ŞƏBƏKƏNIN TƏHLÜKƏSIZLIK KONSEPTLƏRI

Mündəricat

İnformasiya təhlükəsizliyi: əsas anlayışlar

- **Kompüter şəbəkələrinin (KŞ) geniş istifadəsi informasiya təhlükəsizliyi və mühafizə məsələlərinə diqqətin artırılmasını tələb edir.**
- **Çünki, KŞ-də saxlanılan və emal olunan informasiya resurslarının məhv edilməsi və onun müvəqqəti əlçatan olmaması və ya icazəsiz istifadəsi həmin resursların sahibinə ciddi maddi ziyan vura bilər.**
- **İnformasiyanın və şəbəkə infrastrukturunun təhlükəsizliyini təmin edən həllərin istifadəsi KŞ-nin istifadəsinin effektivliyini artırar.**

İnformasiya təhlükəsizliyi: əsas anlayışlar

- **İnformasiya təhlükəsizliyi milli, korporativ və ya şəxsi təhlükəsizliyin ən vacib aspektlərindən biridir.**
- **Hazırda informasiya təhlükəsizliyinin vahid tərifi yoxdur. "İnformasiya təhlükəsizliyi" söz birləşməsi müxtəlif kontekstlərdə müxtəlif məna kəsb edə bilər.**
- **Məsələn, informasiya təhlükəsizliyi dedikdə cəmiyyətin informasiya mühitinin vətəndaşların, təşkilatların və dövlətin maraqları naminə formalaşması və inkişafını təmin edən mühafizəlilik vəziyyəti başa düşülür.**

İnformasiya təhlükəsizliyi: əsas anlayışlar

- **Ayrıca təşkilat və ya müəssisə səviyyəsində informasiya təhlükəsizliyinə informasiyanın icazəsi olmayan şəxslərin təsadüfi və ya qəsdli girişindən, əldə edilməsindən, üstünün açılmasından, modifikasiya olunmasından və ya məhv edilməsindən mühafizəsi kimi baxılır.**

- **Şəxsiyyətin informasiya təhlükəsizliyinin təmin edilməsi onun obyektiv informasiya almaq hüququnu bildirir və nəzərdə tutur ki, insanın müxtəlif mənbələrdən aldığı informasiya onun şəxsiyyətinin azad formalaşmasına və inkişafına mane olumur.**

İnformasiya təhlükəsizliyi: əsas anlayışlar

- **İnformasiya təhlükəsizliyi və mühafizəsi ilə bağlı problemlərin analizi zamanı nəzərə almaq lazımdır ki, informasiya təhlükəsizliyi və mühafizəsi informasiya texnologiyalarının tərkib hissəsidir.**

- **Kompüter vasitəsi ilə yaradılan, yadda saxlanılan, emal olunan və ötürülən informasiyanın təhlükəsizliyi və mühafizəsi KŞ-nin bütün tərkib hissələrinin və birinci növbədə ən zəif həlqənin təhlükəsizliyi və mühafizəliliyi ilə təyin olunur.**

İnformasiya təhlükəsizliyi: əsas anlayışlar

- **İnformasiya təhlükəsizliyi – informasiya və ona xidmət edən infrastrukturun sahibi və ya istifadəçilərinə yolverilməz ziyan vura bilən, təbii və ya süni xarakterli, təsadüfi və ya qəsdli təsirlərdən informasiya və ona xidmət edən infrastrukturun mühafizəliliyidir.**

- **İnformasiyanın mühafizəsi – informasiya təhlükəsizliyinin təmin edilməsinə yönəlmiş tədbirlər kompleksidir.**

Mühafizə predmeti

- **KŞ-də mühafizə predmeti informasiya, verilənlər və şəbəkə infrastukturudur.**

- **Şəbəkə infrastrukturunun təhlükəsizliyi dedikdə bütün aparat və proqram komponentlərinin, o cümlədən kompüterlərin, kommunukasiya avadanlıqlarının, şəbəkə əməliyyat sistemlərinin, şəbəkə tətbiqlərinin, əlaqə kanallarının və s. təhlükəsizliyi başa düşülür.**

