Azərbaycan Respublikası Vergilər Nazirliyinin

Tədris Mərkəzi

“Vergi orqanlarında məlumat təhlükəsizliyinin təmin edilməsi” mövzusu üzrə

TƏLİM MATERİALI

Dinləyicilər	müsabiqə yolu ilə vergi orqanlarına staj müddətinə işə qəbul edilən əməkdaşlar, orta və kiçik menecerlər (mütəxəssislər);
Təhsilalma forması	əyani;
Tədris müddəti	2 saat;
Müəllif	Mirzəyev Anar Cəlilağa oğlu, İqtisadiyyat və menecment kafedrasının baş müəllimi.

Tədrisin məqsədi - Vergi orqanı əməkdaşlarına məlumatların təhlükəsizliyinin təmin olunması və həmçinin iş yerlərində olan avadanlıqlardan təhlükəsiz istifadə barədə praktik və nəzəri məlumatların verilməsi, dinləyicilərin bu məsələlər haqqında biliklərə yiyələnməsidir.

Bakı – 2018

Mövzunun mündəricatı

I. İnformasiya təhlükəsizliyi

İnsana, əşyaya və bütün canlılara zərər vermə ehtimalı olan hər şeyə "təhlükə" deyilir. Təhlükə görünməyinə görə iki növ olur:

gözlə görülən (vizual)

gözlə görünməyən (kiber)

İnformasiya fəaliyyəti sahəsində yaranan təhlükələr əsasən gözlə görünən olmadığı üçün mövzuda əsasən kiber təhlükə mənbələri haqqında fikir mübadiləsi aparılacaq.

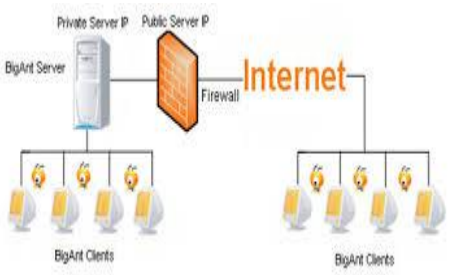
1.1. İnformasiya texnologiyalarından istifadə zamanı yaranan təhlükələr

Sosial şəbəkələrdən daxil olan təhlükələr. Həyatımızın ayrılmaz hissəsinə çevrilən internetdən istifadə edənlərin sayı sürətlə artmaqdadır. ABŞ-ın Virciniya ştatında yerləşən, internet layihələri üzrə marketinq araşdırmaları şirkəti olan "Comscore" tərəfindən yayımlanan son hesabatda dünyanın 3 milyard internet istifadəçisinin 2 milyardan çoxunun sosial şəbəkə saytlarından istifadə etdikləri bildirilir. Məlumat üçün bildirək ki, ilk sosial şəbəkələr 90-cı illərin ortalarında meydana çıxıb. Bu "Classmates" idi; 1999-cı ildə yaradılan "Livejournal" çox populyar olub; 2003-cü ildə "MySpace", bir il sonra yaradılan "Facebook" və "Twitter" və 2006-cı ildə Rusiya yaradılan "Odnoklassniki" və "V kontakte" də fəaliyyətə başlayıb. Yeni yaradılan sosial şəbəkələrin sayı isə durmadan artır. Qeyd edək ki, sosial şəbəkələr arasında ən məşhuru "Facebook"dur. Statistikaya görə, bu gün dünyada 1.5 milyardan çox insan "Facebook" sosial şəbəkəsində qeydiyyatdan keçib. Bir çox insan vaxtının böyük hissəsini "Facebook"da keçirir. Qeyd edək ki, hazırda «Facebook» şəbəkəsindən istifadəyə görə 164 mln. istifadəçi ilə 1-ci yerdə ABŞ, 2-ci yerdə 65 mln. istifadəçi ilə Braziliya, 3-cü yerdə isə 61 mln. istifadəçi ilə Hindistan qərarlaşıb. Türkiyə "Facebook"da ən çox üzvü olan ölkələr sırasında 4-cü yerdədir. Azərbaycanda «Facebook» istifadəçilərinin sayı 996 140-a çatıb. Azərbaycan 213 ölkə arasında 82-ci yerdə qərarlaşıb.

