilmiş variantı. Diferensial və xətti kriptoanalizə eyni dərəcədə yaxşı dayanıqlıq məqsədilə yaradılmışdı.

Safeguards
***Təhlükəsizlik* mexanizmləri** – informasiya sistemi üçün müəyyən edilmiş təhlükəsizlik tələblərini (yəni, konfidensiallıq, tamlıq və əlyetənlik) yerinə yetirmək üçün nəzərdə tutulmuş təhlükəsizlik tədbirləri.

Salami attack
Salami hücumu – maliyyə sahəsində istifadə edilən hücumdur. Hücumun ideyası bank hesabı üçün faizlərin hesablanması zamanı kəsr rəqəmlərinin yanlış yuvarlaqlaşdırılmasından ibarətdir. Hücumun nəticəsi emal edilən hesabların sayından asılıdır. (Salami – müxtəlif növ ətdən hazırlanan italyan kolbasası növüdür.)

Salt
"Duz" – şifrləmə prosesində istifadə edilən məxfi olmayan parametr; adətən bir mərhələdəki hesablamaların nəticələrinin hücum edən tərəfindən yenidən istifadə edilə bilməməsini təmin etməyə xidmət edir.

Sandboxing
Qumqabı – tətbiqi proqram modullarının proqram təminatı ilə həyata keçirilən müxtəlif domenlərdə təcrid edilməsi üsulu.

Sanitizing
Təmizləmə – həssaslığı azaltmaq üçün sənəddən konfidensial informasiyanın silinməsi.

SANS (SysAdmin, Audit, Network, Security) Institute
SANS İnstitutu – 1989-cu ildə təhsil-tədqiqat müəssisəsi kimi yaradılmışdır, informasiya təhlükəsizliyi sahəsində mütəxəssislərin hazırlanması və sertifikatlaşdırılması ilə məşğul olur. SANS İnstitutu təhlükəsizlik məsələləri üzrə çoxsaylı informasiya və təhsil materialları hazırlayır, dəstəkləyir və pulsuz yayımlayır, mütəxəssislərin treninqi və sertifikatlaşdırılması (Global Information Assurance Certification (GIAC) Program) xidmətləri göstərir.

Scanning
Skanlama – sonrakı hücumlarda istifadə olunacaq informasiya əldə etmək üçün başqa bir sistemə paketlər və ya sorğular göndərilməsi.

Scavenging
Tullantı toplanması – giriş kodları, parollar və ya həssas verilənlər kimi faydalı məlumatları müəyyən etmək üçün zibil yeşiyinə atılmış siyahılardan, lentlərdən və başqa informasiya saxlama qurğularından istifadə edilməsi.

Scrambler
Skrembler – rabitə kanalları ilə ötürülən səs informasiyasının şifrlənməsini həyata keçirən qurğu.

Script kiddie və ya **skiddie** (*skid, script bunny, script kitty* kimi də işlədilir)
Skript "körpələri" – kompüter sistemlərinə və şəbəkələrinə hücum etmək, veb-səhifələri difeys etmək üçün başqaları tərəfindən hazırlanmış skriptlərdən və proqramlardan istifadə edən şəxslər.

Secret Key
Məxfi açar – məxfi açarlı (simmetrik) kriptoqrafik alqoritmlərdə istifadə edilən kriptoqrafik açar.

Secret Sharing Scheme
Sirr bölgüsü sxemi – 1979-cu ildə Blekli (Blakley) və A.Şamir (A. Shamir) tərəfindən təklif edilmişdir. Sxemin əsas ideyası məxfi açarı bir neçə subyekt arasında elə bölməkdir ki, onlar bir neçə hissədən açarı bərpa edə bilsin (*n* yerə bölünübsə, *m*<*n* hissədən).

Sector alignment
Sektor düzləndirilməsi – diskin qadağan olunmuş nüsxə olub-olmadığını sektorların cığırlar üzrə düzgün yerləşdirildiyini yoxlamaqla təyin edilən surətçıxarma əleyhinə qorunma üsulu.

Secure domain
Təhlükəsizlik domeni – subyektlər, onların informasiya obyektləri və ümumi təhlükəsizlik siyasəti çoxluğu.

Secure Electronic Transaction (SET)
Təhlükəsiz elektron tranzaksiya **–** ödənişləri açıq şəbəkələr vasitəsilə həyata keçirən kart ödəniş sistemlərində tranzakiyaların təhlükəsizliyi üçün texniki spesifikasiya. SET spesifikasiyası Visa və Master Card şirkətləri tərəfindən IBM, Microsoft, Netscape, SAIT, GTE, Terisa System və Verisign kimi şirkətlərin dəstəyi ilə işlənmişdir. Bu spesifikasiya SET-ə uyğun proqram təminatının işlənməsi zamanı istifadə üçün açıqdır. Simmetrik şifrələmə üçün DES şifri, asimetrik şifrələmə və rəqəmsal imza üçün RSA sistemi, heş-funksiya üçün SHA-1 istifadə edilir. Sertifikatlar X.509 V3 standartına uyğundur.

Security Content Automation Protocol (SCAP)
Təhlükəsizlik kontentinin avtomatlaşdırılması protokolu – boşluqların təsviri formatını standartlaşdırmağa, təhlükəsizlik konfiqurasiyaların idarə edilməsi prosesini avtomatlaşdırmağa, istifadəçilərlə təhlükəsizlik vasitələrinin istehsalçıları arasında informasiya mübadiləsini təmin etməyə xidmət edir. NİST tərəfindən işlənmişdir.

Security Information and Event Management (SIEM)
İnformasiya təhlükəsizliyi məlumatlarının və hadisələrinin idarə edilməsi – proqram təminatının tətbiq sahəsini bildirən iki terminin birləşməsidir: *SIM – Security information management –* təhlükəsizlik informasiyasının idarə edilməsi və *SEM – Security event management –* təhlükəsizlik hadisələrinin idarə edilməsi. SIEM texnologiyası şəbəkə qurğularından, informasiya təhlükəsizliyi vasitələrindən, tətbiqi proqramlardan daxil olan informasiya təhlükəsizliyi hadisələrinin analizini təmin edir.

Secure Hash Algorithm (SHA-1)
SHA-1 ("şa-bir" kimi oxunur) **–** təhlükəsiz heş alqoritmi. 1995-ci ildə ABŞ standartı kimi işlənmişdir, FIPS 180-1 standartında təsvir edilir, heşin uzunluğu 160 bitdir. 2002-ci ildə SHA-2 heş alqoritmlər ailəsi işlənmişdi (FIPS 180-2). Hazırda heş alqoritmlər sahəsində ABŞ standartı kimi SHA-3 qəbul olunub.

SSH (Secure Shell) protocol
Təhlükəsiz örtük protokolu – sistemə və şəbəkə servislərinə məsafədən təhlükəsiz girişi təmin edən protokol. Telnet, rsh, rcmd və rlogin protokollarını əvəz edə bilər. SSH faylların şifrlənmiş kanalla təhlükəsiz ötürülməsini də təmin edə bilir.

Secure Socket Layer (SSL)
Təhlükəsiz soket səviyyəsi – İnternet vasitəsilə məxfi sənədləri ötürmək üçün Netscape tərəfindən yaradılmış protokol. SSL ilə ötürülən məlumatları şifrləmək üçün açıq açardan istifadə edilir.

Secure state
Təhlükəsiz vəziyyət − yerinə yetirilməsi zamanı malik olduğu səlahiyyətləri yoxlamaqdan başqa digər yolla heç bir subyektin heç bir obyektə giriş ala bilmədiyi şərt.

Security filter
Təhlükəsizlik süzgəci – sistemdən keçən verilənlərə aid təhlükəsizlik siyasətini gerçəkləşdirən etibarlı kompüter sistemi.

Security flaw
Təhlükəsizlik çatı − səlahiyyətlərin təyin edilməsi və ya sistemin mühafizə vasitələrinin yaradılması, reallaşdırılması və ya idarə edilməsi zamanı buraxılan səhv, təhlükəsizliyin pozulmasına gətirib çıxara bilər.

Security kernel
Təhlükəsizlik nüvəsi – Etibarlı Hesablama Bazasında müraciətlər monitoru konsepsiyasını həyata keçirən proqram və aparat elementləri. Onlar subyektlərin obyektlərə bütün giriş cəhdlərini ayırmalı, dəyişdırılməkdən mühafizə olunmalı və öz funksiyalarını düzgün yerinə yetirmələri yoxlanılmalıdır.

Security level
Təhlükəsizlik səviyyəsi − informasiyanın kritiklik səviyyəsini göstərən iyerarxik təsnifatın (giriş səviyyəsi) və qeyri-iyerarxik kateqoriyaların kombinasiyası.

Security metrics
Təhlükəsizlik metrikaları **–** informasiya təhlükəsizliyi üzrə faəliyyətin qiymətləndirilməsi ilə əlaqəli relevant verilənlərin toplanması, analizi və hesabat verilməsi yolu ilə qərar qəbul edilməsini asanlaşdırmaq, faəliyyətin məhsuldarlığını və hesabatlılığı yaxşılaşdırmaq üçün nəzərdə tutulmuş alətlərdir. Sadə yanaşmada, metrikalar təhlükəsizliyi ölçmək, xüsusilə təşkilatın təhlükəsizlik səviyyəsini ölçmək üçün standartdır.
İnformasiya təhlükəsizliyinin səviyyəsini qiymətləndirmək üçün əsasən üç termin istifadə edilir: ölçmə (ing. *measurement*), göstəricilər (ing. *measures*) və təhlükəsizlik metrikaları (ing. *security metrics*). Onlar çox zaman sinonim kimi şlədilir (xüsusilə ikinci və üçüncü), çünki fəaliyyətdə olan sistemlərdən emal edilməmiş informasiyanın (ing. *raw data*) bilavasitə toplanması zamanı alınırlar. Lakin bu terminlərin mənaları müxtəlifdir, emal edilməmiş informasiyanın toplanması və analizi zamanı müxtəlif hərəkətlər yerinə yetirilir. Təhlükəsizlik metrikası göstəricinin

kəmiyyət qiymətlərini almaq üçün ölçülən sistemin bir və ya bir neçə obyektinə ölçmə metodunun tətbiqinin nəticəsidir.

Security Operations Center (SOC)
Təhlükəsizlik Əməliyyatları Mərkəzi – təşkilati və texniki səviyyədə təhlükəsizlik məsələləri ilə məşğul olan mərkəzləşləşdirilmiş bölmə.

Security policy
Təhlükəsizlik siyasəti − əsasında kritik informasiyanın idarə edilməsinin, yayılmasının və mühafizəsinin qurulduğu qanunlar, qaydalar və praktiki təcrübələr.

Security policy model
Təhlükəsizlik siyasəti modeli − sistem üçün işlənmiş təhlükəsizlik siyasətinin formal təsviri. Bu modeldə kritik informasiyanın idarə edilməsini, yayılmasını və mühafizəsini müəyyən edən formal təsvirlər verilməlidir.

Security posture
Təhlükəsizlik duruşu **–** daxili və xarici təhdidlərə ünvanlanan texniki və qeyri-texniki elementləri (siyasət, prosedurlar və nəzarət kimi) əhatə edir.

Sensitive information
Kritik informasiya − itirilməsi, qeyri-düzgün istifadəsi, modifikasiyası və ya açılması milli maraqlara ziyan vura bilən və ya milli proqramların yerinə yetirilməsinə mane ola bilən və ya ayrıca şəxslərin maraqlarına ziyan vura bilən, lakin bununla belə milli müdafiə və ya xarici siyasət maraqlarına toxunmayan istənilən informasiya. Kommersiya sektorunda kritik informasiya anlayışı analoji daxil edilir − itirilməsi, qeyri-düzgün istifadəsi, modifikasiyası və ya açılması şirkətin və ya digər təşkilatın maraqlarına maddi və ya qeyri-maddi (mənəvi ziyan) formada ziyan vura bilən informasiya.

Separation of duties
Vəzifələrin bölünməsi – kritik informasiya üçün məsuliyyətin elə bölünməsidir ki, ayrılıqda fəaliyyət göstərən fərd verilənlərin emalı sisteminin yalnız məhdud hissəsinin təhlükəsizliyini risk altına sala bilsin.