Mühafizə predmeti

- **“İnformasiya” anlayışı elmin əsas anlayışlarından biridir.**
- **Maddə, enerji, fəza və zaman kimi anlayışlarla yanaşı informasiya dünyanın müasir elmi mənzərəsinin əsasını təşkil edir.**
- **İnformasiya anlayışını daha sadə anlayışlar vasitəsi ilə müəyyən etmək olmaz.**
- **İnformasiya sözünə texnologiyada, elmdə və həyat situasiyalarında müxtəlif məna verilir.**
- **Məsələn, texnikada informasiya dedikdə işarələr və ya siqnallar formasında ötürülən məlumatlar başa düşülür.**

Mühafizə predmeti

- **İnformasiya təhlükəsizliyinin təmin edilməsində hüquqi tədbirlərin önəmini nəzərə alaraq informasiyanın "İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında" qanunda verilmiş, aşağıdakı tərifindən istifadə ediləcək.**

- **İnformasiya – təqdimat formasından asılı olmayaraq şəxslər, əşya, fakt, hadisə və proseslər haqqında məlumatlardır.**

Mühafizə predmeti

- **İnformasiyanın bir sıra xüsusiyyətləri:**

- **İnformasiya maddi deyil: İnformasiyanın qeyri-maddiliyi o mənada başa düşülür ki, onun parametrlərini məlum fiziki metodlarla və cihazlarla ölçmək olmaz.**

- **İnformasiyanın kütləsi, enerjisi və s. olmur.**

Mühafizə predmeti

- İnformasiya maddi daşıyıcıların köməyi ilə saxlanır və daşınır.
- İnsan beyni, səs və elektromaqnit dalğaları, kağız, maşın daşıyıcıları (maqnit və optik disklər, maqnit lentləri və barabanlar) və s. belə daşıyıcılardır.
- Kompüter və KŞ-də informasiya ancaq iki simvoldan (0 və 1) ibarət olan ikilik əlifba ilə təsvir edilir.
- Belə əlifbanın istifadəsi KŞ-nin texniki realizasiyasını sadələşdirir. Müasir KŞ-də rəqəmli informasiya ilə bərabər mətn informasiyaları da emal edilir.

İnformasiyanın qiyməti

- **İnformasiyanın qiyməti onun mühafizəsi haqqında istənilən qərarın qəbul edilməsi kriteriyasıdır.**
- **Ancaq o informasiya mühafizə olunur ki, onun qiyməti var.**
- **Baxmayaraq ki, informasiya nəzəriyyəsinin üsullarından istifadə edilərək informasiyanın qiymətləndirilməsinə çoxlu sayda cəhdlər edilmişdir, onun qiymətləndirilməsi meyarı çox subyektivdir.**
- **İnformasiyanın qiyməti onun sahibi üçün faydalılıq dərəcəsi ilə müəyyən edilir.**
- **Həqiqi (gerçək) informasiyaya sahib olma onun sahibinə üstünlüklər verir.**

İnformasiyanın qiyməti

- İnformasiyanın qiymətləndirilməsi üçün onun təkcə qiymətinə görə deyil, həmçinin vacibliyi dərəcəsinə görə kateqoriyalara bölünməsi tələb olunur.
- İnformasiyanın vacibliyi dərəcəsinə görə aşağıdakı bölgüləri məlumdur:
  - əvəzolunmaz həyatı vacib informasiya müəssisənin fəaliyyəti üçün mövcudluğu zəruridir;
  - vacib informasiya – o informasiyadır ki, əvəz və ya bərpa oluna bilər, lakin bərpa prosesi çox çətindir və böyük xərclər tələb edir;
  - faydalı informasiya – o informasiyadır ki, bərpa etmək çətindir, lakin onsuz müəssisə effektiv fəaliyyət göstərə bilər;
  - əhəmiyyəti az olan informasiya – elə informasiyadır ki, bir daha müəssisəyə gərəkli olmasın.

İnformasiyanın qiyməti

- **Həyatda informasiyanın bu kateqoriyalara aid edilməsi çox çətin məsələdir, çünki eyni informasiya müəssisənin çoxlu bölmələri tərəfindən istifadə oluna bilər və onlardan hər biri bu informasiyanı müxtəlif kateqoriyaya aid edə bilər.**
- **Bundan başqa vaciblik kateqoriyası və informasiyanın qiyməti zamana görə dəyişir və müxtəlif istehlakçı qruplarının və potensial pozucuların münasibətlərindən asılıdır.**

