AYTƏKİN İBRAHİMOVA
Bakı Dövlət Universiteti, "Konstitusiya hüququ" kafedrasının dosenti, hüquq üzrə fəlsəfə doktoru
aytakin_ibrahimli@mail.ru

İNFORMASİYA TƏHLÜKƏSİZLİYİ; TƏHLÜKƏSİZLİK VƏ İNFORMASİYA ANLAYIŞI

Açar sözlər: informasiya, informasiya təhlükəsizliyi anlayışı, informasiya təhlüksizliyinin əsas prinsipləri, informasiya təhlükəsizliyi və innovasiya

Ключевые слова: информация, концепция информационной безопасности, основные принципы информационной безопасности, информационная безопасность и инновации.

Keywords: information, concept of information security, basic principles of information security, information security and innovation

Keçmişdən bu günədək mübahisə edilən informasiyanın anlayışı çətindir, bundan başqa nəyin informasiya olduğu nəyin informasiya olaraq qəbul edilə bilməyəcəyi, inam və reallıq münasibətləri də hələ mübahisəlidir.

İnformasiya anlayışı, gizlilik bütünlük və əlçatanlıq prinsiplərinə əsaslanır. İnformasiyadan istifdə dərəcəsinə görə bu prinsiplər də öz aralarında fərqli əhəmiyyət dərəcələrinə bölünürlər. Çox əhəmiyyətli milli araşdırmaların aparıldığı bir təşkilatda öncəlik gizlilik prinsipinə verilmişdir. Orada yaranan informasiyada əlçatanlıq və informasiyanın bütünlüyü daha az əhəmiyyət kəsb etməkdədir. Media sahəsində öncəlik isə əlçatanlıqdadır. İnternet üzərindən yayın edən bir qurum üçün öncəlik informasiyanın qarşı tərəfə davamlı və ən sürətli şəkildə çatdırılmasıdır. Bəzən kiçik bir alt yazı digərlərindən fərqlənməyi bacara bilir. Verilən informasiyada gizlilik axtarılmaz, bütünlük gözlənilmədən qarşı tərəfə ötürülə bilər. Bir məhkəmə prosesində hakim üçün öncəlik bütünlük prinsipidir. Bəzən bu proses illərlə davam edir. Bəzi məsələlər ifadələr alınarkən gizliliyini itirə bilir. Məqsəd doğru məlumatlara əsaslanaraq həyati qərarlar vermək olduqda əldə ediləcək informasiyaları daha da əhəmiyyətli hala gətirir. İnformasiya fərqli mühitdə işlənərək baza formalaşdıra bilər. Əvvəllər ancaq danışaraq fərdlər arasında yaranan informasiya, yazının kəşfi ilə daha təsirli bir şəkildə əks olunmağa başladı. Arxiv anlayaşı da bu formada tarixdə bir yer tutdu. Bu gün informasiyanı kağız üzərində yazılı olaraq, danışaraq, elektron informasiya yığım cihazlarında (cd/dvd, usb və b.) internet üzərində virtual mühitdə və internet şəbəkəsi mühitində saxlaya bilirik. İnformasiya əldə etməkdə isə ilk növbədə mobil cihazlar, mətbuat, mesajlardan istifadə edilməkdədir. Fərqli mühitdə saxlanılan informasiyaları qorumaq üçün fərqli mütəxəssislər tələb olunursa, hamısı üçün ortaq informasiya təhlükəsizliyi standartlarını müəyyənləşdirmək isə yetərli olacaqdır. Bu informasiyanı saxlamaq qədər, səlahiyyətli olana, şəxslərin xidmətinə təqdim edə bilmək də olduqca əhəmiyyətlidir.

Müasir dövrümüzdə dövlət və qeyri/dövlət orqanları öz işlərini həyat keçirə bilmək üçün ciddi bir şəkildə informasiyadan istifadə edirlər. Zaman keçdikcə informasiyanın əhəmiyyəti artmış, sadəcə etibarlı bir şəkildə saxlanılması və əldə olunması ilə deyil, eyni zamanda bir yerdən başqa bir yerə ötürülməsi də qaçınılmaz bir ehtiyac halına gəlmişdir. İnformasiyaya olan bu bağlılıq informasiyanın mühafizəsi ehtiyacını da gündəmə gətirmişdir. Bu mə-

nada informasiya hər hansı bir orqanın sahib olduqları arasında çox əhəmiyyətli bir yerə sahibdir.

İnformasiya, təşkilatdakı digər varlıqlar kimi təşkilat üçün əhəmiyyət daşıyan və bu səbəblə də ən yaxşı bir şəkildə mühafizəyə ehtiyac duyan bir varlıqdır. İnformasiyaya yönələn hücumlar (təxribat edilməsi, silinməsi, bütünlüyünün və ya gizliliyinin zərər görməsi), informasiya infrastrukturunun pozulmasına və bu da özü ilə birlikdə işlərin axsamasına səbəb olmaqdadır. Bu baxımdan ilk növbədə əsas olaraq informasiya təhlükəsizliyi anlayışı və informasiya təhlükəsizliyi idarəetmə sistemləri üzərində dayanmaqla informasiya təhlükəsizliyi idarəetmə sistemlərinin tarixçəsi, yaranma müddəti və əsas komponentləri izah edilməlidir.