S-HTTP (Secure HTTP)
Təhlükəsiz HTTP – HTTP protokolunun genişləndirilmiş variantı, veb-serverlə veb-brauzer arasında ötürülən verilənlərin şifrlənməsini, həmçinin serverin və kliyentin autentifikasiyasını təmin edir. 1999-cu ildə RFC 2660 kimi nəşr olunmuşdu. Microsoft və Netscape kimi veb-brauzer istehsalçıları HTTPS-i dəstəklədiklərindən S-HTTP geniş yayılmamışdır.
S-HTTP yalnız ötürülən səhifədəki verilənləri və POST sahəsindəki verilənləri şifrləyir, lakin ilkin protokola dəyişiklıik etmir. Bunun sayəsində, S-HTTP protokolu HTTP ilə paralel işləyə və eyni portdan istifadə edə bilir, çünki paketin şifrlənməyən başlığı ötürülən verilənlərin tipini (şifrlənmiş və şifrlənməmiş) müəyyən edir.

Situational awareness
Situasiyadan məlumatlılıq – zaman və məkan çərçivəsində müəssisənin təhlükəsizlik duruşunun və təhdidlər mühitinin başa düşülməsi.

Skimminq
Skimming – tanış olmayan, baxılan anda verilənləri öz xoşuna təqdim etməyən son istifadəçidən məlumatın əldə edilməsi.

Skipjack
Clipper çipində realizə edilmiş şifrələmə alqoritmi. 64-bitlik blokların şifrələnməsi üçün 80 bitlik açar istifadə edilir. Şifrələmə raundlarının sayı 32-dir. DES alqoritmindən daha etibarlı olduğu iddia edilir.
Alqoritmin nəşr olunmaması və məxfi saxlanması çox tənqid edilmişdir. Hesab edilir ki, alqoritmdə qəsdən buraxılmış boşluqlar

və ya xüsusi lağımlar ola bilər. Bu alqoritmin digər nöqsanı – yalnız hökumətin müəyyən etdiyi avadanlıqlarda realizə edilə bilməsidir.

SMiShing
SMS-fişinq və ya smişinq (“SMS” və “fişinq” sözündən yaranıb) **–** SMS vasitəsilə fişinq.

Sneakernet
Daşınar şəbəkə **–** informasiyanın kompüter şəbəkəsi ilə ötürülməsi əvəzinə, yaddaş vasitələrini (maqnit lentləri, diskləri, CD-ləri, USB flaş-kartları və s.) və ya xarici tərpənməz diskləri bir kompüterdən digərinə daşımaqla elektron məlumatların, xüsusilə də, kompüter fayllarının ötürülməsini təsvir edən qeyri-formal termin.

Snooping
Gizli izləmə **–** bədniyyətlini maraqlandıran informasiyanı tapmaq üçün fayllara və sənədlərə baxılması.

Social engineering
Sosial mühəndislik – bir şəxsi aldadaraq onu sistemə və ya şəbəkəyə hücum üçün istifadə edilə bilən informasiyanı (məsələn, parolu) verməyə təhrik etmək üsulları.

Software piracy
Proqram təminatı piratçılığı – proqram təminatı məhsullarının səlahiyyət olmadan istifadəsi, surətinin çıxarılması və ya yayılması.

Spam
Spam – elektron məktubların anonim, tələb edilməmiş kütləvi göndərilməsi.
Spam ingiliscə “SPices hAM” birləşməsindən yaranmışdır – bibərli vetçina deməkdir (spam – keçən əsrin 20-30-cu illərində çox məşhur olan ət konservlərinin adıdır). Bu termin Hormel şirkəti tərəfindən icad edilmiş və ticarət markası kimi qeydiyyatdan keçirilmişdi, 1930-cu illərdə şirkətdə olduqca böyük həcmdə

satılmayan köhnə ət yığılıb qalmışdı. 1937-ci ildə şirkət yığılıb qalmış ətin satışı üzrə marketinq kampaniyasına başlamışdı.

Spambot
***Spambot* –** spam göndərilməsinə kömək etmək üçün nəzərdə tutulmuş avtomatlaşdırılmış kompüter proqramı

Spear phishing
Nizəli fişinq – xüsusi bir təşkilatı hədəf götürərək, onun konfidensial məlumatlarına icazəsiz giriş yolu axtaran saxta e-poçt vasitəsilə dələduzluq cəhdi

Spillage of classified information
Konfidensial informasiya sızıntısı – aşağı konfidensiallıq səviyyəsində olan sistemlərin yüksək konfidensiallıq sinfindən olan informasiya ilə çirklənməsi.

SPIM (SPam through Instant Messaging)
***Ani ismarıclarla spam* –** e-poçt məktubları ilə deyil, ani ismarıc vasitəsilə çatdırılan spam.

Spiral track
Spiralvari cığır – kopyalamadan mühafizə metodunun bir hissəsi kimi diskə yazılan spiral şəkilli cığır.

SPIT (**SPam over Internet Telephony**)
Internet telefon üzərindən spam – IP üzərindən səs vasitəsilə yayımlanan arzuolunmaz reklam.

Spoofing
Aldatma – "IP spoofing" həqiqi mənbədən deyil, başqa bir mənbədən şəbəkə paketi göndərilməsini bildirir.

Spoofing URL
***Saxta URL* –** başqa bir veb-səhifə kimi təqdim edilən veb-səhifə. Burada bəzən veb-brauzer texnologiyasındakı səhvləri istismar

edərək zərərli kompüter hücumlarına imkan verən mexanizmlər istifadə edilir.

Spyware
Casus proqramlar – adamlar və ya təşkilatlar haqqında onların xəbəri olmadan informasiya toplamaq üçün informasiya sisteminə gizli daxil edilən zərərli proqram təminatı.

SQL injection
SQL inyeksiyası– verilənlərlə işləyən tətbiqi proqramlara hücum etmək üçün istiufadə edilən kod inyeksiyası üsulu; icra ediləcək zərərli SQL operatorları giriş sahəsinə daxil edilir (məsələn, verilənlər bazasının məzmununu hücum edənə yönləndirmə).

Stack mashing
Stek püresi– buferin daşmasından istifadə etməklə kompüteri ixtiyari kodu icra etməyə məcburetmə üsulu.

Steganography
Steqanoqrafiya (στεγανός– gizli + γράφω – yazıram) – ötürülmə faktının gizlədilməsi yolu ilə informasiyanın ötürülməsi üsulları.

Stream cipher
Axın şifri – kriptoqrafik çevirmə zamanı açıq mətn simvollara və ya bitlərə bölünür və hər bir simvol açar axını simvoluna uyğun seçilmiş çevirmə ilə şifrlənir. Blok şifrlərindən fərqli olaraq axın şifrlərində səhv yayılmır və ya yayılma məhdud olur.

Structured Threat Information eXpression (STIX)
Təhdid məlumatlarının strukturlaşdırılmış təsviri – kiber-təhdid məlumatlarının strukturlaşdırılmış təsviri üçün XML əsasında dil.

Subject
Subyekt − sistemin aktiv komponentidir, adətən obyektdən obyektə informasiya axınının və ya sistemin vəziyyətinin dəyişməsinin səbəbi ola bilən istifadəçi, proses və ya qurğu kimi təsvir edilir.

Supersector
Supersektor – kopyalamadan mühafizə metodunun bir hissəsi kimi diskə yazılan çox böyük ölçülü cığır.

Symmetric key
Simmetrik açar – kriptoqrafik əməliyyatı və onun tərsini yerinə yetirmək, məsələn, şifrləmək və deşifrləmək (və ya məlumatın autentifikasiya kodunu yaratmaq və kodu yoxlamaq) üçün istifadə olunan kriptoqrafik açar.

System integrity
Sistemin tamlığı − bütün funksiyalarını düzgün yerinə yetirdikdə və qəsdli və ya təsadüfi manipulyasiyalardan azad olduqda sistemin malik olduğu keyfiyyəti.

T

TACACS+
TACACS+ – məsafədən autentifikasiya protokolu. Cisco Systems şirkəti tərəfindən əlavə təhlükəsizlik tədbirlərini, o cümlədən şəbəkə komunikasiyalarının mühafizəsini (parolların ələ keçirilməsinin qarşısının alınması), girişə nəzarətin təkmilləşdirilməsini və qeydiyyat aparılmasını dəstəkləyir.

Tailoring
Xüsusi uyğunlaşdırma – baza təhlükəsizlik tədbirlərinin redaktə olunması üçün əsas götürülən proses: (i) əhatəli proqramın tətbiqi; (ii) lazım olduqda əvəzləyici təhlükəsizlik tədbirlərinin dəqiqləşdirilməsi; və (iii) aydın təyinat və seçilmə bəyənatlar vasitəsilə təhlükəsizlik tədbirlərində təşkilatın müəyyən etdiyi parametrlərin dəqiqləşdirilməsi.

Tampering
Manipulyasiya – sistemin, onun nəzərdə tutulmuş davranışının və ya verilənlərin qəsdən dəyişdirilməsi.

Targeted threats
Hədəfəyönəlik təhdidlər – xüsusi seçilmiş təşkilat və ya sənaye sahəsi üçün nəzərdə tutulmuş zərərli proqram təminatı sinfi.

TEMPEST (Transient Electromagnetic Pulse Emanation Standard)
Elektrik və elektron avadanlığın şüalandırdığı əlavə elektromaqnit siqnalların öyrənilməsi və analizi üzrə standart. TEMPEST ixtisarı 1960-cı illərin sonu 1970-ci illərin əvvəlində ABŞ Müdafiə Nazirliyində elektron avadanlıqda müxtəlif növ əlavə şüalanmalar vasitəsilə informasiya sızmasının qarşısının alınması metodlarının işlənməsi iüzrə məxfi proqramın adı kimi meydana çıxmışdı. Rusiyada “ПЭМИН (Побочные ЭлектроМагнитные Излучения и Наводки” – əlavə elektromaqnit şüalanmaları və sızmalar),

Avropa və Kanadada “Compromising emanation” (sızma şüalanmaları) termini işlədilir.

Terminal Access Control Access System (TACACS)
Məsafədən autentifikasiya protkolu – BBN Planer İnternet-provayder firması tərəfindən yaradılmış və Cisco Systems şirkəti tərəfindən istifadə edilmişdir. Hazırda IETF tərəfindən standart kimi qəbul edilmiş yeganə standartdır. Məsafədəki istifadəçinin adını və parolunu yoxlamağa imkan verir.

Testbed
Sınaq modeli – əsas təyinatı digər sistemlərin test edilməsi üçün baza yaratmaq olan istənilən sistem. Sınaq modelləri müəyyən proqramlaşdırma dili və realizə metodu üçün, əksər hallarda isə müəyyən tətbiqi məsələlər üçün yaradılır.

Threat
Təhdid − sistemə verilənlərin məhv edilməsi, açıqlanması və ya dəyişdirilməsi və/və ya xidmətdən imtina şəklində ziyan vurulmasına səbəbi ola bilən istənilən hal və ya hadisə.

Time bomb
Vaxt bombası – öncədən müəyyənləşdirilən vaxtda aktivləşdirilən məntiqi bomba.

TLS (Transport Layer Security)
Nəqliyyat səviyyəsinin təhlükəsizliyi – verilənlərin İnternet şəbəkəsində qovşaqlar arasında təhlükəsiz ötürülməsini təmin edən kriptoqrafik protokollar (SSL-i əvəzləyir). TLS və SSL autentifikasiya üçün asimmetrik kriptoqrafiyadan, konfidensiallıq üçün simmetrik şifrləmədən və məlumatların tamlığına nəzarət üçün məlumatı autentifikasiya kodundan istifadə edir.

To Archive
Arxivləşdirmək – ehtiyat nüsxə fayllarını və digər əlaqəli jurnalları konkret zaman müddəti üçün saxlamaq.

Tor (**The Onion Router**)
Tor (The Onion Router-in qısaltması) **–** onlayn anonimliyi təmin etmək və onlayn senzuraya qarşı müqavimət göstərmək üçün istifadə edilən pulsuz proqram təminatı.