Sosial şəbəkə vasitəsilə daxil olan təhlükələrdən ən mühim olanlarından biri sosial şəbəkə istifadəçilərinin kibercinayətkarların potensial qurbanına çevrilməsi ilə bağlıdır. Belə ki, şəbəkədə özləri haqqında ətraflı məlumat yerləşdirmələri onların asanlıqla internet cinayətkarlarının toruna düşməsinə səbəb ola bilər. Digər tərəfdən hazırkı şəraitdə *şəkil və məlumatlar sosial şəbəkələrin bazalarında müddətsiz saxlanılır. Məlumat üçün deyim ki, əvvəllər fiziki yaddaşların qiyməti baha olduğundan heç bir təşkilat fərdi məlumatları yaddaşda saxlamırdı. Hal hazırda tam əksinə, bütün fərdi və ümumi məlumatlar onların bazasında saxlanılır və istifadəçi tərəfindən heç cür silinmə ehtimalı yoxdur. Düzdü, sosial şəbəkədən şəkli və məlumatı silərkən interfeysdə silinmiş kimi görsənsədə, axra prosesdə heç də belə deyil.*

İkinci təhlükə mənbəyi proqram təminatları ilə bağlı olan təhlükələrdir. Nəzərə alsaq ki, nazirliyin tətbiqi proqramları (Microsoft ofis, Oracle, antivirus və s.) xarici şirkətlərdən alınır və istifadə edilir, buna görə də arxa prosesdə (insanlar gözlə görməyən) sistemlərindən

məlumatlar nazirliyin şəbəkəsindən kənara çıxıb oğurlana bilər. Nazirliyin əməkdaşları məlumat mübadiləsi üçün Skype-dən istifadə edirdilər. Nəzərə alsaq ki Skype proqramı Microsoft şirkətinin məhsuludur və ötürülən fayllar və ya mətnlər onların serverində digər iştirakçılara ötürülür. Bu cür hallarda kommersiya sirri təşkil edilən məlumatların sızmasına şərait yaradır. Bu sahədə təhlükəsizliyin təmin edilməsi üçün 2012-ci ildə intranetdə çalışan BigAnt proqram təminatı tətbiq edildi və Active Directory ilə əlaqələndirildi (ActiveDirectory- işçilərin ağac formasında strukturu).