İnformasiyanın qiyməti

- **İnformasiya mülkiyyət obyektidir və KŞ-nin sahibinin, dövlətin, müəssisənin, firmanın xüsusi və ya ictimai, insanın isə şəxsi mülkiyyəti ola bilər.**
- **İnformasiyanın və KŞ-nin resurslarının sahibləri müxtəlif şəxslər və müəssisələr ola bilər.**
- **Sahibkarlıq hüquqlarının təmin edilməsi informasiya təhlükəsizliyini təmin edir.**
- **Beləliklə iddia etmək olar ki, resursların mühafizəsi heç də həmişə informasiyanın mühafizəsinə təminat vermir.**

İnformasiya mühafizəsi obyekti KŞ-dir

- **KŞ verilənlərin ötürülməsi kanalları vasitəsi ilə birləşmiş kompüterlər məcmusu olaraq, istifadəçilərə informasiya mübadiləsi imkanı verir və şəbəkənin proqram, texniki, informasiya resurslarına girişi və şəbəkə xidmətlərdən istifadəni təmin edir.**

İnformasiya mühafizəsi obyekti KŞ-dir

- Ümimi halda isə, KŞ informasiyanın avtomatlaşdırılmış toplanması, saxlanması, emalı, ötürülməsi və qəbulu üçün nəzərdə tutulmuş aparat və proqram vasitələri kompleksidir və aşağıdakı sistemləri əhatə edir:
  - kompüterlər;
  - kommunukasiya avadanlıqları;
  - şəbəkə əməliyyat sistemləri;
  - şəbəkə tətbiqləri (network applications);
  - əlaqə kanalları;
  - hesablama kompleksləri və sistemləri;
  - hesablama şəbəkələri (lokal, regional və qlobal).

İnformasiya mühafizəsi obyekti KŞ-dir

- **Qeyd etmək lazımdır ki, KŞ insan-maşın sistemləri sinfinə aiddir və xidmətçi heyət, istifadəçilər də informasiya daşıyıcılarıdır.**
- **Buna görə icazəsiz təsirlərdən təkcə qurğu və daşıyıcıları deyil, həmçinin xidmətçi heyəti və istifadəçiləri də mühafizə etmək lazımdır.**
- **KŞ-də informasiya təhlükəsizliyi problemlərini həll edərkən, həmçinin sistemin insan amilinin ziddiyyətli olmasını nəzərə almaq lazımdır.**

İnformasiya mühafizəsi obyekti KŞ-dir

- **Xidmətçi heyət və istifadəçilər informasiyaya icazəsiz təsirin həm obyekti, həm də mənbəyi ola bilərlər.**
- **İcazəsiz təsir "obyekti" anlayışına təkcə KŞ-nin informasiya resursları, aparat, proqram vasitələri, xidmətçi heyət, istifadəçilər deyil, həmçinin otaqlar, binalar və hətta binalara bitişik olan ərazi də daxildir.**

İnformasiya mühafizəsi obyekti KŞ-dir

- Mühafizəli KŞ-in üç aksiomu:
- Aksiom 1. Mühafizəli KŞ-də subyektin obyekt üzərində əməliyyatlarına həmişə nəzarət edən aktiv komponent (subyekt) mövcuddur. Bu komponent faktiki olaraq müəyyən təhlükəsizlik siyasətinin reallaşdırılmasına cavabdehdir.
- Aksiom 2. Mühafizəli KŞ-də obyektlər üzərində əməliyyatların həyata keçirilməsi üçün subyektin obyektlə apara biləcəyi icazə verilən və qadağan olunmuş əməliyyatlar haqqında əlavə məlumatlar lazımdır.
- Aksiom 3. KŞ-də informasiya təhlükəsizliyinin bütün məsələləri subyektlərin obyektlərə daxil olması ilə təsvir olunur.