To Scavenge
Təmizləmək – həqiqiliyi yoxlanmadan qalıq verilənlərdən mühüm informasiya əldə etmək üçün axtarış aparmaq.

To Spoof
Aldatmaq – istifadəçini, mütəxəssisi (məsələn, dinləmə operatorunu) və ya resursu aldatmaq və ya çaşdırmaq niyyəti ilə tədbir görmək.

To Tailgate
Yaxından təqib etmək – nəzarət edilən giriş vasitəsilə səlahiyyətli şəxsi müşayiət etməklə səlahiyyət olmadan fiziki giriş əldə etmək.

Traffic analysis
Trafikin analizi – trafik axınını müşahidə etməklə informasiyanın çıxarılması.

Traffic Light Protocol (TLP)
Svetofor protokolu – informasiya təhlükəsizliyi insidenti haqqında konfidensial informasiyanın yayılma auditoriyasını göstərmək üçün işarə sistemi. İnformasiya dörd rəngdən biri ilə işarələnir:
Qırmızı – olduqca konfidensial informasiya, informasiyanın hazırlanması prosesinin iştirakçılarından başqa heç bir əməkdaş və ya qurum arasında yayıla bilməz. İnformasiyanın paylaşılması üçün bütün iştirakçıların imzası tələb olunur.
Sarı – məhdud yayılma, paylaşılması lazım olduqda informasiyanı alan şəxs yalnız öz təşkilatı daxilində paylaşa bilər.
Yaşıl – geniş yayılma, müəyyən icma daxilində geniş yayıla bilər, lakin KİV-də nəşr oluna bilməz.

Ağ – qeyri-məhdud yayılma, müəlliflik hüququ qorunmaqla yayılması sərbəstdir.

Traffic padding
Trafikin doldurulması – trafikin analizini və deşifrlənməsini daha da çətinləşdirmək üçün ötürmə kanallarında saxta verilənlər generasiya edən əks-tədbir.

Tranquility
Sakitlik – informasiya sistemi ilə emal olunduğu zaman obyektin təhlükəsizlik səviyyəsinin dəyişə bilməməsi xassəsi.

Trapdoor
"Arxa qapı" – adətən testetmə və nasazlığın aradan qaldırılması üçün yaradılan, kompüter təhlükəsizliyini "aldatmaq" üçün istifadə edilə bilən gizli proqram təminatı və ya aparat mexanizmi.

Triple DES
Üçqat DES – DES şifrinin variantıdır, açıq mətn üç dəfə şifrələmə prosesindən keçir. Bu alqoritmin bir neçə istifadə rejimi var: DES-EEE2, DES-EDE3, DES-EEE2, DES-EDE2. Bu rejimlərdə iki və ya üç müxtəlif açar istifadə edilə bilər.

Trollinq
Trollinq – oxucuları emosional cavablara təhrik etmək və ya mövzu ətrafında normal müzakirələri pozmaq niyyəti ilə onlayn cəmiyyətlərdə (xəbər qrupları, forum, çat otaqları və ya bloqlar) təhrikedici, mövzudan kənar statuslar yerləşdirərək provakasiya yaradılması.

Trojan horse
Troya atı, troyan – funksiyaları baxımından faydalı proqram kimi görünən zərərli proqramlardır. Troyanlar işə düşdükdə elan edilmiş faydalı funksiyalarla yanaşı verilənlərin icazəsiz toplanması,

saxtalaşdırılması və ya məhv edilməsi kimi elan olunmamış funksiyaları da yerinə yetirirlər.

Trusted Automated Exchange of Indicator Information (TAXII)
Kiber-təhdid məlumatlarının avtomatlaşdırılmış etibarlı mübadiləsi – kiber-təhdid məlumatlarının mübadiləsi üçün spesifikasiyalar toplusu; təşkilatların kiber-təhdid məlumatlarını öz tərfədaşları ilə paylaşmasını asanlaşdırmağa xidmət edir.

Trusted Computing Base (**TCB)**
Etibarlı Hesablama Bazası **(*EHB*)** − hesablama sisteminin təhlükəsizlik siyasətinin dəstəklənməsi üçün cavabdeh olan proqram və aparat komponentləri daxil olmaqla təhlükəsizlik mexanizmləri. EHB bir və ya bir neçə komponentdən ibarətdir, onlar birlikdə sistem çərçivəsində vahid təhlükəsizlik siyasətinin həyata keçirilməsinə cavabdehdirlər. EHB-nin vahid təhlükəsizlik siyasətini düzgün həyata keçirməsi xassəsi ilk növbədə EHB-nin özünün mexanizmlərindən, həmçinin sistem inzibatçılığının düzgün idarə etməsindən asılıdır.

Trusted path
Etibarlı marşrut − terminal arxasındakı istifadəçinin EHB ilə bilavasitə qarşılıqlı əlaqədə olmasına kömək edən mexanizm. O yalnız istifadəçi və ya EHB tərəfindən aktivləşdirilə bilər, onun işi şübhəli proqram təminatı tərəfindən dayandırıla, təqlid edilə və ya pozula bilməz.

Trusted software
Etibarlı proqram təminatı − ***Etibarlı Hesablama Bazasına*** daxil olan proqram təminatı.

Trustworthy computing (TwC)
Etibarlı hesablama – təhlükəsiz, əlyetər və etibarlı olan hesablama sistemlərini bildirir.

U

User ID (user identification)
İstifadəçinin identifikasiya kodu – verilənlərin emalı sistemi tərəfindən istifadəçini identifikasiya etmək üçün istifadə edilən simvol sətri və ya şablon.

User profile
İstifadəçi profili – 1) Adətən, girişə nəzarət üçün istifadə edilən istifadəçi təsviri. İstifadəçi profilinə istifadəçinin identifikasiya kodu, istifadəçi adı, parol, müraciət hüquqları və digər atributlar daxil ola bilər.
2) Fəaliyyətindəki dəyişiklikləri aşkarlamaq üçün istifadə edilə bilən istifadəçi fəaliyyətinin şablonu.

V

Verification
Verifikasiya − sistemin spesifikasiyalarının iki səviyyəsinin onlar arasında zəruri uyğunluğu sübut etmək üçün qarşılaşdırılması prosesi (məsələn, təhlükəsizlik siyasəti modelinin və sistemin spesifikasiyalarının; sistemin spesifikasiyalarının və ilkin kodların; ilkin kodların və yerinə yetirilən kodların və s.). Bu proses tamamilə və qismən avtomatlaşdırıla bilər.

Virtual Private Network (VPN)
***Virtual xüsusi şəbəkə* (*VXŞ*)** – məxfi verilənlərin açıq rabitə kanalları ilə ötürülməsi üçün təhlükəsiz virtual şəbəkə yaratmağa imkan verən texnologiya**.** Bu texnologiyanın əsas xüsusiyyəti korporativ IP-trafikin ötürülməsi üçün Internet şəbəkəsinin magistral kimi istifadə edilməsidir. VXŞ-lər istifadəçinin məsafədə yerləşən şəbəkəyə qoşulması və bir neçə lokal şəbəkənin birləşdirilməsi məsələlərinin həlli üçün nəzərdə tutulmuşdur.

Virus
Virus – özünün mümkün dəyişdirilmiş surətini daxil etmək üçün digər proqramları modifikasiya etməklə özünü yayan və yoluxmuş proqramın aktivləşməsi zamanı icra edilən proqram.

Virus hoax
Virus uydurması – mövcud olmayan virus haqqında təcili xəbərdarlıq məlumatı.

Virus signature
Virus siqnaturası – konkret virusun hər bir surəti üçün ümumi olan və virusu aşkarlamaq üçün antivirus proqramında istifadə edilə bilən unikal proqram kodları.

Vishing
Vişinq – IP protokolu üzərindən səs (VoIP) vasitəsilə məlumatlara icazəsiz giriş.

Vulnerability

Boşluq − sistem təhlükəsizlik vasitələrində zəiflik, sistemin layihəsində, yaradılmasında, prosedurlarında və daxili nəzarətində səhvlər və ya zəifliklər nəticəsində meydana çıxır və sistemin təhlükəsizlik siyasətinin pozulması üçün istifadə edilə bilər.

W

WAF (Web Application Firewall)
Tətbiqi veb proqram ekranı – müraciətlər HTTP və HTTPS ilə həyata keçirilən tətbiqi proqramlara mümkün hücumlardan qorunmaq üçün nəzərdə tutulmuşdur.

WAP (Wireless Application Protocol)
Simsiz tətbiqi proqram protokolu – mobil telefonları, peycerləri və başqa daşınan qurğuları e-poçt və mətn əsaslı veb-səhifələrə təhlükəsiz giriş ilə təmin etmək üçün standart.

Warchalking
Wi-Fi reklamı (“vay-fay” kimi oxunur) – açıq Wi-Fi şəbəkəsini reklam etmək məqsədilə ictimai yerlərdə simvolların çəkilməsi.

War dialing or **wardialing**
“Döyüş zəngləri” – kompüterləri axtarmaq üçün modem qurğusundan istifadə edərək, adətən yerli kod ilə hər bir nömrəni yığmaqla, siyahıdakı telefon nömrələrini avtomatik araşdıran üsul.

Wardriving
Simsiz şəbəkə axtarışı – hərəkət edən nəqliyyatda olan şəxs tərəfindən portativ kompüterdən, smartfon və ya fərdi rəqəmsal köməkçidən (PDA) istifadə edilərək Wi-Fi simsiz şəbəkələrinin axtarılması.

Warez
Varez – kopyalamadan mühafizə vasitələrinin hamısı söndürülmüş, qeyri-qanuni kopyalanan və yayılan kommersiya proqram təminatını bildirmək üçün hakerlər tərəfindən geniş istifadə edilən termin.

Waterhole
Su çuxuru – hücum üsuludur; hədəf sistemlərin gedə biləcəyi ehtimallı olan veb-səhifələrin ələ keçirilərək əlaqədar

səhifəyə iFrame qoymaq yolu ilə, səhifəyə girməsi gözlənilən hədəf sistemlərdəki boşluğun istismar edilməsi ilə sistemə sızmaq üsuludur.

Weak bit
Zəif bit – sıfır və ya bir kimi şərh oluna bilən zəif maqnit sahəsi ilə diskə bilərəkdən yazılan və kopyalama əleyhinə qorunma metodunun bir hissəsi kimi yazılan bit.

Web Bug
Veb-böcək – veb-saytlarda xüsusi üsulla yerləşdirilən, istifadəçiyə görünməyən kiçik təsvirlər, onlar üçüncü şəxsə web-serverlərin istifadəsini izləməyəvə istifadəçi haqqında İP-ünvan, host adı, brauzerin tipi və versiyası, əməliyyat sisteminin adı və versiyası, veb-brauzer cookie-si daxil olmaqla informasiya toplamağa imkanı verir.

Web jacking
Veb jacking – sosial mühəndislik hücumlarında istifadə edilə bilən fişinq üsulu.

Website defacement
Veb-sayt üzlüyünün eybəcərləşdirilməsi – veb-saytın və ya veb-səhifənin vizual görünüşünü dəyişən veb-sayt hücumu.

WEP (Wired Equivalent Privacy)
Naqilli şəbəkəyəyə ekvivalent məxfilik – 802.11b standartında simsiz lokal şəbəkələr (Wireless LAN, WLAN) üçün müəyyən etdilmiş təhlükəsizlik protokolu.

Whackers
Vi-hakerlər – simsiz şəbəkə hakerləri. Simsiz şəbəkə hakerləri öz fəaliyyətlərinə haqq qazandırmaq üçün icazəsiz giriş imkanlarından cinayət əməlləri törətməkdə istifadə etmədiklərini iddia edirlər, bu bəzi hallarda doğrudur. Lakin bəzi Qara Şlyapa vi-hakerləri

“**warspamming**” ilə məşğuldurlar – qorumasız şəbəkənin Simple Mail Transfer Protocol (SMTP) şlüzündən istifadə edərək spam göndərirlər. Digər Qara Şlyapa vi-hakerləri isə telekommunikasiya oğurluğu ilə məşğuldurlar.