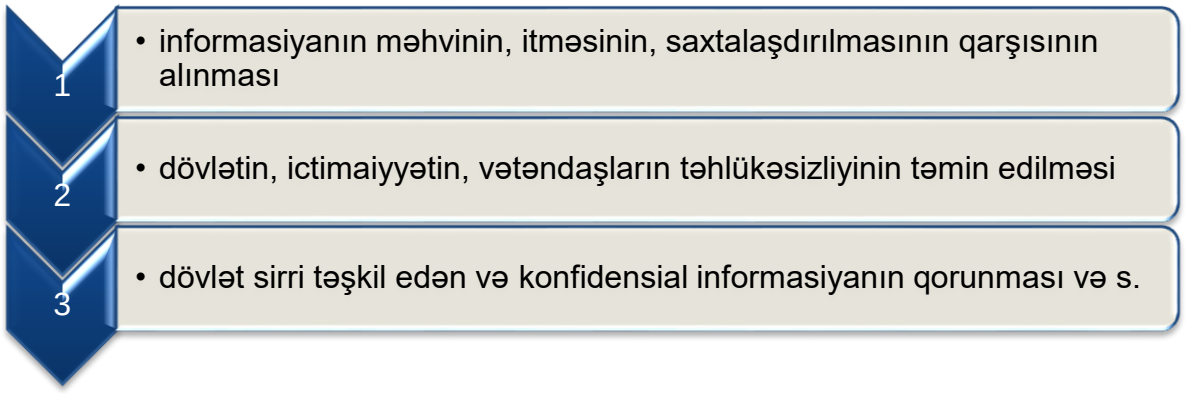


Əvvəllər əməkdaşlar iş komputerlərinə müxtəlif proqramlar yazırdılar məsələn skype kimi və ya müxtəlif qurğulardan istifadə edirdilər məsələn flashkart kimi qurğular. Bunlardan da isitifadə zamanı Nazirlik sisteminə çoxlu sayda virusların düşməsi təhlükəsi yaranırdı. Bu problemlərin qarşısın almaq üçün 2012-ci ilin sonlarından etibarən Nazirlik üzrə zərif müştəri sisteminin tətbiqinə başlanıldı. Bu sistemin tətbiqi zamanı bütün işçi fayılları mərkəzləşdirilmiş Storage-də saxlanılır və hər həftə arxivləşir. Hər bir fərdi məlumatı yalnız profilin sahibi görür və idarə edə bilir. Misal üçün işçi yerdəyişmə etdi və ya işdən azad olundu. Əgər adi komputer olsa, işdən azad olunanın komputerini yeni əməkdaşa verilsə və onun fayılları komputerdə qalsa, kommersiya sirri təşkil edilən məlumatlar əldən ələ keçə bilər. “İncə Müştəri”də yanaşma fərqlidir. Yeni təyin edilən əməkdaşa yeni profil açılır və yalnız özünə məxsus məlumatları görür. İşdən azad olunan şəxsin isə profili bloklaşdırılır və arxivdə saxlanılır. Zərif Müştərilərdə yeni profil açılarkən standart şifrə təyin edilir. İlk dəfə sistemə daxil olandan sonra həmin şifrə istifadəçi tərəfindən dəyişdirilməlidir.

1.2. informasiya təhlükəsizliyin təmin olunması

İnformasiya təhlükəsizliyinin təmin olunmasına yönəlmiş tədbirlər kompleksi İnformasiyanın mühafizəsi adlanır. Əldə olunma növünə görə informasiya ümumi istifadə üçün açıq və alınması məhdudlaşdırılan informasiyalara bölünür. Qanunvericilikdə əldə olunması məhdudlaşdırılmayan informasiyalar açıq informasiyalar sayılır. Əldə edilməsi qanunla məhdudlaşdırılan informasiyalar hüquqi rejiminə görə məxfi və gizli (konfidensial) olur. Dövlət sirri məxfi, vətəndaşların, mülkiyyət növündən asılı olmayaraq yaradılmış idarə, müəssisə və təşkilatların, digər hüquqi şəxslərin qanuni maraqlarının qorunması məqsədilə əldə olunmasına məhdudiyyət qoyulan peşə (həkim, vəkil, notariat), kommersiya, istintaq və məhkəmə sirləri , habelə fərdi məlumatlar konfidensial xarakter daşıyır. Fərdi məlumatlar daxilolma (əldə olunma) növünə görə konfidensial və açıq kateqoriyalara bölünür. Məlumatların dövlət sirrinə aid edilməsi, istifadəsi qaydaları və mühafizəsi Dövlət sirri haqqında Azərbaycan Respublikasının Qanunu ilə müəyyən edilir. Konfidensial informasiyanın toplanmasına, işlənməsinə, istifadəsinə və yayılmasına yalnız Azərbaycan Respublikasının qanunvericiliyində müəyyən edilmiş hallarda yol verilə bilər.

İnformasiyanın mühafizəsinin məqsədləri aşağıdakılardan ibarətdir:



Şifrələnmə: İnformasiya təhlükəsizliyi üçün informasiya dünyasında istifadə olunan bütün alətləri, dataları istifadə edərkən hədəflənən disiplindir və 3 təməl prinsipi vardır:

Gizlilik- dataların və dataların əldə olunduğu mənbələrin gizlənilməsi prinsipidir. Məlumatın pis niyətli insanların (icazəsi olmayan) əllərinə keçməsini əngəlləməyi hədəfləyir.

Bütövlülük- Məlumatın dəyişdirilmədən, zərər görmədən saxlanılması məqsədlidir. Kiber hücum edənlər məlumatların yerdəyişməsi zamanı içindəki məlumatı silə bilər, dəyişdirə bilər. Bu kimi vəziyyətlərin əngəllənməsi hədəflənməkdədir.

Davamlılıq- məlumatların istənilən zaman qəbul olunması və ötürülməsi hədəflənməkdədir. Bu prinsip vasitəsilə icazəsi olan şəxslər məlumatı təhlükəsiz bir şəkildə istənilən vaxt əldə edə bilərlər.