İnformasiya təhlükəsizliyi- dövlət və qeyri dövlət sektorunda işlərin davamlılığının təmin olunması, iş vaxtı yarana biləcək çatışmazlıqların aradan qaldırılması və gələcəkdə investisiyalardan faydanın artırılması üçün informasiyanın daha çox təhlükələrdən müdafiəsini təmin edir.

İnformasiya bir çox formada əldə oluna bilər. İnformasiya kağız sənədlər üzərində yazılı ola bilər, elektron formada saxlanıla bilər, poçt və ya elektron poçt formasında bir yerdən başqa bir yerə göndərilə bilər, ya da şəxslər arasında adi sözlərlə ifadə edilə bilər. İnformasiya hansı formada olursa olsun mütləq uyğun bir şəkildə müdafiə olunmalıdır. Bu səbəblə İnformasiya Təhlükəsizliyi İdarəetmə Sistemi tətbiq olunmalıdır.

Hər bir dövlət və qeyri dövlət orqanları öz funksiyalarına uyğun fəaliyyətlə məşğul olmalıdır, amma bu fəaliyyət zamanı da bir-birlərindən təcrid olunmadan birgə informasiya mübadiləsi çərçivəsində faəliyyət göstərməlidirlər ki, daha effektiv nəticə əldə edə bilsinlər. Unutmamaq lazımdır ki, hər biri bir-birinin informasiyasına bağlıdırlar. Təşkilat daxilində hər kəs bir müştəri, bir idarəedici və bir tədarükçü yəni 3 fərqli rola malikdir.

İnformasiya təhlükəsizliyindən danışmaq üçün ilk növbədə informasiyanın nə olduğunu, əhəmiyyətini və hansı səbəbə görə təhlükəsizliyin təmin olunmasının vacibliyi məsələsi kimi əsas anlayışları izah etmək lazımdır.

İnformasiya sözünün Azərbaycan dilinin izahlı lüğətindəki mənası belədir: müəyyən sahəyə dair məlumatlar, hər hansı xüsusi biliklər. İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında Azərbaycan Respublikası Qanununun 2-ci maddəsində isə informasiyaya belə bir anlayış verilmişdir: informasiya-yaranma tarixindən, təqdimat formasından və təsnifatından asılı olmayaraq istənilən fəaliyyət nəticəsində yaradılan, yaxud əldə olunan faktlar, rəylər, bilgilər, xəbərlər və ya digər xarakterli məlumatlar başa düşülür. [15] Türk dil təşkilatı informasiyaya belə bir anlayış vermişdir ki, informasiya insan zəkasının fəaliyyəti nəticəsində meydana gələn fikir məhsulu, məlumatdır. Buna görə də informasiyaya bir məhsul olaraq baxıldıqda, həm insan, həm dövlət, həm də qeyri-dövlət qurumları üçün necə bir əhəmiyyətə sahib olduğu ehtimal edilə bilər.

İnformasiyaya eyni zamanda bəlli bir məqsəd daxilində təşkilatı, əsaslı bir məzmuna malik olan məlumatlar kimi də anlayış vermək olar.

İnformasiyanın olduğu mühit müxtəlifdir. Dövlət və qeyri-dövlət orqanlarında, təşkilatlarda bu məlumatlar daha çox kompyuterin yaddaşında olur. Ancaq bununla yanaşı informasiya insan yaddaşında, sosial mühitdə, yazılı kağız üzərində də mövcuddur. Bu səbəblə də bu cür mühitdə informasiyanın müdafiə olunması, onun təhülkəsizliyi məsələsi çox böyük əhəmiyyət daşımaqdadır.[16]

İnformasiyanı mühazifə edən bir qurum, informasiyanın mövcud olduğu yerləri təsnifləndirməli və necə bir müdafiə vasitəsindən istifadə edəcəyinə dair özündə plan hazırlamalıdır. Hansı cəbhədən baxılarsa baxılsın informasiya hər bir orqanın, təşkilatın əsas sərmayələrindən biridir. Fərdlər nöqteyi nəzərindən yanaşsaq isə informasiya, əsasən gizli qalması vacib olan və ya əlçatan olması hədəflənən və bir bütün daxilində istifadəliliyi vacib olan bir vasitədir. [5, s.7]

İnformasiya təhlükəsizliyinin əsas prinsipləri:

Informasiya təhlükəsizliyində tətbiq olunan əsas nəzarət (prinsiplər), bir çox risqə qarşı tətbiq olunan nəzarətlərdən belə əvvəl qoruya bilmə qabiliyyətinə malikdir. Hər fəaliyyətə yanaşmada açar rolunu oynayan bu prinsiplərdən ən çox istifadə olunanı bunlardır: ən az səlahiyyətli, icazə verilmədikcə hər şey qadağa olunan, vəzifələrin fərqləndiyi, istifadə olunmayan elementlərin kənarda tutulması və istifadə oluna bilən təhlükəsizliyin tarazlığı prinsipləridir. [9,s.173]

1. Ən az səlahiyyət

Bir şəxsə, bir sistemə, bir təşkilata səlahiyyət verilərkən o səlahiyyətin reallaşdırılması planlanan işi görümək üçün ən az əhatəyə sahib olduğundan əmin olunmalıdır. Misal üçün bir sistem daxilində sadəcə bir sənədi oxumaq üçün səlahiyyətə ehtiyacı olan bir şəxsə eyni zamanda o sənədi hazırlamaq haqqı da verilmədir. Oxşar formada şəxsin bütün sistemdə idarəedici hüququna sahib olmaması olduqca vacibdir.[8, s.257]