İnformasiya təhlükəsizliyinin əsas aspektləri

- **İnformasiya təhlükəsizliyi çoxcəhətli olduğuna görə onun təmin edilməsi sistemli, kompleks yanaşma tələb edir.**
- **KŞ-nin informasiya təhlükəsizliyinə emal olunan informasiya resurslarının və şəbəkə infrastrukturun əlyetənliyinin, bütövlüyünün və konfidensiallığının təmin edilməsi ilə nail olunur.**

İnformasiya təhlükəsizliyinin əsas aspektləri

- **Əlyetənlik – yol verilən vaxt ərzində lazım olan informasiya xidmətinin əldə edilməsi imkanıdır.**
- **Bütövlük – informasiyanın aktuallığı və ziddiyyətsizliyi, həmçinin onun məhv edilməsindən və icazəsiz dəyişilmədən mühafizəliliyidir.**
- **Konfidensiallıq – informasiyaya sanksiyasız daxil olmadan mühafizədir.**

İnformasiya təhlükəsizliyinin əsas aspektləri

- **KŞ müəyyən informasiya xidmətlərinin alınması üçün yaradılır.**
- **Əgər müxtəlif səbəblərdən istifadəçilərə bu xidmətləri vermək mümkün olmursa bu informasiya münasibətləri subyektlərinə ziyan vurur.**
- **Buna görə də əlyetənliyi informasiya təhlükəsizliyi aspektlərinin ən vacibi kimi saymaq olar.**
- **Əlyetənliyin aparıcı rolu özünü müxtəlif idarəetmə sistemlərində məsələn, istehsalatın, nəqliyyatın və s. idarə edilməsi sistemlərində göstərir.**

İnformasiya təhlükəsizliyinin əsas aspektləri

- Bütövlük iki növə bölünür:
  - Statik-informasiya obyektlərinin dəyişməzliyi;
  - Dinamik-mürəkkəb əməliyyatların (tranzaksiyaların) korrekt yerinə yetirilməsi.
- Bütövlüyə dinamiki nəzarət vasitələri, məsələn, oğurluğu müəyyən etmək üçün maliyyə məlumatları axınının analizində istifadə olunur.
- Bütövlük o hallarda informasiya təhlükəsizliyinin vacib aspekti sayılır ki, informasiya vacib qərarların qəbul edilməsinə xidmət edir.

İnformasiya təhlükəsizliyinin əsas aspektləri

- Konfidensiallıq ən geniş öyrənilmiş informasiya təhlükəsizliyi aspektidir, lakin onun praktiki realizasiyası ciddi çətinliklərlə üzləşir.
- Birincisi, informasiyanın sızmasının texniki kanalları haqda məlumatlar açılmamışdır və buna görə də əksər istifadəçilər potensial risklər barədə təsəvvür yaratmaq imkanından məhrumdurlar.
- İkincisi, istifadəçi kriptoqrafiyası sahəsində çoxlu sayda qanunvericilik əngəlləri və texniki problemlər mövcuddur.
- Konfidensiallıq dövlət, kommersiya və digər sirlərin qorunmasında informasiya təhlükəsizliyinin ən vacib aspekti sayılır.

İnformasiya təhlükəsizliyinin əsas aspektləri

- **Təhdid (threat) – kiminsə maraqlarına ziyan vurmağa səbəb ola (gətirib çıxara) bilən potensial hadisə, hərəkət, prosesdir. Təhdidlər əsasən KŞ-də zəifliklərin olması nəticəsində yaranır.**
- **Təhdidin həyata keçirilməsi cəhdi hücum(attack) adlanır və belə cəhdi edən isə bədəməlçi adlanır.**
- **Bədəməlçinin qəsdli hərəkəti ilə əlaqədar olmayan, təsadüfi zaman anlarında realizə olunan təhdidlər təsadüfi və ya qəsdən törədilməyən təhdidlər adlandırılır.**

İnformasiya təhlükəsizliyinin əsas aspektləri

- **Zəiflik (vulnerability) – sistemin mühafizəsində boşluqdur və sistemin layihələndirilməsində, realizəsində və ya proqram təminatında səhvlərin nəticəsində meydana çıxır və sistemin təhlükəsizlik siyasətinin pozulması üçün istifadə edilə bilər.**
- **Zəiflik təhdidin meydana çıxmasını mümkün edir və hücumun yerinə yetirilməsi üçün potensial yoldur.**

İnformasiya təhlükəsizliyinin əsas aspektləri

- **İdentifikasiya (identification) istifadəçiyə (və ya müəyyən istifadəçinin adından fəaliyyət göstərən prosesə) özünü adlandırmağa (öz adını bildirməyə) imkan verir.**
- **Autentikasiya (authentication) vasitəsi ilə ikinci tərəf əmin olur ki, subyekt doğrudan da özünü qələmə verdiyi şəxsdir. Autentikasiya sözünün sinonimi kimi çox vaxt "həqiqiliyin yoxlanması" işlədilir.**

İnformasiya təhlükəsizliyinin əsas aspektləri

- Avtorizasiya (icazələrin idarə edilməsi) – KŞ-də subyektlərin (istifadəçi və proseslərin) obyektlər (informasiya və digər kompüter resursları) üzərində yetinə yetirə biləcəyi əməliyyatları müəyyən etməyə və onlara nəzarət etməyə imkan verir.
- İcazələrin məntiqi idarə edilməsi (icazələrin fiziki idarə edilməsindən fərqli olaraq) proqram vasitələri ilə realizə olunur.