Məlumat üçün bildiririk ki, hər bir kompüterə girmək üçün şifrə olmalıdır. Beynəlxalq standartlara görə şifrənin müddəti **15** gündən çox olmamalıdır. Buna görə də, hər **15** gündən bir şifrənin dəyişdirilməsi tövsiyə edilir. Şifrənin tərkibində doğulduğun gün, ay, il, istifadəçinin adının istifadəsi tövsiyə edilmir. T*anımadığınız ünvandan daxil olan elektron məktubların oxumasına diqqət yetirin. Əgər şübhəli məktubdursa və məktubda əlavə fayllar varsa, bu zaman antivirusla skan edib baxılması və ya heç baxılmaması məsləhətdir. Bu cur hallarda müvafiq mütəxəssisə müraciət olunması tövsiyyə olunur.*

II.Vergilər Nazirliyində informasiya təhlükəsizliyinin təmin olunması

Məlumdur ki, informasiya texnologiyaları iş fəaliyyətini avtomatlaşdırır, dəfələrlə asanlaşdırır və operativləşdirir. Lakin informasiya təhlükəsizliyi siyasəti düzgün təyin edilməsə informasiya texnologiyaları sahəsində çoxlu boşluqlar yaranar. Həmin boşluqlardan xarici ölkələrin kəşfiyyatı, xakerlər və digərləri istifadə edib istədikləri kimi yararlana bilər. Buna görə də bütün dövlət orqanlarında o cümlədən Vergilər Nazirliyində informasiya təhlükəsizliyinin təmin olunması qarşıya qoyulmuş əsas məqsədlərdən hesab olunur.

Vergilər Nazirliyində informasiya təhlükəsizliyinin təmin olunması məqsədi ilə vergilər nazirinin 12.06.2013-cü il tarixli 1317040100621000 nömrəli əmri ilə “Avtomatlaşdirilmiş Vergi İnformasiya sistemində məlumat təhlükəsizliyinin qorunması üzrə Şura” yaradılmış, vergilər nazirinin 09.07.2013-cü il tarixli 1317040100709900 nömrəli əmri ilə Şuranın Əsasnaməsi təsdiq edilmişdir.

Şura Vergilər Nazirliyinin Avtomatlaşdirilmiş Vergi İnformasiya sistemində məlumat təhlükəsizliyinin təmin olunması sahəsində siyasətin formalaşmasında iştirak edir və bu siyasətin həyata keçirilməsinə rəhbərlik edir. Şuranın 23 dekabr 2013-cü il tarixdə keçirilmiş iclasında Avtomatlaşdirilmiş Vergi İnformasiya sistemində məlumatların fiziki qorunması, server otaqlarının, o cümlədən ehtiyat server otaqlarının daimi təhlükəsiz və işlək vəziyyətdə saxlanılması barədə qaydaların hazırlanması tapşırılmışdır.

Vergilər Nazirliyində məlumatların təhlükəsizliyinin qorunması üçün Azərbaycan Respublikası vergilər nazirinin 11.06.2014-cü il tarixli 1417040100771200 nömrəli Əmri ilə "Avtomatlaşdirilmiş Vergi İnformasiya Sistemində məlumat təhlükəsizliyinin təmin edilməsi ilə bağli qaydalar", 01.08.2014-cü il tarixli 1417040101035000 nömrəli Əmri ilə "Vergi orqanlarında məlumaların təhlükəsizliyinin qorunması və iş yerlərindən təhlükəsiz istifadənin təmin edilməsi Qaydaları" və 16.09.2014-cü il tarixli 1417040101320900 nömrəli Əmri ilə "Vergi orqanlarında smartfon tipli, internetə çıxış imkanına və foto və video görüntüsünə malik olan mobil telefon cihazlarından, planşet və noutbuk tipli kompüterlərdən, foto və video görüntü, səs qeydə alan cihazlardan, xarici yaddaş qurğularından və elektron yaddaşa malik digər mobil cihazlardan istifadə qaydaları" təsdiq edilmişdir.

2.1. Avtomatlaşdirilmiş Vergi İnformasiya Sistemində məlumat təhlükəsizliyinin təmin edilməsi

Dövlət vergi orqanlarının vahid avtomatlaşdırılmış məlumat sisteminin və bu sistemin yardımedici və xidmətedicilərinin məlumat təhlükəsizliyinin təmin edilməsi, sistemin qüsursuz və fasiləsiz işləməsi, server və ehtiyat server otaqlarının (və ya bina və tikililərin), server avadanlığı və qurğularının daim təhlükəsiz, işlək vəziyyətdə saxlanılması və mühafizəsi, məlumat (və ya məlumat surətlərinin) daşıyıcılarının təhlükəsiz daşınması, saxlanılması və mühafizəsi Azərbaycan Respublikası vergilər nazirinin 11.06.2014-cü il tarixli 1417040100771200 nömrəli Əmri ilə "Avtomatlaşdirilmiş Vergi İnformasiya Sistemində məlumat təhlükəsizliyinin təmin edilməsi ilə bağli qaydalar"la tənzimlənir.