Whaling
Balina ovu – “fişinq” və ya “nizəli fişinqin” xüsusi formasıdır. Özəl şirkətlərdə yuxarı səviyyə rəhbərlərinin hədəfə alındığını nəzərdə tutur.

White Hats or Ethical Hackers or Samurai Hackers
Ağ şlyapalar və ya etik hakerlər və ya samuray hakerlər – yaradıcı kompüter bacarıqlarından zərərli məqsədlər üçün deyil, cəmiyyətin faydası üçün istifadə edən hakerlər. Məsələn, 1990-cı illərin ortalarında haker cəmiyyətinin Kiber Mələklər kimi tanınan anti-kriminal istiqaməti meydana çıxmışdı. O vaxtdan bəri Kiber Mələklər gündə 24 saat, həftədə yeddi gün ümumdünya hörümçəyini skanlayaraq uşaq pornoqrafiyasına və kiber-təqibə qarşı mübarizə aparırlar. Haker cəmiyyətində başqa Ağ Şlyapa nişanları da geniş yayılmışdır. Məsələn, Ağ Şlyapa Etikası ilə yaşayan elit hakerlər məlumatı qəsdən məhv etməməyə, kompüter sistemlərinə və ya şəbəkələrə ziyan vurmamağa çalışırlar.

White team
Ağ komanda – informasiya təhlükəsizliyi sistemini sındırmağa çalışan *Qırmızı komanda* ilə sistemi müdafi edənlərin *Mavi komandası* arasında mübarizədə hakimliyi həyata keçirən qrup.

Wide track
Geniş cığır – surətçıxarma əleyhinə qorunma metodunun bir hissəsi kimi, eyni verilənlərin yazıldığı diskdə iki və ya daha çox qonşu cığırlar dəsti.

Windowing system (**window system**)
Pəncərə sistemi – qrafiki istifadəçi interfeysi (graphical user interface, GUI) üçün WIMP (windows, icons, menus, pointer –

pəncərələr, ikonlar, menyular, maus işarələri) paradiqmasını reallaşdıran qrafik istifadəçi interfeysinin bir növü.

Wiretapping
Gizli dinləmə – xəttə xüsusi qurğu qoşmaqla telefon danışıqlarına gizli qulaq asılması; verilənləri əldə etmək, dəyişdirmək və ya daxil etmək üçün məlumat kanalının müəyyən hissəsinə gizli qoşulma.

Worms
Soxulcanlar – müstəqil, yəni başqa proqramlara yeridilmədən öz surətlərini kompüter sistemlərində yaymağa və onları işə salmağa qabil olan proqramlardır (virusun aktivləşməsi üçün yoluxmuş proqramın işə salınması tələb olunur). Soxulcanların sel kimi yayılması rabitə kanallarının, yaddaşın həddən artıq yüklənməsinə və son nəticədə sistemin çökməsinə gətirib çıxarır..

WPA (Wi-Fi Protected Access)
Təhlükəsiz Wi-Fi girişi – WEP protokolunun kriptoqrafik dözümlə əlaqəli bir neçə vacib probleminin həlli üçün 2003-cü ildə standart kimi təklif edilib. Əsas xüsusiyyəti şifrləmə açarlarının TKIP (Temporal Key Integrity Protocol) protokolu bazasında dinamik generasiyası texnologiyasıdır. Bundan başqa, WPA-da kriptoqrafik nəzarət cəmləri MIC (Message Integrity Code – məlumatın tamlıq kodu) adlı yeni metod ilə hesablanır və AES standartı ilə şifrləmə də dəstəklənir.

X

X.509
X.500 kataloqlar xidməti üçün autentifikasiya mexanizmini təsvir edən ITU-T tövsiyələridir. Autentifikasiya prosesi həm məxfi açarlı, həm də açıq açarlı kriptosistemlərə əsaslana bilər. Açıq açarlı kriptosistemlərdə autentifikasiya rəqəmsal sertifikatlara əsaslanır. X.509 daha çox rəqəmsal sertifikatların formatını təsvir edən sənəd kimi məşhurdur. Birinci versiyası 1988-ci ildə, geniş yayılan üçüncü versiyası isə 1995-ci ildə nəşr edilmişdir.
X.509 standartını PEM, PKCS, S-HTTP və SSL daxil olmaqla bir çox protokol dəstəkləyir.

X-Force
ISS (Internet Security Systems) şirkətində informasiya təhlükəsizliyi sahəsində ekspertləri birləşdirən elmi-tədqiqat qrupu. ISS şirkətini 1994-cü ildə CERT/CC koordinasiya mərkəzinin təşkilatçılardan biri olan Kristofr Klaus yaratmışdı. X-Force qrupu aparat və proqram vasitələrinin test edilməsini həyata keçirir və bu tədqiqtların nəticələri boşluqlar və təhdidlər bazasında yerləşdirilir (ISS X-Force Threat and Vulnerability Database).

XOR (e**X**clusive **OR**)
Istina edən VƏ YA – bitlər cütü üzərində aparılan riyazi əməl: 0+1=1, 1+0=1, 0+0=0, 1+1=0. Bitlər eyni olduqda nəticə 0, müxtəlif olduqda 1 olur.

Z

Zero-day (**zero-hour** or **day zero**) **attack** or **zero day threat**
Sıfır gün (və ya ***sıfır saat***) **hücumu** – tətbiqi proqramlarda və ya əməliyyat sistemlərində öncədən bilinməyən, proqram təminatı istehsalçılarının aradan qaldırmağa vaxt tapmadıqları boşluğu istismar edən hücum.

Zero day vulnerability
Sıfır gün boşluğu – proqram təminatının proqram istehsalçısına məlum olmayan boşluğu.

Zombie
Zombi – başqa sistemlərə hücum etmək üçün sistemdə quraşdırılan proqram.

Zoo
Zoopark − tədqiqatçılar tərəfindən antivirus proqramlarını test etmək üçün istifadə olunan viruslar toplusu.

Zoo virus
Laboratoriya virusu − yalnız virus laboratoriyalarında olan, ümumi dövriyyəyə buraxılmayan virus.

Qısaltmalar

A	
AAA	Authentication, Authorization and Audit *Autentifikasiya, avtorizasiya və audit*
ABEND	ABnormal END *Anormal son*
ACE	Access Control Entry *Girişi idarəetmə yazısı*
ACL	Access Control List *Girişi idarəetmə siyahısı*
AD	Active Directory *Aktiv kataloq*
ADSL	Asymmetric Digital Subscriber Line *Asimmetrik rəqəmsal abunə xətti*
AES	Advanced Encryption Standard *Qabaqcıl şifrləmə standartı*
AFIS	Automated Fingerprint Identification System *Barmaq izlərinin avtomatlaşdırılmış identifikasiyası sistemi*
AH	Authentication Header *Autentifikasiya başlığı*
AIS	Automated Information Systems *Avtomatlaşdırılmış informasiya sistemləri*
AJAX	Asynchronous JavaScript and XML) *Asinxron Cava skripti və XML*
ALE	Annual Loss Expectancy *İllik itki gözləntisi*
AMTSO	Anti-Malware Testing Standards Organization *Zərərli Proqramların Testləşdirilməsi Standartları Təşkilatı*
ANSI	American National Standards Institute *Amerika Milli Standartları İnsititutu*
API	Application Program Interface *Tətbiqi proqramlaşdırma interfeysi*
ARP	Address Resolution Protocol *Ünvanı müəyyənləşdirmə protokolu*
ARPA	Advanced Research Projects Agency *Perspektiv Elmi-Tədqiqat Layihələri Agentliyi*

ASAX	Advanced Security Audit-trail Analysis on Unix *UNİX-də təhlükəsizlik auditi jurnallarının analizi*
ASCII	American Standard Code for Information Interchange *İnformasiya mübadiləsi üçün Amerika standart kodu*
ASN.1	Abstract Syntax Notation One *Mücərrəd sintaksis işarələnməsi 1*
ASP	Active Server Page *Aktiv server səhifəsi*
ASPECT	Automated Security Protocol Examination And Checking Tool *Təhlükəsizlik protokolunun avtomatlaşdırılmış ekspertiza və yoxlama aləti*
ASSIST	Automated Systems Security Incident Support Team *Avtomatlaşdırılmış sistemlərdə təhlükəsizlik insidentlərinin emalı komandası*
ATM	Asynchronous Transfer Mode *Asinxron ötürmə rejimi*
AUP	Acceptable Use Policy *Münasib istifadə siyasəti*
ASW	*Attack Sensing and Warning* *Hücumun aşkarlanması və xəbər verilməsi*

B

BAPI	Biometrics Application Programming Interface *Biometrik tətbiqi proqramlaşdırma interfeysi*
BBS	Bulletin Board System *Məlumat lövhəsi sistemi*
BC	Block Chaining *Blokların qoşulması*
BCP	Business Continuity Plan *Fəaliyyətin fasiləsizliyi planı*
BER	Basic Encoding Rules *Əsas kodlaşdırma qaydaları*
BIA	Business Impact Analysis *Fəaliyyətə təsirin analizi*
BIND	Berkeley Internet Name Domain *Berkli İnternet adları domeni*
BIOS	Basic Input/Output System *Əsas giriş/çıxış sistemi*

BISO	Business Information Security Officer *İnformasiya təhlükəsizliyi meneceri*
BO	Back Orifice
BO2K	Back Orifice 2000
BootP	Bootstrap Protocol *Yükləmə protokolu*
Bps	Bits per second *Saniyədə bit*
BREACH	Browser Reconnaissance and Exfiltration via Adaptive Compression of Hypertext *Hipermətnin adaptiv sıxılması ilə brauzerin izlənməsi və verilənlərin köçürülməsi*
BRP	Business Recovery-Resumption Plan *Fəaliyyətin bərpası planı*
BS 7799	British Standard 7799 *Britaniya standartı 7799*
BSD	Berkeley Software Distribution *Berkli proqram təminatı yayımı*
BSI	British Standards Institution *Britaniya Standartlar İnstitutu*

C

CA	Certification Authority *Sertifikat mərkəzi*
CAN	Campus Area Network *Kampus kompüter şəbəkəsi*
CAPEC	Common Attack Pattern Enumeration and Classification *Hücum şablonlarının ümumi siyahısı və təsnifatı*
CAPI	Cryptographic Application Programming Interface *Kriptoqrafik tətbiqi proqramlaşdırma interfeysi*
CASL	Custom Audit Scripting Language *Xüsusi audit skript dili*
CBC	Cipher Block Chaining *Şifr blokların qoşulması*
CBK	Common Body of Knowledge *Biliklərin ümumi məcmusu*
CC	Common Criteria *Ümumi Meyarlar*

CCSE	Check Point Certified Security Engineer *Check Point üzrə sertifikatlı təhlükəsizlik mühəndisi*
CCSP	Cisco Certified Security Professional *Cisco sertifikatlı təhlükəsizlik mütəxəssisi*
CCSS	Common Configuration Scoring System *Konfiqurasiyanı ümumi qiymətləndirmə sistemi*
CCTL	Common Criteria Testing Laboratory *Ümumi Meyarlar üzrə test laboratoriyası*
CD	1. Carrier Detect *Daşıyıcının aşkarlanması* 2. Committee Draft *Komitə layihəsi*
CDMA	Code Division Multiple Access *Kod bölgülü çoxsaylı giriş*
CDR	Critical Design Review *Kritik layihə icmalı*
CEH	Certified Ethical Hacker *Sertifikatlı etik haker*
CEM	Common Evaluation Methodology *Ümumi qiymətləndirmə metodologiyası*
CEO	Chief Executive Officer *Baş icraçı menecer*
CERIAS	Center for Education and Research in Information Assurance and Security *İnformasiya Təhlükəsizliyi üzrə Təhsil və Tədqiqat Mərkəzi*
CERT	Computer Emergency Response Team *Kompüter insidentlərinə cavab komandası*
CERT/CC	CERT (Computer Emergency Response Team)/ Coordination Center *Kompüter İnsidentlərinə Cavab Komandası/Koordinasiya Mərkəzi*
CFB	Cipher Feedback *Şifr əks əlaqəsi*
CGI	Common Gateway Interface *Ümumi şlüz interfeysi*
CHAP	Challenge Handshake Authentication Protocol *Çağırış-əlsıxma autentifikasiya protokolu*
CIAC	Computer Incident Advisory Capability