2. İcazə verilməyən hər şey qadağandır

Bir sistemin səlahiyyətləri müəyyənləşdirilərkən "hər şey qadağandır" yanaşması ilə əhatəli olması vacibdir. Bunun sayəsində nəzərdən qaçan səlahiyyətlərin önünə keçilərək sadəcə ehtiyac duyulan səlahiyyətlər verilmiş olar. Buna ən bariz nümunə Firewall ("təhlükəsizlik divarı") üzərində edilən Port filtirləmə və IP filtirləmə vasitələri göstərilə bilər. Bir çox təhlükəsizlik divarı bu prinsipə bağlı olaraq fəaliyyət göstərməkdədir. Beləcə də nəzərdən qaçabiləcək Port protokol və IP adresləri daha ən başdan qadağan olunar.

3. Vəzifələrin fərdiliyi

Bir işi həyata keçirərkən işi görən və bu işin görülməsinə icazə verən mexanizm ayrı olmalıdır. İşi görən eyni zamanda edəcəyi iş üçün bir icazə gözləmirsə, ya da bir başqa deyimlə icazəni özü verirsə, bu vəziyyət səhvin yaranmasına və ya işdə sui istifadə hallarına səbəb olacaqdır.

4. İstifadə olunmayan elementlərin kənarda tutulması

İcazə verilməyən hər şey qadağandır prinsipinin bir hissəsi sayıla biləcək bu prinsip "İstifadə olunmayan elementlərin kənarda tutulması" prinsipidir. Bu prinsipin məqsədi hücuma açıq olan sahələrin sayının azaldılmasıdır. İstifadə olunmayan bir sistem və ya bir məlumat, içində mövcud olan zəiflik səbəbilə istifadə olunan və əhəmiyyətə sahib olan başqa bir sistem və ya məlumata təsir edəcəkdir. Bu prinsipə verilə biləcək ən geniş yayılmış nümunələrin başında istifadə olunmayan vasitələrin aradan qaldırılması və Portların ötürülməsi gəlməkdədir. [9, s.227]

5. İstifadəlilik və təhlükəsizlik tarazlığı

İnformasiya təhlükəsizliyinin əsas anlayışları arasında yer tutan mövzulardan biri də istifadəlilik-təhlükəsizlik tarazlığıdır. Bu tarazlıq tərəzinin iki tərəfinə qoyulmuş ağırlıqlara və ya riyaziyyatdakı tərs mütənasibliyə bənzədilir. İstifadəliliyin artdığı hər ssenaridə təhlükəsizliyin bir təhlükə altında olması vəziyyəti ortaya çıxa bilər. İstifadəlilik və təhlükəsizlik tarazlığının anlaşılması üçün bir nümunə göstərsək daha yaxşı olardı:

Müasir dövrümüzdə internet bankçılıq üçün bir çox mərhələlərdən keçilməli olan formalar doldurulmalıdır. Bu təsdiqedici addımlardan bir də çoxmərhələli təsdiqləmə (Multi Factor Authentication) ilə reallaşmaqdadır. Bu təsdiq istifadəçinin bildiyi bir şeyə, özünə və ya sahib olduğu bir fakta əsaslanmaqdadır. Bir sıra digər təsdiqlər isə sadəcə istifadəçinin bildiyi faktlara əsaslanmaqdadır. (PİN, parol, gizli suala cavab və s.) Sadəcə bir istifadəçi adı və paroldan istifadə edərək giriş edilən İnternet Bank xidməti günümüzdə demək olar ki, yoxdur. Ən azı 2 parol və ya əl telefonuna gələn bir PİN (Personal İdentification Number) kodunun soruşulduğu suallardan ibarətdir. Bu vəziyyət İnternet Banka giriş edə bilmək üçün sərf edilən səyi artırmaqla, bu xidməti açmaq üçün vacib olan tələblərdəndir. . [10, s.189]

İnformasiya təhlükəsizliyinin innovasiya ilə əlaqəsi.

İnformasiya, günümüzdəki təşkilat sərmayələrindən birini yaratmaqdadır. İnnovasiya isə təşkilatın sahib olduğu sərmayənin və mənfəətin artırılması və beləcə də rəqabətdə bir addım önə çıxılması nəticələrini hədəfləməkdədir. İnformasiya təhlükəsizliyi informasiyanın müdafiəsini hədəfləməkdədir, dolayısı ilə informasiya təhlükəsizliyi hər hansı bir müəsissəyə aid bir sərmayənin müdafiəsini qarşısına məqsəd qoymaqdadır. İnnovasiyanın məqsədi sərmayənin müdafiəsi və artırılması ilə mənfəətin müdafiəsi və artırılmasıdırsa, informasiya təhlükəsizliyi də əslində bu məqsədlərə xidmət etməkdədir. [6, s.11]

İnformasiya təhlükəsizliyi müəsissənin bir sərmayəsi olan informasiyanın gizliliyinin, əlçatanlığının və bütünlüyünün müdafiəsi məqsədini hədəfləməkdədir. İnformasiyanın bir sərmayə olması səbəbilə müdafiə altına alınmış olması, müəsissələr üçün əldə ediləcək maddi gəlirlərdən biridir. İnnovasiya mövcud quruluşun davam etdirilməsi və ya daha da yaxşıya çatdırılması məqsədini da-