Vergilər Nazirliyinin informasiya infrastrukturu informasiya təhlükəsizliyi standartının tələblərinə uyğun olmalıdır. Bu tələblər aşağıdakılardan ibarət olmaqla informasiya sistemlərinin alınması, işlənib hazırlanması və tətbiqi də daxil olmaqla onların bütün fəaliyyəti boyunca informasiya sistemlərinə tətbiq olunmalıdır:

- Vergilər Nazirliyində yalnız lisenziyalaşdırılmış proqram təminatından istifadə edilməlidir. Müvafiq struktur vahid ilə razılaşdırmaqla sərbəst yayılan proqram təminatından və açıq lisenziya sazişi şərtləri ilə yayılan proqram təminatından istifadə edilməsinə yol verilir
- İnformasiya sistemi təkmilləşdirilərkən və təkmilləşdirilmiş versiya işə salınarkən informasiya sisteminin əvvəlki surəti, o cümlədən proqram təminatı və məlumatlar ehtiyat surətçıxarma prosedurlarına uyğun olaraq bütünlüklə köçürülməlidir.
- Yeni informasiya sistemlərinin işlənib hazırlanmasını və ya onların təkmilləşdirilməsini bilavasitə onların real istismarı mühitində həyata keçirmək qadağandır
- İnformasiya sistemlərinin daxildə işlənib hazırlanması və ya təkmilləşdirilməsi məqsədləri üçün Nazirliyin əsas şəbəkəsindən məntiqcə ayrılmış xüsusi yardımçı şəbəkə yaradılmalıdır
- İnformasiya sistemlərini hazırlayanlar informasiya resurslarının real istismarı mühitində onların üzərində inzibati hüquqlara malik olmamalıdırlar
- İşləyib hazırlamaq məqsədilə real iş məlumatlarından istifadə etmək lazım gəldikdə bu məlumatlar adlı və real məlumatlardan ibarət olmamalıdır
- işlənilib hazırlanmış proqram təminatları test rejimində yoxlanılmalıdır

İnformasiya daşıyıcılarından istifadəyə qoyulan tələblər: Xarici informasiya daşıyıcıları (USB flaş-kartlar, CD disklər, MemoryStik, External Hard Drive) informasiyanin saxlanması və ötürülməsi üçün mühüm vasitədir. Xarici informasiya daşıyıcılarından istifadə zamanı aşağıdakılara əməl edilməlidir:

- Xarici informasiya daşıyıcılarına kommersiya sirri təşkil edən informasiya yazarkən kriptoqrafiya vasitələrindən istifadə edilməlidir;
- xidməti informasiyanın xarici informasiya daşıyıcılarında saxlanması qəti qadağandır.

Ümumi resurslardan istifadəyə qoyulan tələblər: Ümumi şəbəkə resursları (şəbəkə fayl serveri, direktoriyalar və fayllar) Vergilər Nazirliyinin müvafiq struktur vahidinə verilmiş tələbləri üzrə yaradıla, ləğv edilə və giriş üçün açıla bilər. İstifadəçilər ancaq müvafiq giriş hüquqi verilmiş ümumi istifadə resurslarının sahələrində fayllar və direktoriyalar yarada, onları modifikasiya və ləğv edə bilərlər.

İstifadəçi fayl serverdə yerləşən şəxsi şəbəkə kataloqunda saxlanılan ona məxsus bütün informasiyaya görə məsuliyyət daşıyır. Ümumi istifadədə olan şəbəkə resursları yalniz Nazirliyin fəaliyyətinə aid informasiyanın saxlanılması üçün (xidməti və məxfi xarakterli informasiyanın saxlanması) nəzərdə tutulmuşdur. Fayl serverdə yerləşdirilmiş məhlumatların ehtiyat surətlərinin çıxarılmasını müvafiq struktur vahidi təmin edir.

İnternet resurslarından istifadəyə qoyulan tələblər: Vergilər Nazirliyinin struktur bölmələrində internet şəbəkəsinin resurslarından yalnız xidməti məqsədlərlə istifadə edilməlidir. İstifadəçilərə İnternet şəbəkəsindən vəzifə funksiyalarının icrası ilə əlaqədar istifadə imkanları Avtomatlaşdırılmış Vergi İnformasiya Sistemində məlumatların təhlükəsizliyinin qorunması üzrə Şuranın sədrinin icazəsi ilə verilir.