	Kompüter insidentlərinə məsləhət bacarığı
CIDF	Common Intrusion Detection Framework *Müdaxilələrin aşkarlanması üzrə vahid arxitektura*
CIO	Chief Information Officer *Əsas informasiya meneceri*
CIRT	1. Cyber-Incident Response Team *Kiber-insidentlərə cavab komandası*
	2. Computer Incident Response Team *Kompüter insidentlərinə cavab komandası*
CIS	Center for Internet Security *İnternet Təhlükəsizliyi üzrə Mərkəz*
CISA	Certified Information Systems Auditor *Sertifikatlı informasiya sistemləri auditoru*
CISF	Catalyst Integrated Security Framework *Catalyst inteqral təhlükəsizlik sxemi*
CISL	Common Intrusion Specification Language *Müdaxilə spesifikasiyası üzrə ümumi dil*
CISM	Certified Information Security Manager *İnformasiya təhlükəsizliyiüzrə sertifikatlı meneceri*
CISO	Chief Information Security Officer *İnformasiya təhlükəsizliyi üzrə director*
CISSP	Certified Information Systems Security Professional *İnformasiya sistemlərinin təhlükəsizliyi üzrə sertifikatlı mütəxəssis*
CMM	Capability Maturity Model *Potensialın yetkinliyi modeli*
CMOS	Complementary Metal Oxide Semiconductor *Əlavə metal oksidli yarımkeçirici*
CMS	Cryptographic Message Syntax *Kriptoqrafik məlumat sintaksisi*
CMSS	Common Misuse Scoring System *Sui-istifadəni ümumi qiymətləndirmə sistemi*
COAST	Computer Operations, Audit, and Security Technology *Kompüter əməliyyatları, audit və təhlükəsizlik texnologiyaları*
COBIT	Control Objectives for Information and related Technology *İnformasiya və əlaqəli texnologiyalar üçün idarəetmə məsələləri*
CoC	Chain of Custody *Mühafizə zənciri*

COE	Common Operating Environment *Ümumi əməliyyat mühiti*
COMPSEC	Computer Security *Kompüter təhlükəsizliyi*
COMPUSEC	Computer Security *Kompüter təhlükəsizliyi*
COMSEC	Communications Security *Kommunikasiya təhlükəsizliyi*
COPS	Computer Oracle and Password System *Kompüter orakulu və parol sistemi*
CORES	Computer Response Squad *Kompüter cinayətkarlığı üzrə bölmə*
CP	Certificate Policy *Sertifikatların tətbiqi siyasəti*
CPE	Common Platform Enumeration *Platformaların ümumi siyahısı*
CPS	Certificate Practices Statement *Sertifikatın verilməsi qaydası*
CPU	Central Processing Unit *Mərkəzi prosessor*
CRAMM	CCTA Risk Analysis and Management Method *Dövlət təşkilatları üçün riskin analizi və idarə edilməsi metodu*
CRC	Cyclic Redundancy Check *Tsiklik izafi kod*
CRL	Certificate Revocation List *Ləğv edilmiş sertifikatlar siyahısı*
CryptoAPI	Cryptographic Application Programming Interface *Kriptoqrafik tətbiqi proqramlaşdırma interfeysi*
CSI	Computer Security Institute *Kompüter Təhlükəsizliyi İnsititu*
CSIR	Computer Security Incident Response *Kompüter təhlükəsizliyi insidentlərinin emalı*
CSIRT	Computer Security Incident Response Team *Kompüter təhlükəsizliyi insidentlərinin emalı komandası*
CSMA/CD	Carrier Sense Multiple Access/Collision Detection *Daşıyıcını aşkarlamaqla çoxsaylı giriş/toqquşmanın aşkarlanması*
CSO	Chief Security Officer *Təhlükəsizlik üzrə direktor*

CSP	Cryptographic Service Provider *Kriptoqrafik servis provayderi*
CSRC	Computer SecurityResponse Center *Kompüter təhlükəsizliyi insidentləri üzrə mərkəz*
CSS	Cascading Style Sheets *Kaskad stil cədvəlləri*
CTR	Counter Mode *Sayğac rejimi*
CVE	1. Common Vulnerabilities and Exposures *Boşluqlar üzrə ümumi tezaurus* 2. Common Vulnerability Enumeration *Boşluqlar üzrə ümumi baza*
CVSS	Common Vulnerability Scoring System *Boşluqları ümumi qiymətləndirmə sistemi*
CWE	Common Weakness Enumeration *Boşluqların ümumi siyahısı*
CybOX	Cyber Observable eXpression *Kiberdomendə müşahidələrin təsviri*

D

DAC	Discretionary Access Control *Girişin diskresion idarə edilməsi*
DACL	Discretionary Access Control List *Girişin diskresion idarə edilməsi siyahısı*
DAF	Deutsches Advisory Format *Təhlükəsizlik bülleteni formatı*
DAP	Directory Access Protocol *Kataloqa giriş protokolu*
DARPA	Defense Advanced Research Projects Agency *Perspektiv Müdafiə Elmi-Tədqiqat Layihələri Agentliyi*
DBMS	Database Management System *Verilənlər bazasını idarəetmə sistemi*
DCFL	Defense Computer Forensics Laboratory *ABŞ Müdafiə Nazirliyi Kompüter Ekspertizası Laboratoriyası*
DCOM	Distributed Component Object Model *Paylanmış komponent obyekt modeli*
DDN	Defense Data Network *ABŞ Müdafiə Nazirliyi Məlumat Şəbəkəsi*

DDoS	Distributed Denial of Service *Paylanmış xidmətdən imtina*
DER	Distinguished Encoding Rules *Fərqləndirici kodlaşdırma qaydaları*
DES	Data Encryption Standard *Verilənləri şifrləmə standartı*
DH	Diffie-Hellman *Diffi-Helman*
DHCP	Dynamic Host Configuration Protocol *Hostun dinamik konfiqurasiyası protokolu*
DIB	Directory Information Base *Kataloqun informasiya bazası*
DIDS	Distributed Intrusion Detection System *Müdaxilələrin paylanmış aşkarlanması sistemi*
DISA	Defense Information Systems Agency *ABŞ Müdafiə Nazirliyi İnformasiya Sistemləri Agentliyi*
DLL	Dynamic Link Library *Dinamik əlaqə kitabxanası*
DMZ	Demilitarized zone *Demilitarizasiya zonası*
DN	Distinguished Name *Fərqləndirici ad*
DNS	1. Domain Name System 1. *Domen adları sistemi* 2. Domain Name Service 2. *Domen adları xidməti*
DNSSEC	Domain Name System Security Extensions *DNS təhlükəsizlik genişlənməsi*
DOI	Domain of Interpretation *İnterpretasiya domeni*
DoS	Denial of Service *Xidmətdən imtina*
DOS	Disk Operating System *Disk əməliyyat sistemi*
DPA	Differential Power Analysis *Enerjinin diferensial analizi*
DPI	Deep Packet Inspection *Dərin Paket Təftişi*

DR	Design Review *Layihə icmalı*
DRM	Digital Rights Management *Rəqəmsal hüquqların idarə edilməsi*
DRP	Disaster Recovery Plan *Qəzadan sonra bərpaetmə planı*
DSA	Digital Signature Algorithm *Rəqəmsal imza alqoritmi*
DSL	Digital Subscriber Line *Rəqəmsal abunə xətti*
DSO	Data Security Officer *Verilənlərin təhlükəsizliyi üzrə mütəxəssis*
DSP	Digital Signal Processing *Rəqəmsal siqnalların emalı*
DSS	Digital Signature Standard *Rəqəmsal imza standartı*

E

EAL	Evaluation Assurance Level *Qiymətləndirmənin zəmanət səviyyəsi*
EAP	Extensible Authentication Protocol *Genişlənən autentifikasiya protokolu*
EARN	European Academic Research Network *Avropa Akademik Tədqiqatlar Şəbəkəsi*
ECB	Electronic codebook *Elektron kod kitabı*
ECC	Elliptic Curve Cryptosystem/Cryptography *Elliptik əyrilər üzərində kriptosistem/kriptoqrafiya*
ECDL	Elliptic Curve Discrete Logarithm *Elliptik əyrilər üzərində diskret loqarifm*
ECDSA	Elliptic Curve Digital Signature Algorithm *Elliptik əyrilər üzərində rəqəmsal imza alqoritmi*
ECPA	Electronic Communications Privacy Act *Elektron kommunikasiyaların gizliliyi qanunu*
EES	Eccrowed Encryption Standart *Açarların deponə edilməsi ilə şifrləmə standartı*
EFS	Encrypting File System *Şifrlənmiş fayl sistemi*

EGP	Exterior Gateway Protocol *Xarici şlüz protokolu*
EIA	Electronic Industries Association *Elektronika Sənayesi Assosiasiyası*
EICAR	European Institute of Computer Anti-Virus Research *Avropa Kompüter Antivirusu Tədqiqat İnstitutu*
ELESEC	Electronic Emission Security *Elektron şüalanmaların təhlükəsizliyi*
E-mail	Electronic Mail *Elektron poçt*
EMERALD	Event Monitoring Enabling Responses to Anomalous Live Disturbances *Anomal insidentləri real rejimdə emal edən hadisə monitorinqi*
EMRT	Emergency Response Time *Qəzalara reaksiya vaxtı*
EMSEC	1. Emanation security 2. Emissions Security *Şüalanmaların təhlükəsizliyi*
ENISA	European Network and Information Security Agency *Avropa Şəbəkə və İnformasiya Təhlükəsizliyi Agentliyi*
ESP	Encapsulating Security Payload *Şifrlənmiş verilənlərin inkapsulyasiyası protokolu*
ETSI	European Telecommunications Standardization Institute *Avropa Telekommunikasiya Standartlaşdırma İnstitutu*
Eunet	European UNIX Network *Avropa UNİX şəbəkəsi*
EUT	End User Terminal *İstifadəçi terminal*
EUUG	European UNIX Users Group *Avropa UNİX istifadəçiləri qrupu*
EW	Electronic warfare *Radioelektron müharibə*

F

FAR	False Acceptance Rate *Səhv qəbul əmsalı*
FIPS	Federal Information Processing Standard *Federal informasiya emalı standartı*
FIRST	Forum of Incident Response and Security Teams *İnsidentlərin emalı və təhlükəsizlik komandalarının beynəlxalq forumu*

FRR	False Rejection Rate *Səhv imtina əmsalı*

G

GAWN	GIAC Auditing Wireless Networks *Naqilsiz şəbəkələrin auditi üzrə GIAC sertifikatı*
GCFA	GIAC Certified Forensics Analyst *Kriminalistik ekspertiza və analiz üzrə GIAC sertifikatı*
GCFW	GIAC Certified Firewall Analyst *Şəbəkələrarası ekran analizi üzrə GIAC sertifikatı*
GCHQ	Government Communications HeadQuarters *Hökumət kommunikasiyaları qərargahı*
GCIA	GIAC Certified Intrusion Analyst (Certified Professionals) *Müdaxilələrin analizi üzrə GIAC sertifikalı*
GCIH	GIAC Certified Incident Handler *İnsidentlərin emalı üzrə GIAC sertifikatı*
GEWF	GIAC E-warfare Certified Professionals *E-müharibə üzrə GIAC sertifikatı*
GHSC	GIAC HIPAA Security Implementation *HIPAA təhlükəsizliyinin realizasiyası üzrə GIAC sertifikatı*
GHTQ	GIAC Cutting Edge Hacking Techniques *Yüksək haker texnologiyaları üzrə GIAC sertifikatı*
GIAC	1. Global Information Assurance Certification *İnformasiya Təhlükəsizliyi üzrə Qlobal Sertifikatlaşdırma şirkəti* 2. Global IncidentAnalysisCenter *Qlobal İnsident Analizi Mərkəzi*
GIF	Graphics Interchange Format *Qrafiki mübadilə formatı*
GIG	Global Information Grid *Qlobal informasiya qridi* (*şəbəkəsi*)
GII	Global Information Infrastructure *Qlobal informasiya infrastrukturu*
GINA	Graphical Identification and Authorisation *Qrafiki identifikasiya və autentifikasiya*
GISA	German Information Security Agency *Almaniya İnformasiya Təhlükəsizliyi Agentliyi*
GISF	GIAC Information Security Fundamentals *İnformasiya təhlükəsizliyinin əsasları üzrə GIAC sertifikatı*