şıyır. Bir təşkilatda informasiya təhlükəsizliyinə aid bir idarəetmə sisteminin həyata keçirilməsi elə özü-özlüyündə innovasiyadır. Bu nümunədə innovasiya informasiya təhlükəsizliyini yaradır. İnformasiya təhlükəsizliyi isə sərmayənin qorunmasını və karlılığının artırılmasına yardım etməyi hədəfləyir. İnnovasiyanın təsirlərinin ən rahat görülə bilən sektorlarının başında texnologiya sektoru gəlməkdədir. Texnologiya sektoru digər sektorlarla müqayisə edildikdə dəyişikliyə, innovasiyaya daha açıq olan sektordur. Hər yeniliyin bir dəyişiklik gətirməsi vəziyyəti hər dəyişikliyin də yeniliyə açıq olması vəziyyətini özü ilə birlikdə gətirməkdədir. Bu səbəbdən texnologiya sektorları üçün innovasiya bir vasitədən çox bir məqsəd halına gəlmişdir. İnnovasiya məsələsində geridə qalan təşkilat, bazarda yerini çox sürətlə itirmək təhlükəsi ilə qarşı-qarşıya qalır. Onu da qeyd edək ki, texnologiya sektorunda bu itkilər saniyələr içərisində olur. Sürətin və yeniliyin daha çox olduğu sektorda innovasiya ən vacib faktorlardan biri olaraq rol oynamaqdadır. Bunun bir nümunəsi Sony firması üçün göstərilə bilər.

Sony şirkəti istehsal etdiyi Playstation adlı oyunların pirat olaraq istifadəsinin qarşısını almaq üçün təhlükəsizlik tədbirlərini təkmilləşdirmişdir. Bu təhlükəsizlik tədbirləri sayəsində sadəcə orijinal olaraq satın alınmış oyunlar Playstationla oynanıla bilir və bu oyunların kopyaları edilməməkdədir. İnformasiya təhlükəsizliyinin texniki olaraq reallaşdığı bu vəziyyətdə Sony birgə çalışdığı oyun firmalarının kar əldə etməsi ilə bərabər ticari qazanc əldə etməkdədir. Bu günədək Sony istehsal etdiyi Playstation oyunlarının hər birində kopyalamaya qarşı təhlükəsizlik tədbirləri yer almışdır. Ancaq Playstation 1 və Playstation 2 adlı məhsullarda bu kopyalama müdafiəsi sürətli bir şəkildə piratçılar tərəfindən oğurlanmış və kopya oyunlar bazara piratçılar tərəfindən təqdim olunmuşdur. Sony bu vəziyyətdə həll yolu olaraq texniki təhlükəsizlik üzərində işləyərək bazara təqdim etdiyi Playstation 3 oyununda bu yenilikləri tətbiq etmişdir. [17]

Tətbiq etdiyi yeniliklərə görə rəqiblərinin əksinə Sony öz məhsulunu 4 il boyunca piratların hücumundan qoruya bilmişdir. Lakin 4 ilin sonunda digər məhsulları kimi yeni oyun da pirat hücumuna məruz qalmışdır. Bu müddət Sony-nin rəqiblərinə nisbətən informasiya təhlükəsizliyi təmin edən bir şirkət kimi uğur əldə etməsi idi. İnformasiya təhlükəsizliyində zaman ən vacib meyardır. Belə ki, informasiya təhlükəsizliyi zamanın tələblərinə və dəyişən şərtlərə cavab verməyi hər zaman hədəfləyir. Günümüzdə informasiya təhlükəsizliyinə əhəmiyyət verən dövlətlər informasiya təhlükəsizliyinin istifadə sahələrində innovasiyaya gedərək ölkələrinin milli maraqlarını qorumağı hədəfləməkdədir. 27 may 2011-ci ildə Türkiyənin Sabah qəzeti belə bir məqalə yayımladı: Çin dövləti tarixi bir çıxışla ilk dəfə "super elit kiber hücumçu birliyinə" sahib olduğunu bildirdi. Kiber hücumçulardan olan heyətin Çin Xalq Qurtuluş Ordusunun (PLA) internet brauzerlərini xarici hücumlardan qorumaq məqsədini daşıdığını ifadə etdi. Çin 30 nəfərdən ibarət olan birliyin adını "Mavi Ordu" olduğunu bildirdi. İngiltərənin Times qəzetinə müsahibə verən sabiq bir Çin Xalq Qurtuluş Ordusunun generalı "Mavi Ordu"nu təşkil edən şəxslərin xüsusi olaraq seçildiyini və "xüsusi bir bacarığa" malik olduğunu dedilər. Dövlət tərəfindən dəstəklənən Çin Silah Nəzarəti və Silahsızlanma Dərnəyinin yuxarı səviyyədə tədqiqatçılarından olan Xu Guangyu, "İnternet sərhəd tanımır. Bu səbəbdən hansı qruplaşmanın və ya ölkənin düşmənimiz olacağını və bizə hücum edə biləcəyini bilmirik. Mavi Ordunun əsil hədəfi özünü müdafiə xarakteri daşıyır. Heç bir dövlətə hücum etmək niyyətində deyilik."