İnternet şəbəkəsindən kommersiya sirri təşkil edən materialların göndərilməsi, habelə Vergilər Nazirliyinin fəaliyyətinə aid olan hər hansı informasiyanın saxlanması üçün istifadə edilməsi qadağandır.

İnternet şəbəkəsində ictimai rəy üçün təhqiramiz hesab edilən, yaxud əyləncə xarakterli informasiya daşıyan, irqi və dini nifrəti təbliğ edən və digər bu qəbildən hər hansı saytlardan istifadə etmək qadağandır. Vergilər Nazirliyinin rəhbərliyinin müvafiq göstərişləri olmadan xidməti fəaliyyətə aid məsələləri internet şəbəkəsinin forumlarında və konfranslarında müzakirə etmək qadağandır.

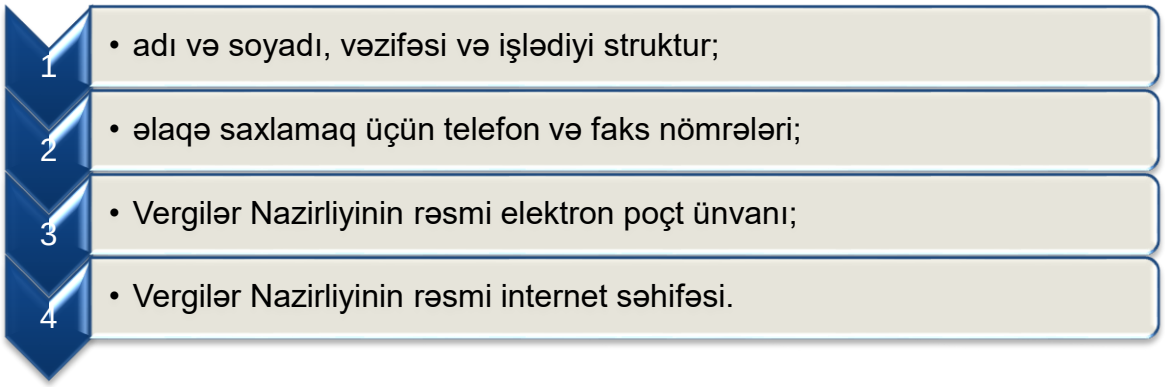
***Qeyd**: Qadağaların pozulması "Vergi işçisinin etik davranış Kodeksi"nə görə məsuliyyət yaradır.*

Korporativ elektron poçtdan istifadəyə qoyulan tələblər: Elektron poçt sistemi Vergilər Nazirliyinin mülkiyyətidir. Elektron poçt sistemi əməkdaşlar tərəfindən yalnız xidməti məqsədlər üçün istifadə olunmalıdır. İstifadəçilərə elektron poçt sistemindən istifadə imkanı Şura sədrinin dərkənarı ilə struktur bölmənin müraciəti əsasında müvafiq struktur vahidi tərəfindən yaradılır. Qəbul edilən kriptoqrafik mühafizə vasitələri tətbiq etmədən kommersiya sirri təşkil edən informasiyadan ibarət məlumatları üçüncü şəxslərə göndərmək üçün elektron poçtdan istifadə edilməsi qadağandır.

Korporativ elektron poçtdan istifadə zamanı aşağıdakılar qəti qadağan olunur:

- şəxsi yazışma məlumatlarını göndərmək;
- digər şəxsin poçt qutusundan məlumatlar göndərmək;
- hər hansı xidməti fəaliyyəti həyata keçirmək üçün internet xidmətlərinin şəxsi poçt qutusundan (Mail, Hotmail kimi) istifadə etmək;
- şəxsi məqsədlər üçün poçt göndərişlərinə, diskussiya qruplarına və ya digər belə poçt xidmətlərinə abunə yazılmaq;

Bütün elektron məktublarda göndərən şəxs barədə aşağıdakı məlumatlar olmalıdır:



Avadanlığın və server otağının təhlükəsizliyi üzrə tələblər: Bütün server və şəbəkə avadanlığı xüsusi server otaqlarında yerləşdirilməli və oraya giriş yalnız Vergilər Nazirliyində daxili nəzarət funksiyalarının həyata keçirilən struktur və müvafiq struktur vahidinin rəhbərləri ilə razılaşmaya əsasən olmalıdır. İstifadəçilərin lokal şəbəkəyə girişini təmin edən telekommunikasiya avadanlığının server otaqlarından kənar yerdə qıfıllı və möhürlənmiş dolablarda yerləşdirilməsinə yol verilir, bu şərtlə ki, dolabların video müşahidəsi təmin edilsin. Dolabların açılması qeydiyyata alınmalıdır.