GISO GIAC Information Security Officer
GIAC sertifikatlı informasiyası təhlükəsizliyi meneceri

GLBA Graham-Leach-Billey Act
Qrem Liç Billi qanunu

GLIT GIAC Legal Issues in Information Technologies
İnformasiya texnologiyalarının hüquqi problemləri üzrə GIAC sertifikatı

GMT Greenwich Mean Time
Qrinviç vaxtı

GNOSC Global Network Operations and SecurityCenter
Qlobal şəbəkə əməliyyatları və təhlükəsizlik mərkəzi

GPO Group Policy Object
Qrup siyasəti obyekti

GPS Global Positioning System
Qlobal Mövqetəyinetmə Sistemi

GRE Generic Routing Encapsulation
Ümumi marşrutlamanın inkapsulyasiyası

GrIDS Graph-based Intrusion Detection System
Qrafəsasında müdaxilələri aşkarlama sistemi

GRIP Guidelines and Recommendations for Security Incident Processing
Təhlükəsizlik insidentlərinin emalı üçün direktivlər və tövsiyələr

GSAE GIAC Security Audit Essentials
Təhlükəsizliyin auditi üzrəGIAC sertifikatı

GSE GIAC Security Expert
Təhlükəsizlik eksperti üzrə GIAC sertifikatı

GSEC GIAC Security Essentials Certification
Təhlükəsizliyin əsas prinsipləri üzrə GIAC sertifikatı

GSI Grid Security Infrastructure
Qrid təhlükəsizliyi infrastrukturu

GSLC GIAC Security Leadership Certification
Təhlükəsizliyin idarə edilməsi üzrə GIAC sertifikatı

GSM Global System for Mobile Communications, əvvəllər Groupe Spécial Mobile
Mobil rabitə üçün qlobal sistem

GSNA GIAC Systems and Network Auditor
Sistem və şəbəkə auditi üzrə GIAC sertifikatı

GSS Generic Security Services *Ümumi təhlükəsizlik servisləri*

GSS-API Generic Security Services – Application Programming Interface
Ümumi təhlükəsizlik servisləri – tətbiqi proqramlaşdırma interfeysi

GUI Graphical User Interface
Qrafik istifadəçi interfeysi

GUID Globally Unique Identifier
Qlobal unikal identifikator

GW Gateway *Şlüz*

H

HA High Availability
Yüksək əlyetənlik

HDLC High-level Data Link Control
Yüksəviyyəli verilənlər kanalını idarəetmə

HDSL High Bit-Rate Digital Subscriber Line
Yüksək bit sürətli rəqəmsal abunə xətti

HIDS Host-based IDS
Host-əsaslı IDS

HIPAA Health Insurance Portability and Accountability Act
Sağlamlıq sığortasının mobilliyi və məsuliyyət qanunu

HMAC Hash- Message Authentication Code
Məlumatın heş əsasında autentifikasiya kodu

HSM Hardware Security Module
Aparat təhlükəsizlik modulu

HTML HyperText Markup Language
Hipermətni nişanlama dili

HTTP HyperText Transfer Protocol
Hipermətni ötürmə protokolu

HTTPS HyperText Transfer Protocol Secure
Hipermətni təhlükəsiz ötürmə protokolu

I

I2WAR Infrastructural And Information Warfare
Infrastruktur və informasiya müharibəsi

IAB Internet Activities Board
İnternet Koordinasiya Şurası

IAM	Identity and Access Management *Identifikasiya və girişin idarə edilməsi*
IAP	Intrusion Alert Protocol *Müdaxilə xəbərdarlığı protokolu*
IATF	Information Assurance Technical Framework *Informasiya təhlükəsizliyi tədbirlərinin texniki strukturu*
IAVA	Information Assurance Vulnerability Alert *İnformasiya təhlükəsizliyi boşluq xəbərdarlığı*
IAVM	Information Assurance Vulnerability Management *Informasiya təhlükəsizliyi boşluqlarının idarə edilməsi*
IBAC	Identity Based Access Control *Identifikator əsasında girişin idarə edilməsi*
IBE	Identity Based Encryption *Identifikator əsasında şifrləmə*
ICF	Internet Connection Firewall *Internet bağlantıları üçün şəbəkələrarası ekran*
ICMP	Internet Control Message Protocol *Internet idarəetmə məlumatları protokolu*
ICSA	International Computer Security Association *Beynəlxalq kompüter təhlükəsizliyi assosiasiyası*
ICQ	I seek you – "*Səni axtarıram*" *Ani ismarıc sistemi*
ICV	Integrity Check Value *Tamlığı yoxlama kodu*
ID	Identifier (identification) *İdentifikator (eyniləşdirmə)*
IDEA	International Data Encryption Algorithm *Verilənlərin şifrlənməsi üzrə beynəlxalq alqoritm*
IDES	Intrusion Detection Expert System *Müdaxilələrin aşkarlanması üzrə ekspert sistemi*
IDIOT	Intrusion Detection In Our Time *Müdaxilələrin müasir aşkarlanmasısistemi*
IDMEF	Intrusion Detection Message Exchange Format *Müdaxilələrin aşkarlanması məlumatlarını mübadilə formatı*
IDP	Intrusion Detection and Prevention System *Müdaxilələrin aşkarlanmsı və qarşısının alınması sistemi*
IDS	Intrusion Detection System *Müdaxilələrin aşkarlanması sistemi*

IDWG	Intrusion Detection Working Group *Müdaxilələrin aşkarlanması üzrə işçi qrupu*
IDXP	Intrusion Detection Exchange Protocol *Müdaxilələtin aşkarlanması üzrə mübadilə protokolu*
IEEE	Institute of Electrical and Electronic Engineers *Elektrik və elektron mühəndislərin institutu*
IEEE-CS	IEEE Computer Society *IEEE hesablama texnikası üzrə mütəxəssislər cəmiyyəti*
IESG	Internet Engineering Steering Group *İnternet Texnologiyaları idarəetmə Qrupu*
IETF	Internet Engineering Task Force *İnternet Texnologiyaları İşçi qrupu*
IGP	Interior Gateway Protocol *Daxili şlüz protokolu*
IGRP	Internet Gateway Routing Protocol *Internet şlüz marşurutlama protokolu*
IISSCC	International Information Systems Security Certification Consortium *İnformasiya sistemlərinin təhlükəsizliyi üzrə Beynəlxalq sertifikatlaşdırma konsorsiumu*
IKE	Internet Key Exchange *İnternet açar mübadiləsi*
IKP	Internet Keyed Payments Protocol *Internet açarlı ödənişlər protokolu*
INFOCON	Information Condition *Informasiya şərti*
INFOSEC	Information Security *İnformasiya təhlükəsizliyi*
INFOWAR	Information Warfare *Informasiya müharibəsi*
IOS	Internet Operating System *Internet əməliyyat sistemi*
IP	Internet Protocol *İnternet protokolu*
IPR	Intellectual Property Rights *Intellektual mülkiyyət hüquqları*
IPRA	Internet Policy Registration Authority *İnternet siyasət qeydiyyatı mərkəzii*

IPS	Intrusion Prevention System *Müdaxilələrin qarşısını alma sistemi*
IPSec	Internet Protocol Security *İnternet protokolun təhlükəsizliyi*
IPX/SPX	Internet Packet eXchange *Internet paket mübadiləsi*
IRC	Internet Relay Chat *İnternetdə danışıq protokolu*
IRF	Inherited Rights Filter *İrsi hüquqlar süzgəci*
ISA	Internet Security and Acceleration *İnternet təhlükəsizliyi və sürətləndirmə*
ISACA	Information Systems Audit and Control Association *Informasiya sistemlərinin auditi və idarə edilməsi assosiasiyası*
ISAKMP	Internet Security Association and Key Management Protocol *Internet təhlükəsizlik assosiasiyası və açar idarəetmə protokolu*
ISC	International Security Consortium *Beynəlxalq təhlükəsizlik konsorsiumu*
ISC)^2	International Information Systems Security Certification Consortium *İnformasiya sistemlərinin təhlükəsizliyi üzrə Beynəlxalq sertifikatlaşdırma konsorsiumu*
ISDN	Integrated Services Digital Network *İnteqral rəqəmsal xidmətlər şəbəkəsi*
ISMS	Information Security Management System *İnformasiya təhlükəsizliyini idarəetmə sistemi*
ISO	1. International Standards Organization 1*. Beynəlxalq standartlaşdırma təşkilatı* 2. Information Security Officer *2. İnformasiya təhlükəsizliyi meneceri*
ISP	Internet Service Provider *Internet xidmət provayderi*
ISS	Internet Security Scanner *Internet təhlükəsizlik skaneri*
ISSA	1. Information Systems Security Association *Informasiya sistemləri təhlükəsizliyi assosiasiyası*

	2. International Systems Security Association *Sistemlərin Təhlükəsizliyi üzrə Beynəlxalq Assosiasiya*
ISSM	Information Systems Security Manager *İnformasiya sistemləri təhlükəsizlik meneceri*
ISSO	Information Systems Security Officer *Informasiya sistemləri təhlükəsizlik meneceri*
ISSP	Information System Security Policy *İnformasiya sisteminin təhlükəsizlik siyasəti*
IT	InformationTechnology *İnformasiya texnologiyası*
ITA	Intruder Alert *Müdaxilə xəbərdarlığı*
ITSCC	Information Technology Security Common Criteria *İnformasiya texnologiyalarının təhlükəsizliyi üzrə ümumi meyarlar*
ITSEC	Information Technology Security Evaluation Criteria *İnformasiya texnologiyalarının təhlükəsizliyini qiymətləndirmə meyarları*
ITU-T	International Telecommunications Union, Telecommunication Standardization Sector *Beynəlxalq Telekommunikasiyalar İttifaqı, Telekommunikasiya standartlaşdırma bölməsi*
IV	Initialization Vector *İlkin yükləmə vektoru*
IW	Information warfare *İnformasiya müharibəsi*

J

JCE	Java Cryptographic Extension *Java şifrləmə əlavəsi*
JSON	JavaScript Object Notation *Java Skript Obyekt İşarələri*

K

Kbps	Kilobits per second *Saniyədə kilobit*
KDC	KeyDistribution Center *Açar paylaşdırma mərkəzi*

KMC	KeyManagement Center *Açar idarəetmə mərkəzi*
KMI	Key Management Infrastructure *Açar idarəetmə infrastrukturu*
KMP	Key Management Protocol *Açar idarəetmə protokolu*
KMS	Key Management System *Açar idarəetmə sistemi*
KSOS	Kernelized Secure Operating System *Nüvəli təhlükəsiz əməliyyat sistemi*

L

L2FP	Layer 2 Forwarding Protocol *2-ci səviyyə ötürmə protokolu*
L2TP	Layer 2 Tunneling Protocol *2-ci səviyyə tunel protokolu*
LAN	Local Area Network *Lokal şəbəkə*
LDAP	Lightweight Directory Access Protocol *Kataloqa sadə giriş protokolu*
LES	LAN Emulation Server *Lokal şəbəkənin emulyasiyası serveri*
LFSR	Linear Feedback Shift Register *Xətti əks-əlaqə sürüşmə registri*
LIDS	Linux Intrusion Detection System *Linux müdaxilələri aşkarlama sistemi*
LSA	Local Security Authority *Lokal təhlükəsizlik mərkəzi*

M

MAC	1. Message Authentication Code *Məlumatın autentifikasiya kodu* 2. Mandatory Access Control *Girişi məcburi idarəetmə* 3. Media Access Control *Mühitə girişi idarəetmə*
MAEC	Malware Attribute Enumeration and Characterization