İnformasiya təhlükəsizliyi təşkilatlar üçün bir kapital olan informasiyanı hədəfləməkdədir. İnnovasiya idarəetməsi isə təşkilatın maraqlarını qorumaq və artırmaq məqsədilə ediləcək yenilikləri əhatə edər. Əgər informasiyanın qorunması üçün idarəetmə həyata keçirilirsə bu innovasiyadır. Eyni şəkildə innovasiya informasiya təhlükəsizliyi sistemlərinin özlərinə tətbiq oluna biləcək yeniliklərdən də formalaşa bilər. Bu vəziyyət onu göstərir ki, innovasiya etmək istəyən bir təşkilat bunu özündə informasiya təhlükəsizliyini həyata keçirərək edə bilər. Eyni şəkildə informasiya təhlükəsizliyi məsələsində ediləcək yeniliklər də həm təşkilatlara, həm də dövlətlərə yeni qapılar açmaqda fürsət verə bilər.

İnformasiya hər bir qurum üçün əhəmiyyət da-

şıyan və bu səbəblə də ən yaxşı şəkildə qorunması gərəkən bir varlıqdır. İnformasiya təhlükəsizliyi qurumdakı işlərin davamlılığının təmin olunması, işlərdə meydana gələ biləcək çatışmazlıqların azaldılması və kapitallardan gələcək üçün faydanın artırılması üçün informasiyanın geniş əhatəli təhdidlərdən müdafiəsini təmin edər. İnformasiya anlayışını izah etmədən əvvəl aşağıdakı anlayış və informasiya anlayışlarını izah edək:

Verilənlər mənası olan və yazılan reallıqlar. (bir şəxsin adı, adresi, telefon nömresi və s.) Verilənlər faktların, anlayışların və ya təlimatların insan tərəfindən və ya avtomatik yolla, əlaqə yaratma, şərh etmə və fəaliyyət məqsədinə uyğun bir şəkildə ifadəsidir. Verilənlər həm işlənməmiş, tənzimlənməmiş, əlaqələndirilməmiş tez məna verilməyən simvol, hərf, rəqəm, işarə və təəssüratlardır. Verilənlər informasiyanın əsas xam maddəsidir. [7, s.123]

İnformasiya bir bildirişdir, əsasən sənəd şəklində ya da şəkil və vizual münasibətdir. Hər bir bildirişdə olduğu kmi informasiyada da bir göndərən və bir də bildirişi alan tərəf mövcuddur. İnformasiyanın məqsədi, bildirişi alanın informasiyanı əldə etmə şəklini dəyişdirmək, qərar ya da davranışı üzərində bir təsir yaratmaqdır. İnformasiya alıcısını formalaşdırmaq məcburiyyətindədir və onun baxışında ya da anlayışında bir fərq yaratmaqdadır. Bu mənada informasiya fərq yaradan veriləndir. Verilənlər müxtəlif yollarla (bağlama yerləşdirmək (məqsədə yönəltmək) təsnifləndirmək, hesablamaq, düzəltmək, yekunlaşmaq) anlamaq və dəyərlər əlavə olunub əlaqələndirməklə informasiyaya çevrilir. [12, s.175]

İnformasiya təşkil edilmiş, tənzimlənmiş veriləndir.

Məlumat: İnformasiya verilənlərdən yarandığı kimi məlumat da informasiyadan yaranır. Bu 4 C hərfi (comparison, consequences, connection, conversation) ilə başlayan sözlərin vasitəsilə meydana gəlir. İnformasiya təcrübə, dəyərlər, yeni təcrübə və informasiyanı dəyərləndirmək və birləşdirmək üçün bir sklet formalaşdıran anlayışdır. Məlumat şərh olunaraq işlək vəziyyətə gətirilmiş və məna kəsb edən informasiyadır.

İnformasiya təhlükəsizliyi anlayışı işçilər arasında fəaliyyət göstərən bir sistemi yavaşlatma kimi başa düşülə bilər. Ona görə də İnformasiya təhlükəsizliyi İdarəetmə Sistemi yaradılarkən işçilərə bunun mahiyyəti izah edilməli onlar maarifləndirilməlidirlər ki, daim dinamik qala bilsinlər. Görülən bütün işlərin mərkəzində insan dayandığını hər zaman diqqətdə saxlamaq lazımdır ki, bilmədən edilən bir xətanın nəinki hər hansısa bir quruma zərər verməyəcəyi, eyni zamanda insana zərər vuracağı daim xatırlansın. Bir idarəetmə sistemi yaxşı təşkil olunarsa getdikcə işçilərdə qaydalar davranışa dönüşməyə başlayacaqdır.

İnformasiya Təhlükəsizliyi İdarəetmə Sistemi risq əsaslı bir idarəetmə sistemidir. Sistemin əsasında subyektlərin təsbit olunması, subyektlərə yönələn təhlükələrin və risqlərin müəyyən olunması, müəyyən edilən bu risq və təhlükələrin aradan qaldırılmasına yönələn nəzarətin təyin edilməsi və nəhayət bu nəzarətlərin dövlət tərəfindən təsbit edilmiş siyasətlə dəstəklənməsinə əsaslanmaqdadır. Qeyd edilən bu addımlar daim nəzarətdə saxlanılmalıdır.