İnformasiya təhlükəsizliyinin əsas aspektləri

- **Təhlükəsizlik siyasəti qiymətli informasiyanın idarə edilməsi, mühafizəsi və paylanmasını tənzimləyən normalar, qaydalar və praktiki üsullar toplusudur.**
- **Təhlükəsizlik siyasətinin təsviri, hətta sadə hallarda da böyük həcmdə olur.**
- **Çox sadə dildə desək – təhlükəsizlik siyasəti daxil olmanın idarə olunması qaydaları toplusudur.**
- **Təhlükəsizlik siyasəti həm icazəli, həm də icazəsiz daxil olmaları təyin edir.**

İnformasiya təhlükəsizliyinin əsas aspektləri

- **Daxilolma – subyekt-obyekt modelinin kateqoriyasıdır və subyektin obyekt üzərində əməliyyat həyata keçirməsi prosesini təsvir edir.**
- **Daxilolmanın idarə olunması subyektin obyekt üzərində həyata keçirə biləcəyi əməllərin spesifikasiya və nəzarət edilməsidir.**
- **Daxil olmanın əsas komponentləri: daxil olma hüququ, daxil olma obyekti, daxil olma subyekti, daxil olma növləri və s.**

İnformasiya təhlükəsizliyinin əsas aspektləri

- **Daxilolma obyekti – daxil olmanın müvafiq məhdudlaşdırma qaydaları ilə nizamlanan KŞ-nin və avtomatlaşdırılmış sistemlərin informasiya və digər resurslardır.**
- **Daxilolma subyekti – informasiya proseslərində hüquqi münasibətlərin iştirakçıları olan, hərəkətləri daxil olmanın məhdudlaşdırılması qaydaları ilə nizamlanan istifadəçilər və proseslərdir.**

İnformasiya təhlükəsizliyinin əsas aspektləri

- **Daxilolmanın məhdudlaşdırılması qaydaları – daxilolma subyektlərinin daxilolma hüquqlarını nizamlayan qaydalar toplusudur.**
- **Daxilolma hüququ – müəyyən edilmiş əməliyyatların aparılması məqsədilə müəyyən obyektə giriş üçün subyektə verilən icazədir.**

İnformasiya təhlükəsizliyinin əsas aspektləri

- **Protokollaşdırma KŞ-də baş verən hadisələr haqqında informasiyanın yığılması və toplanmasıdır.**
- **Hər bir xidmətin özünəməxsus mümkün hadisələr dəsti var, lakin istənilən halda onların xarici (digər xidmətlərin fəaliyyəti nəticəsində meydana çıxan hadisələr), daxili (xidmətlərin özlərinin fəaliyyəti nəticəsində meydana çıxan hadisələr) və kliyent (istifadəçilərin və inzibatçıların fəaliyyəti nəticəsində meydana çıxan hadisələr) hadisələrinə bölmək olar.**

İnformasiya təhlükəsizliyinin əsas aspektləri

- **Audit – toplanmış informasiyanın operativ, real zamanda və ya periodik (məsələn, gündə bir dəfə) analizidir.**
- **Qeyri-ştat vəziyyətin üzə çıxarılmasına avtomatik reaksiya verən operativ audit aktiv audit adlanır.**

İnformasiya təhlükəsizliyinin əsas aspektləri

- Protokollaşdırma və auditin realizasiyası aşağıdakı məsələləri həll edir:

- istifadəçilərin və inzibatçıların cavabdehliyini təmin edir;
- hadisələrin ardıcıllığının yenidən qurulması imkanının təmin edilməsi;
- informasiya təhlükəsizliyinin pozulması cəhdinin aşkar edilməsi;
- problemlərin aşkara çıxarılması və analizi üçün informasiya ilə təmin edilməsi.

Diqqətinizə görə təşəkkür edirəm!