Zərərli proqram təminatı atributlarının siyahısı və xarakteristikaları

MAN Metropolitan Area Network *Şəhər şəbəkəsi*

MANET Mobile Ad Hoc Networking
Mobil adhok şəbəkə

MARS Monitoring, Analysis and Response System
Monitorinq, analiz və cavab sistemi

MBR Master Boot Record
Əsas yükləmə yazısı

MBSA Microsoft Baseline Security Analyzer
Microsoft baza təhlükəsizlik analizatoru

MD Message Digest
Məlumat heş-kodu

MDC Manipulation Detection Code
Manipulyasiyanı aşkarlama kodu

MHz Megahertz
Meqahers

MIB Management Information Base
İdarəetmə informasiyası bazası

MIC Message Integrity Check
Məlumatın tamlığını yoxlama

MIDAS Multics Intrusion Detection and Alerting System
Multics müdaxilələri aşkarlama və xəbərdarlıq sistemi

MILNET MILitary NETwork
Hərbi şəbəkə

MIME Multipurpose Internet Mail Extensions
Çoxməqsədli İnternet poçt genişlənmələri

MITM Man-in-the-middle
Ortada adam

MLS Multi Level Security
Çoxsəviyyəli təhlükəsizlik

MOSS MIME Object Security Services
MIME obyekt təhlükəsizliyi xidmətləri

MPLS Multiprotocol Label Switching
Çoxprotokollu nişan kommutasiyası

MS-CHAP Microsoft Challenge Handshake Authentication Protocol
Microsoft çağırış-əlsıxma autentifikasiya protokolu

MTA Message Transfer Agent

	Məlumat ötürmə agenti
MTBF	Mean Time Between Failure *Qəzalararası orta vaxt*
MtE	Mutation Engine *Mutasiya mühərriki*
MTS	1. Mail Transfer System *Poçt ötürmə sistemi* 2. Message Transfer System *Məlumat ötürmə sistemi*
MTTR	Mean Time to Repair *Orta bərpaetmə müddəti*
MTU	Maximum Transmission Unit *Maksimal ötürmə vahidi*

N

NADER	Network Anomaly Detection and Intrusion Reporter *Şəbəkə anomaliyasını aşkarlama və müdaxilə xəbərçisi*
NADIR	Network Audit Director and Intrusion Reporter *Şəbəkə audit direktoru və müdaxilə xəbərçisi*
NAT	Network Address Translation *Şəbəkə ünvanının translyasiyası*
NCSA	National Computer Security Association *Milli kompüter təhlükəsizliyi assosiasiyası*
NCSC	NationalComputerSecurityCenter *Milli kompüter təhlükəsizliyi mərkəzi*
NES	Network Encryption System *Şəbəkə şifrləmə sistemi*
NetBEUI	NetBIOS Extended User Interface *NetBIOS genişləndirilmiş istifadəçi interfeysi*
NetBIOS	Network Basic Input Output System *Baza şəbəkə giriş-çıxış sistemi*
NFS	Network File System *Şəbəkə fayl sistemi*
NIAC	National Infrastructure Advisory Council *Milli infrastruktur məsləhət şurası*
NIC	Network Interface Card *Şəbəkə interfeysi kartı*

NIDES	1. Network Intrusion Detection Expert System *Şəbəkədə müdaxilələri aşkarlama üzrə ekspert sistemi* 2. Next-generation IDES (Intrusion Detection Expert System) *Yeni nəsl IDES (müdaxilələri aşkarlama üzrə ekspert sistemi)*
NIDS	Network-based IDS (Intrusion Detection System) *Şəbəkədə müdaxilələri aşkarlama sistemi*
NII	National Information Infrastructure *Milli informasiya infrastrukturu*
NIPC	National Infrastructure Protection Center *Milli infrastrukturu mühafizə mərkəzi*
N-ISDN	Narrowband Integrated Services Digital Network *Ensiz zolaqlı inteqral xidmətlərin rəqəmsal şəbəkəsi*
NIST	National Institute of Standards and Technology *Milli standartlar və texnologiyalar institutu*
NNTP	Network News Transfer Protocol *Şəbəkə xəbərlərini ötürmə protokolu*
NOC	Network Operations Center *Şəbəkə əməliyyat mərkəzi*
NOP	No-OP *Heç bir əməliyyat*
NOS	Network Operating System *Şəbəkə əməliyyat sistemi*
NSA	National Security Agency *Milli Təhlükəsizlik Agentliyi*
NSEP	National Security Emergency Preparedness *Milli təhlükəsizlik insidentlərinə hazırlıq dərəcəsi*
NSIRC	National Security Incident Response Center *Təhlükəsizlik İnsidentlərinin Emalı üzrə Milli tMərkəz*
NSM	Network Security Monitoring *Şəbəkə təhlükəsizliyinin monitorinqi*
NVD	National Vulnerability Database *İnformasiya təhlükəsizliyi boşluqları üzrə vahid baza*
NTLM	Windows NT LAN Manager *Windows NT LAN meneceri*

O

OAEP	Optimal Asymmetric Encryption Padding

	Optimal asimmetrik şifrləmə əlavəsi
OCB	Offset Codebook Mode *Sürüşmə kod kitabı rejimi*
OCSP	On-line Certificate Status Protocol *Onlayn sertifikat statusu protokolu*
ODBC	Open Data Base Connectivity *Verilənlər bazalarının birləşdirmə imkanı*
OFB	Output Feedback *Çıxışla əks-əlaqə rejimi*
OFBNLF	Output Feedback With A Nonlinear Function *Qeyri-xətti funksiya ilə çıxışla əks-əlaqə rejimi*
OID	Object ID *Obyekt ID*
OO	Object-Oriented *Obyekt yönümlü*
OOB	Out-Of-Band *Buferin daşması*
OOP	Object-oriented programming *Obyekt yönümlü proqramlaşdırma*
OPSEC	1. Open Platform for Secure Enterprise Connectivity *Təhlükəsiz müəssisə birləşməsi üçün açıq platforma* 2. Operational security *Əməliyyatların təhlükəsizliyi*
OS	Operating System *Əməliyyat sistemi*
OSI	Open Systems Interconnection *Açıq sistemlərin qarşılıqlı əlaqəsi*
OSINT	Open-source intelligence *Açıq mənbə kəşfiyyatı*
OSPF	Open Shortest Path First *Əvvəlcə ən qısa yol protokolu*
OSSTM	Open-Source Security Testing Methodology *Açıq kodun təhlükəsizliyini testetmə metodologiyası*
OSVDB	Open Source Vulnerability DataBase *Boşluqlar üzrə açıq verilənlər bazası*
OTP	1. One-Time Password *Birdəfəlik parol*

	2. One-Time Pad *Birdəfəlik bloknot*
OWASP	Open Web Application Security Project *Tətbiqi veb proqramların təhlükəsizliyi üzrə açıq layihə*
	P
PAP	1. Password Authentication Protocol *Parol autentifikasiya protokolu*
	2. Pre-Attack Probe *Hücum öncəsi analiz*
PBC	Plaintext Block Chaining *Açıq mətn bloklarının qoşulması*
P-BEST	Production-Based Expert System Toolset *İstehsalat-əsaslı ekspert sistemləri alətləri*
PBX	Private Branch Exchange *Xüsusi bölmə mübadiləsi*
PC	Personal Computer *Fərdi kompüter*
PCBC	Propagating Cipher Block Chaining *Şifrlənmiş blok zəncirinin yayılması rejimi*
PCI	Protocol Control Information *Protokolu idarəetmə məlumatları*
PCM	Pulse Code Modulation *İmpuls kod modulyasiyası*
PCMCIA	Personal Computer Memory Card International Association *Fərdi kompüter yaddaş kartı beynəlxalq assosiasiyası*
PD	Protocol Decode *Protokolun dekodlaşdırılması*
PDA	Personal Digital Assistant *Fərdi rəqəmsal köməkçi*
PEAP	Protected EAP *Qorunan EAP*
PEM	Privacy Enhanced Mail *Yüksək gizlilik poçtu*
PERT	Program Evaluation and Review Technique *Proqramların qiymətləndirilməsi və icmalı metodu*
PFB	Plaintext Feedback *Açıqmətnlə əks əlaqə rejimi*

PFS	Perfect Forward Secrecy *Birbaşa mükəmməl məxfilik*
PGP	Pretty Good Privacy *Yüksək gizlilik proqramı*
PIN	Personal Identification Number *Fərdi identifikasiya nömrəsi*
PING	Packet Internet Groper *İnternet yoxlama paketi*
PIX	1. Private Internet eXchange *Məxfi İnternet mübadiləsi* 2. Personal Information eXchange *Fərdi informasiya mübadiləsi*
PKC	Public Key Cryptography *Açıq açarlı kriptoqrafiya*
PKCS	Public-Key Cryptography Standards *Açıq açarlı kriptoqrafiya standartı*
PKI	Public Key Infrastructure *Açıq açar infrastrukturu*
PKIX	Public Key Infrastructure X.509 *Açıq açar infrastrukturu X.509*
POSIX	Portable Operating System Interface uniX *Portativ UNIX əməliyyat sistemi interfeysi*
PP	Protection Profile *Mühafizə profili*
PPL	Preferred Products List *Üstün tutulan məhsullar siyahısı*
PPP	Point-to-Point Protocol *Nöqtə nöqtə protokolu*
PPTP	Point-to-Point Tunneling Protocol *Nöqtə-nöqtə tunel ləmə protokolu*
PRNG	Pseudo Random Number Generator *Psevdotəsadüfi ədədlər generator*
PROM	Programmable Read Only Memory *Proqramlaşdırılan operativ yaddaş*
PSS	Probabilistic Signature Scheme *Ehtimala əsaslanan imza sxemi*

PVC	Permanent Virtual Connection *Daimi virtual əlaqə*
PVLAN	Private VLAN *Özəl VLAN*

Q

QKD	Quantum Key Distribution *Açarların kvant paylanması*
QOP	Quality Of Protection *Mühafizənin keyfiyyəti*
QoS	Quality of Service *Xidmətin keyfiyyəti*

R

RA	Registration Authority *Qeydiyyat mərkəzi*
RADIUS	1. Remote Access Dial-In User Service *Məsafədən modemlə giriş edən istifadəçi xidməti* 2. Remote Authentication Dial-In User Service *Məsafədən modemlə autentifikasiya edən istifadəçi xidməti*
RAID	Recent Advances in Intrusion Detection *Müdaxilələrin aşkarlanmasında yeni irəliləyişlər*
RAM	Random Access Memory *Təsadüfi girişli yaddaş*
RARP	Reverse Address Resolution Protocol *Tərs ünvanı müəyyənləşdirmə protokolu*
RBAC	Role Based Access Control *Rol əsasında girişin idarə edilməsi*
RC4/RC5/RC6	Rivest Chiper *Rayvest şifri*
RFC	Request for Comment *Şərh üçün sorğu*
RFI	Request For Information *Informasiya üçün sorğu*
RIP	Routing Information Protocol *Marşurutlayıcı informasiya protokolu*
RIPEMD	RIPE Message Digest

	RIPE məlumat icmalı
ROM	Read Only Memory *Yalnız oxunan yaddaş*
ROSI	Return of Security Investment *Təhlükəsizlik investisiyasının qayıtması*
RPC	Remote Procedure Call *Məsafədən prosedur çağırışı*
RSA	Rivest, Shamir, and Adleman *Rayvest, Şamir və Adleman*
RSVP	Resource Reservation Setup Protocol *Resursun ehtiyat saxlanması protokolu*
RTCP	Real-Time Transport Control Protocol *Real zaman nəqliyyatı idarəetmə protokolu*
RTP	Real-Time Transport Protocol *Real vaxtda nəqliyyat protokolu*
RTS	Request To Send *Göndərmək üçün sorğu*
RTSE	Reliable Transfer Service Element *Etibarlı ötürmə xidməti elementi*