İnformasiya Təhlükəsizliyi İdarəetmə Sistemində informasiya təhlükəsizliyinin yaradılması, tətbiqi, izlənməsi, davam etdirilməsi, yaxşılaşdırılması və eyni zamanda iş risqlərinin həll olunması üçün bəzi standartlar müəyyən olunar. İnformasiya Təhlükəsizliyi İdarəetmə Sisteminin faydalı ola bilməsi üçün təsirli bir şəkildə tətbiq olunması vacibdir. İnformasiya Təhlükəsizliyi İdarəetmə Sistemi bir dəfədə tamamlanacaq bir tətbiq deyildir. Davamlı yaxşılaşdırma üçün davam edəcək bir fəaliyyət görülməlidir. Bunun üçün də istənilən fəaliyyət istiqamətində informasiya mədəniyyəti olmalıdır. İnformasiya təhlükəsizliyi üçün nəzarəti yaxşı seçilmiş, uyğun olaraq tətbiq olunmuş və istifadə olunmuş bir idarəetmə sistemi, günün sonunda bir itirilmiş xərc deyil, əksinə idarəetmənin daha yaxşı işləməsi üçün töhvə olacaqdır. [11, s.2091]

İnformasiya təhlükəsizliyi anlayışı olduqca dinamikdir. Bu gün bizim üçün normal qəbul edilən bir davranış sabah çalışdığımız bir qurum üçün təhlükə ola bilər. İnkişaf edən texnologiya özü ilə birlikdə davamlı yenilik də gətirir. Hər bir şəxs texnologiyanın inkişafından istifadə edərkən və ya xidmət təqdim edərkən şəxsi informasiyalardan istifadə edir. Bura fəaliyyət göstərdiyi qu-

rumlarla yanaşı, bank fəaliyyəti və sairə kimi fəaliyyətlər də daxildir. Belə olduqda unutmamalıyıq ki, hər bir təşkilatın daxilində təhlükəsizlik təmin olunmazsa şəxsi təhlükəsizlik də təmin oluna bilməz. Təşkilatın informasiya təhlükəsizliyi dedikdə, informasiyalı şəxslərin təsbit edilməsi, zəif nöqtələrin müəyyənləşməsi, istənilməyən hədəqorxulardan təhlükələrən müdafiəsi məqsədi ilə lazımı təhlükəsizlik analizlərinin aparılaraq qabaqlayıcı tədbirlərin görülməsidir.[1, 233]

İnformasiya təhlükəsizliyi ən əsas mənada informasiyanın müdafiə olunduğu informasiya sistemlərinin və sistemin əhatə etdiyi informasiyanın icazəsiz əldə edilməsinə, istifadə edilməsinə, ifşa edilməsinə, dəyişdirilməsinə, tətdiq edilməsinə, zərər verilməsinə qarşı müdafiəsi və buna bağlı tədbirlərin cəmidir. Burada diqqət edilməli məqam informasiya təhlükəsizliyi anlayışının əslində istifadə edilən texnologiyadan asılı olmayan şəkildə nəzərdən keçirilməsidir. İstər kağız üzərində olsun, istərsə də elektron formada olsun informasiya özünə yönələn təhlükələrə qarşı bu informasiyaları daşıyanlar və istifadə edənlər tərəfindən hər zaman müdafiəyə möhtacdır. Onsuz da informasiya təhlükəsizliyinin ilk istifadə sahəsi gizlilik və sirr anlayışının olduqca əhəmiyyətli olduğu diplomatik və hərbi mövzulardır. İlk vaxtlar informasiya təhlükəsizliyi sadəcə milli təhlükəsizliyin qorunmasına xidmət edən tədbirlər bütünü olaraq nəzərdən keçirilirdi. Ancaq informasiya və komunikasiya texnologiyalarının inkişafı ilə informasiyanın rəqəmsallaşaraq sistemdə yerləşdirilməsi və saxlanılması nəticəsində informasiyanın təhlükəsiz bir formada saxlanılması, müdafiəsi və lazım olduqda istifadə edilməsi problemi artıq informasiya sistemlərinə sahib hər kəsin ortaq məsələsi halına gəlmişdir. İnformasiya cəmiyyətinə keçid dövrü ilə bərabər şəxsi kompyuterdən ən qarışıq informasiya texnologiyalarınadək bütün informasiya sistemləri informasiyanı özündə saxlamış və bu səbəblə də informasiya təhlükəsizliyi anlayışı rəqəmsallaşma ilə birlikdə əhəmiyyət qazanmağa başlamışdır.

Tarixi inkişafından da göründüyü kimi informasiya təhlükəsizliyi yeni anlayış deyildir. İnformasiyanın yazılı bir formada saxlanılmağa başladığı ilk vaxtlardan etibarən informasiya müdafiə oluna bilən və oğurlana bilən, yox edilə bilinən bir məlumatdır. Tarix boyunca insanlar özləri belə dərk etmədən saxladıqları əhəmiyyətli informasiyaların təhlükəsizliyini təmin edə bilmək üçün tədbirlər görmək məcburiyyətində qalmışlar.

İnformasiya anlayışı.

İnformasiya təhükəsizliyi anlayışını daha yaxşı başa düşmək üçün ilk öncə informasiya və komunikasiya texnologiyalarının əsas təməli olan informasiyaya anlayış verilməlidir. İngiliscə informasiyaya aid istifadə edilən (data, information, knowledge) anlayışların azərbaycanca qarşılığı olaraq informasiya anlayışından istifadə edilir. Ancaq bu terminlərin dilimizdə qarşılığı olaraq verilənlər, informasiya, məlumat anlayışlarının istifadəsi daha uyğun olacaqdır. Bu terminlərin aşağıdakı anlayışları, aralarındakı fərqi ortaya çıxarmaqdadır.

Verilənlər (data): Verilənlər bir-biri ilə əlaqəsi olmayan rəqəmsal şəbəkələrə verilən addır. Bu informasiya sistemində mövcud olan verilənlər rəqəmlərdən təşkil olunur və təkbaşına hər hansı bir məna daşımır. (misal üçün: 1.400; 6.3 və ya 29000 AZN) Digər bir tərəfdən informasiya texnologiyası baxımından verilən, bir məsələ haqqında bir-biri ilə əlaqəsi hələ yaranmamış informasiyalar və ya qısaca desək rəqəmsal mühitdə mövcud olan və daşınan siqnallar olaraq izah edilə bilər.

İnformasiya (information): verilənlərin quruluşca tənzimlənmiş və ya mənalı bir formaya salınmış şəklinə deyilir. Bir verilənin istifadə edilə bilməsi üçün informasiya formasına çevrilmiş olması lazımdır. İnformasiya sistemində mövcud olan verilənlər mesaj xüsusiyyəti daşıyan halda mənalı bir formaya gətirilərək istifadə edənə təqdim edilir.

Məlumat: Məlumat (knowledge) təcrübə qazanmaq, öyrənmək və ya daxili müşahidə qaydasında əldə edilən reallıqların, həqiqətlərin, ya da informasiyaların əldə edilməsi və ya anlaşılması olaraq izah edilməldir. Məlumat bir şeyin nə olduğunu, nə üçün olduğunu, necə olduğunu və kim olduğunu bilmək şəklində dörd sinifdən ibarətdir. Bu dörd ana sualın cavabı ümumilikdə məlumatın əhatəsini formalaşdırmaqdadır.

Yuxarıda qeyd edilən verilənlər, informasiya, məlumat kimi anlayışlar nəzəri anlayışlar olmaq-

dan əlavə praktik bir sıra nəticələrə də səbəb olmaqdadır.

İnformasiya təhlükəsizliyinin əhatə dairəsi

İnformasiya təhlükəsizliyi, şəxsi kompyuterlərdən korporativ və milli səviyyədəki bütün informasiya sistemlərinə əsaslanan geniş bir çərçivədə informasiya sistemlərini əhatə edən bir təhlükəsizlik idarəetmə anlayışıdır.[18]Korporativ səviyyədə informasiya sistemi, üçüncü tərəf olaraq informasiya sistemlərindən istifadə edən istifadəçiləri və informasiya sistemlərinə texniki dəstək verməkdə olan xidmət, proqram təminatını əhatə etməkdədir. İnformasiya təhlükəsizliyi rəqəmsal müahitdəki informasiyanın saxlanması və daşınması əsasında informasiyanın bütünlüyü pozulmadan, icazəsiz əldə etməkdən çəkinməsi, təhlükəsiz bir informasiya saxlama və emalından ibarət bütündür. Bunun təmin olunması üçün uyğun təhlükəsizlik siyasətləri müəyyən olunmalı və tətbiq olunmalıdır. Bu siyasətlər, faəliyyətlərin müzakirə olunması, əldə etmənin izlənilməsi, dəyişikliklərin qeydiyyatının qiymətləndirilməsi, verilənlərin silinməsi qaydasında məhdudiyyətlər kimi bəzi istifadə qaydalarına toxunmaqdadır. İnformasiya təhlükəsizliyi daha ümumi mənada təhlükəsizlik mövzularını ətraflı olaraq nəzərdən keçirən "təhlükəsizlik mühəndisliyi"nin bir sahəsi olaraq görülməkdədir.[2, s.171] Digər bir tərəfdən informasiya təhlükəsizliyi geniş mənada kriptoloji, risq idarəetməsi, təhlükəsizlik mədəniyyəti kimi intizam ilə əlaqədar olub informasiya təhlükəsizliyinin anlayışında təbii olaraq əhatə olunan sahələr olaraq sayılmaqdadır. İngiliscə "İnformation security" anlayışı informasiya təhlükəsizliyi olaraq dilimizə çevrilməkdədir. "İnformastion assurance" anlayışının azərbaycanca qarşılığı olaraq informasiya təminatı anlayışının istifadəsi daha uyğun olacaqdır. İnformasiya təminatında informasiya sistemində informasiya təhlükəsizliyini təmin etmək üçün vacib olan texniki və müddətli ehtiyaclar daha strateji səviyyədə nəzərdən keçirilərkən informasiya təhlükəsizliyi anlayışı isə daha taktiki səviyyədə bir məna daşımaqdadır.

Bundan başqa informasiya təhlükəsizliyinin əsas anlayışları çərçivəsində tez-tez sözü keçən informasiya sistemləri kimi anlayışlara da toxunmaq lazımdır.