S

S\MIME	Secure/Multipurpose Internet Mail Extensions *Təhlükəsiz /çoxməqsədli internet poçt genişlənmələri*
SA	1. System Administrator *Sistem administrator* 2. Security Association *Təhlükəsizlik assosiasiyası*
SACL	System Access Control List *Sistemə girişi idarəetmə siyahısı*
SAFE	Security Architecture for the Enterprise *Müəssisə üçün təhlükəsizlik arxitekturası*
SAFER	Secure And Fast Encryption Routine *Təhlükəsiz və sürətli şifrləmə alqoritmi*
SAM	Security Access Monitor *Təhlükəsizlik giriş monitoru*
SAML	Security Assertion Markup Language *Təhlükəsizlik funksiyalarını nişanlama dili*
SAMP	Suspicious Activity Monitoring Protocol

	Şübhəli fəaliyyətin monitorinqi protokolu
SANS Institute	System Administration, Networking, and Security Institute *Sistem inzibatçılığı, Şəbəkə və Təhlükəsizlik İnsititutu*
SATAN	System Administrator Tool for Analyzing Networks *Şəbəkə analizi üçün sistem administratoru aləti*
SBU	Sensitive but Unclassified *Həssas, lakin məxfi olmayan*
SCEP	Simple Certificate Enrollment Protocol *Sadə sertifikat qeydiyyatı protokolu*
SD	Security Descriptor *Təhlükəsizlik təsviri*
SDLC	Synchronous Data Link Control *Sinxron verilənlərin əlaqə kanalının idarə edilməsi*
SDLS	Single-Line Digital Subscriber Line *Simmetrik rəqəmsal abunə xətti*
SEAL	Software-optimized Encryption Algorithm *Proqram təminatına optimallaşdırılmış şifrləmə alqoritmi*
SEI	CarnegieMellonUniversity's Software Engineering Institute *Karneqi-Mellon Universiteti Proqram Təminatı Mühəndisliyi İnstitutu*
SERT	Security Emergency Response Team *Təhlükəsizlik insidentlərinin emalı komandası*
SET	Secure Electronic Transaction *Təhlükəsiz elektron tranzaksiya*
SF	Security Function *Təhlükəsizlik funksiyası*
S-FTP	Secure File Transfer Protocol *Təhlükəsiz fayl ötürmə protokolu*
S-HTTP	Secure HyperText Transfer Protocol *Təhlükəsiz hipermətn ötürməsi protokolu*
SHA	Secure Hash Algorithm *Təhlükəsiz heş alqoritmi*
SHS	Secure Hash Standard *Təhlükəsiz heş standartı*
SID	Security ID *Təhlükəsiz ID*
SIM	Subscriber Identity Module *Abunəçini identifikasiya modulu*

SIEM	Security Information and Event Management *İnformasiya təhlükəsizliyi məlumatlarının və hadisələrinin idarə edilməsi*
SKIP	Simple Key-management for Internet Protocols *Internet protokolu üçün sadə açar idarəetməsi*
SLA	Service Level Agreement *Xidmət səviyyəsi razılaşması*
SLIP	Serial Line Internet Protocol *Ardıcıl kanal üçün İnternet protokolu*
SMB	Server Message Block *Server məlumatı bloku*
SMIB	Security Management Information Base *Təhlükəsizliyi idarəetmə məlumatları bazası*
SMTP	Simple Mail Transfer Protocol *Sadə poçt ötürmə protokolu*
SNMP	Simple Network Management Protocol *Sadə şəbəkə idarəetməsi protokolu*
SOAP	Simple Object Access Protocol *Sadə obyekt girişi protokolu*
SOF	Strength of Function *Təhlükəsizlik funksiyasının dayanıqlığı*
SPC	Software Publisher Certificate *Proqram təminatı istehsalçısının sertifikatı*
SPI	Security Parameters Index *Təhlükəsizlik parametrləri indeksi*
SPIM	SPam through Instant Messaging Ani ismarıclarla spam
SPIT	SPam over Internet Telephony *Internet telefon üzərindən spam*
SPKI	Simple Public Key Infrastructure *Sadə açıq açar infrastrukturu*
SQL	Structured Query Language *Strukturlaşdırılmış sorğu dili*
SSL	Secure Socket Layer *Təhlükəsiz soket səviyyəsi*
SSM	System Security Manager *Sistem təhlükəsizliyi meneceri*

SSO	1. Special Security Officer *Xüsusi təhlükəsizlik meneceri* 2. System Security Officer *Sistem təhlükəsizliyi meneceri*
SSPI	Security Support Provider Interface *Təhlükəsizliyə dəstək provayderi üçün interfeys*
ST	Security Target *Təhlükəsizlik hədəfi*
STAT	State Transition Analysis Tool *Vəziyyət keçidi analizi aləti*
STP	Shielded Twisted Pairs *Qorunan dolama naqillər*
STU	Secure Telephone Unit *Təhlükəsiz telefon vahidi*
STU III	Secure Telephone Unit Third Generation *Üçüncü nəsil Təhlükəsiz telefon bloku*
S/WAN	Secure Wide Area Network *Təhlükəsiz qlobal şəbəkə*

T

TACACS	Terminal Access Controller Access Control System *Terminal giriş dispetçeri girişi idarəetmə sistemi*
TAXII	Trusted Automated Exchange of Indicator Information *Kiber-təhdid məlumatlarının avtomatlaşdırılmış etibarlı mübadiləsi*
TCB	Trusted Computing Base *Etibarlı Hesablama Bazası*
TCP/IP	Transmission Control Protocol/Internet Protocol *Ötürməyə nəzarət protokolu/ internet protokolu*
TCSEC	Trusted Computer System Evaluation Criteria *Etibar edilən kompüter sistemini qiymətləndirməsi meyarları*
TDMA	Time Division Multiple Access *Vaxt bölgülü çoxsaylı giriş*
TFS	Traffic Flow Security *Trafik axınının təhlükəsizliyi*
TFTP	Trivial File Transfer Protocol *Trivial fayl ötürməsi protokolu*
TKIP	Temporal Key Integrity Protocol

	Müvəqqəti açarın tamlığı protokolu
TLP	Traffic Light Protocol *Svetofor protokolu*
TLS	Transport Layer Security *Nəqliyyat səviyyəsinin təhlükəsizliyi*
TNI	Trusted Network Interpretation *Etibar edilən şəbəkə interpretasiyası*
TOC/TOU	Time Of Check versus Time Of Use *İstifadə vaxtı ilə yoxlama vaxtının müqayisəsi*
TOE	Target of Evaluation *Qiymətləndirmə hədəfi*
TPEP	Trusted Products Evaluation Program *Etibar edilən məhsulların qiymətləndirilməsi proqramı*
TRA	Threat and Risk Assessment *Təhdidin və riskin qiymətləndirilməsi*
Triple-DES	Triple Data Encryption Standard *Üç qat məlumat şifrləməsi standartı*
TS	Top Secret *Tam məxfi*
TSA	Time-Stamping Authority *Vaxt möhürü mərkəzi (xidməti)*
TSF	TOE Security Functions *TOE təhlükəsizlik funksiyası*
TSP	TOE Security Policy *TOE təhlükəsizlik siyasəti*
TTP	Trusted third party *Etibar edilən üçüncü tərəf*
	U
UART	Universal Asynchronous Receiver Transmitter *Universal asinxron qəbuledici-ötürücü aparat*
UDP	User Datagram Protocol *İstifadəçi dataqram protokolu*
UID	User ID *İstifadəçi identifikatoru*
UKAS	United Kingdom Accredited Service *Birləşmiş Krallıq Akkreditasiya Xidməti*
UPS	UninterruptiblePowerSupply

	Fasiləsiz elektrik enerjisi təchizatı
URL	Universal Resource Locator *Universal resurs ünvanı*
UTC	UniversalTimeCoordinated *Razılaşdırılmış universal vaxt*
UUCP	UNIX to UNIX Copy Program *UNIX-dən UNIX-ə surətçıxarma proqramı*

V

VBA	Visual BASIC Application *Tətbiqi proqramlar üçün vizual BASIC*
VDL	Vulnerability Descriptive Language *Boşluqları təsvir dili*
VDSL	Very High Bit-Rate Digital Subscriber Line *Çox yüksək bit sürətli rəqəmsal abunə xətti*
VEL	Vulnerability Exploit Language *Boşluqları istismar dili*
VLAN	Virtual Local Area Network *Virtual lokal şəbəkə*
VM	Virtual Machine *Virtual maşın*
VoIP	Voice over Internet Protocol *Internet protokolu üzərindən səs*
VPN	Virtual Private Network *Virtual xüsusi şəbəkə*

W

WAN	Wide-Area Network *Qlobal şəbəkə*
WAP	Wireless Application Protocol *Simsiz tətbiqi proqram protokolu*
WEP	Wired Equivalent Privacy *Naqilli şəbəkəyə ekvivalent gizlilik*
WIDS	Wireless IDS *Simsiz IDS*
WINS	Windows Internet Naming Service *Windows İnternet adları xidmət*

WLAN	Wireless Local Area Network *Simsiz lokal şəbəkə*
WPA	Wi-Fi Protected Access Təhlükəsiz Wi-Fi girişi
WSH	Windows Script Host *Windows skript hostu*
WTLS	Wireless Transport Layer Security *Simsiz nəqliyyat səviyyəsi təhlükəsizliyi*
WWW	World Wide Web *Ümumdünya hörümçək toru*

X

XACML	XML Access Control Markup Language *Girişi idarəetmə üçün XML nişanlama dili*
XAUTH	Extended Authentication *Geniş autentifikasiya*
XKMS	XML Key Management Service/Specification *XML açar idarəetmə xidməti/spesifikasiyası*
XSS	Cross-site scripting *Saytlararası skript*

0-9

3A	Authentication, authorization and accounting *Autentifikasiya, avtorizasiya və audit*
3DES	Triple DES *Üçqat DES*
8lgm	8 Little Green Men *8 kiçik yaşıl adam*

Ədəbiyyat

1. Azərbaycan dilinin qloballaşma şəraitində zamanın tələblərinə uyğun istifadəsinə və ölkədə dilçiliyin inkişafına dair Dövlət Proqramı. 9 aprel 2013-cü il.
2. Y.N.İmamverdiyev, İnformasiya təhlükəsizliyinin terminoloji problemləri. İnformasiya cəmiyyəti problemləri, 2014, No. 1, səh. 43-49.
3. Əliquliyev R.M., İmamverdiyev Y.N., İnformasiya təhlükəsizliyi insidentləri. Bakı: "İnformasiya Texnologiyaları" nəşriyyatı, 2012, 219 səh.
4. V. Qasımov, İnformasiya təhlükəsizliyinin əsasları. Dərslik. 2009.
5. AZS 420-2010 (ISO/IEC 2382-8) "İnformasiya Texnologiyaları – Hissə 8 – Təhlükəsizlik".
6. AZS 493-2010 (ISO/IEC TR 18044-2007) İnformasiya texnologiyası – Təhlükəsizliyin təmin edilməsinin metod və vasitələri – İnformasiya təhlükəsizliyi insidentlərinin idarə olunması".
7. AZS 494-2010 (ISO/IEC 27001-2005) İnformasiya Təhlükəsizliyi. Təhlükəsizlik metodları. İnformasiya təhlükəsizliyinin idarə edilməsi sistemləri. Tələblər.
8. С. Мак-Клар, Дж. Скембрей, Дж. Курц, Секреты хакеров. Безопасность сетей - готовые решения. 4-е издание. М.: ТД Вильямс, 2004. 656 с.
9. В. Ярочкин, Информационная безопасность. Учебник для вузов. М.: Академический Проект, Мир, 2008. 544 с.
10. Н. Г. Милославская, М. Ю. Сенаторов, А. И. Толстой, Управление рисками информационной безопасности. 2-е изд. 2014. 130 с.
11. А. А. Бирюков, Информационная безопасность: Защита и нападение. М.: ДМК Пресс, 2012. - 474 с.
12. NCSC-TG-004 Glossary of Computer Security Terms, National Computer Security Center, 1988.

13. R. Kissel (ed.) NIST IR 7298, Glossary of Key Information Security Terms. Revision 2. May 2013.
14. B. Schell, C. Martin, Webster's New World Hacker Dictionary. Wiley Publishing. 2006.
15. Glossary of Security Terms. http://www.sans.org/security-resources/glossary-of-terms/