İnformasiya sistemləri: informasiya texnologiyaları və istifadəçinin qarşılıqlı təsiri daxilində olduqları və taktiki, idarəedici və dəstək sistemi olaraq istifadə edilən sistemlərdir. [14] Bu mənada informasiya sistemi, sadəcə informasiya və komunikasiya texnologiyalarının problemlərini deyil, eyni zamanda insanların iş müddətlərini dəstəkləyən bu texnologiyalar ilə qarşılıqlı təsir məqsədilə istifadə etdikləri yolları da əhatə etməkdədir. Bu gün informasiya sistemləri daha çox komyüter əsasında fəaliyyət göstərməkdədir. Ancaq komyuterlərlə yanaşı proqram, internet və dünya miqyasında şəbəkə (www-world wide web), avadanlıq, rabitə sistemləri kimi işi asanlaşdıranlar da rəqəmsal əsaslı bir informasiya sisteminin işləməsi üçün vacibdir. Digər bir tərəfdən şəxsi komyuterlərdən başqa ən mürəkkəb səviyyədə super komyuterlərə qədər geniş bir ölçüdə təyin olunan informasiya sistemləri informasiyanı əldə etmə, saxlama və əlçatan kimi xüsusiyyətlərə sahibdir.

İstifadə olunmuş ədəbiyyat:

1. Baykara, M., Daş, R. ve İ. Kardoğan., Bilgi Güvenliği Sistemlerinde Kullanılan Araçların İncelenmesi, 1st International Symposium on Digital Forensics andSecurity, Elazığ, s:231-239.
2. Canbek G., Sağıroğlu Ş. "Bilgi, Bilgi Güvenliği ve Süreçleri Üzerine Bir İnceleme", Gazi Üniversitesi Politeknik Dergisi, 2006, Cilt: 9 Sayı: 3 ss. 165-174,
3. Daniel M. White, "The Federal Information Security Management Actof 2002: A Potemkin Village 79 FordhamL. Rev. (2011) p.370-405,
4. Öztürk, G., Bilgi Güvenliği Politikası Oluşturma Kılavuzu. Kocaeli: TÜBİTAK Ulusal Bilgi Güvenliği Kapısı.2008, 13 s.
5. Önel, D., Dinçkan, A. Bilgi Güvenliği Yönetim Sistemi Kurulumu. Kocaeli: TÜBİTAK Ulusal Bilgi Güvenliği Kapısı. 2007, 16 s.
6. Önel, D., Erişim Kontrol Politikası Oluşturma Kılavuzu. Kocaeli: TÜBİTAK Ulusal Bilgi Güven-

liği Kapısı.2007 16 s.
7. Öğüt Adem, Bilgi çağında yönetim. Nobel akademik yayıncılık 2016, 336 s.
8. Clarke, G., CompTIA Security+ Certification Study Guide (Exam SY0-301). s.l.:McGraw Osborne Media (2011) 806 p.
9. Dulaney, E. Chuck, E, . CompTIA Security+Study Guide: Exam SY0-201. Fourth Edition dü. s.l.:John Wiley & Sons, 2017, 528 p.
10. Graves, K.,. CEH Certified Ethical Hacker Study Guide. s.l.:John Wiley & Sons. Grutzmacher, 2010, .393 p

https://pdfs.semanticscholar.org/ecbd/a49848fec7a69ac5cc102f0c5051566cebca.pdf 2019

11. Kajava J., Anttila J., Varonen R., Savola R, Roning J.,(2006), "Information Security Standards and Global Business", IEEE, p.2091-2097
12. Thomas H. Davenport., Big Data at Work : Dispelling the Myths, Uncovering the Opportunities, Harvard Business Review Press, 2014, 240 p.
13. http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.897.6228&rep=rep1&type=pdf
14. <http://web.archive.org/web/20070903115947/http://www.sei.cmu.edu/publications/documents/03.reports/03tr002/03tr002glossary.html>. 13.11.2019
15. https://www.google.com/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&cad=rja&uact=8&ved=2ahUKEwjIkd-FiOflAhXIgVwKHfpECuQQFjAAegQIAhAB&url=http%3A%2F%2Fe-qanun.gov.az%2Fframework%2F3525&usg=AOvVaw08TQrDpBC2ggoO0TmYe5hc 11.10.2020
16. http://www.businessdictionary.com/definition/information.html 11.10.2020
17. https://en.wikipedia.org/wiki/PlayStation_3 15.10.2020
18. http://ina.bnu.edu.cn/docs/20140520102905252150.pdf 17.10.2019

Aytakin İbrahimova

INFORMATION SECURITY; CONCEPT OF SECURITY AND INFORMATION

Summary

The concept of information has gained more meaning with the experience gained from the past to the present. When we look at the definition of information in a dictionary, we mean the information that a person acquires using reality, information, or rules obtained through learning, research, or observation. Every field of science, every author has given different concepts to information in his books. However, it should be noted that information is a concept that changes not only in the field of science, but also in time and conditions. In the past, information was shaped by people, but today it is a factor of production and has the characteristics of buying and selling.

Айтекин Ибрагимова

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ; КОНЦЕПЦИЯ БЕЗОПАСНОСТИ И ИНФОРМАЦИЯ

Резюме

Концепция информации приобрела большее значение с опытом, накопленным из прошлого в настоящее. Когда мы смотрим на определение информации в словаре, мы имеем в виду информацию, которую человек получает, используя реальность, информацию или правила, полученные в результате обучения, исследования или наблюдения. В каждой области науки каждый автор дал разные концепции информации в своих книгах. Однако следует отметить, что информация - это понятие, которое изменяется не только в области науки, но также во времени и условиях. В прошлом информация формировалась людьми, но сегодня она является фактором производства и имеет характеристики покупки и продажи.