Server otaqlarına giriş nəzarət altında olmalı və avtomatlaşdırılmış girişə nəzarət sistemi tərəfindən qeydiyyata alınmalıdır.

Server və şəbəkə avadanlığı dayaqlar üzərində qıfıllı dolablarda yerləşdirilməlidir.

Dolabların və dayaqların açarları sistem administratorlarında, açarların dublikatları isə Vergilər Nazirliyində daxili nəzarət funksiyalarını həyata keçirən strukturunun və müvafiq struktur vahidinin rəhbərlərində saxlanılmalıdır.

Kommunikasiyaların qoyulmasına olan tələblər: Server otağından mühəndis sistemlərinin heç bir magistralı və ya şaxələri keçməməlidir, buraya həmçinin ümumi kanalizasiya sistemi, isti və soyuq su təchizatı, ümumi havalandırma və kondisioner sistemi, elektroqidalandırma və işıqlandırılma paylanması sistemləri və Server otağının özündə olan sistemlər istisna olmaqla digər zəif axınlı sistemlər aiddir.

İnformasiyanın ehtiyat surətinin çıxarılması, onun bərpa edilməsi və informasiyanın ehtiyat surətlərinin saxlanması üzrə tələblər: Vergilər Nazirliyində məlumatların və proqram təminatının müntəzəm surətdə ehtiyat surətinin çıxarılması həyata keçirilməli, habelə informasiyanın surətinin çıxarılması, saxlanması və bərpa edilməsinin etibarlığını təmin edən müvafiq ehtiyat surətçıxarma vasitələri quraşdırılmalıdır.

Vergilər Nazirliyinin müvafiq struktur vahidi informasiyanın ehtiyat surətinin çıxarılması və bərpa edilməsi prosedurlarını həyata keçirməsini təmin etməlidir. Saxlanılan informasiyanın tamlığını və ona giriş imkanını yoxlamaq üçün ehtiyat surətlərdən informasiyanın bərpa edilməsi vaxtaşırı testdən keçirilməlidir.

Ehtiyat surətçıxarma prosedurlarının müvəffəqiyyətlə yerinə yetirilməsini və tətbiq olunan informasiya təhlükəsizliyi tələblərinə uyğunluğunu yoxlamaq üçün Vergilər

Naziriliyində daxili nəzarət funksiyasını həyata keçirən struktur informasiyanın ehtiyat surətinin çıxarılması və onun ehtiyat surətlərinin saxlanması prosesinə vaxtaşırı nəzarət etməlidir.

Ehtiyat surətlərin təhlükəsiz saxlanmasını təmin etmək üçün informasiyanın yaradıldığı və işlənildiyi əsas yerdən (yəni əsas binanın server otaqlarından) ərazicə uzaqda, fövqəladə vəziyyətlərdə ehtiyat surətlərin saxlanmasını təmin etmək üçün yetərincə aralı məsafədə yerləşən və mühafizə olunan obyektdən istifadə edilməlidir.

İnformasiyanın ehtiyat surətlərinin daşıyıcıları ən azı saxlanan informasiyanın identifikatorunu, informasiyanın ehtiyat surətinin yaradılması tarixini və saxlanma müddətini göstərməklə markalanmalıdır.

AVIS-in məlumat bazasının ehtiyat mərkəzinə ötürülməsi mümkün olmayan hallarda məlumatların arxiv surətlərinin saxlanması və mühafizəsi aşağıdakı qaydada həyata keçirilməlidir:

- ❖ Proqram servislərini və məlumatlarını dəstəkləyən icraçı təşkilat hər gün saat 14.00-dək məlumatları müvafiq daşıyıcılara köçürür və bu zaman xüsusi proqram təminatı vasitəsilə arxivləşdirilən məlumatlara parol verilir.
- ❖ Məlumat daşıyıcısının tutumundan asılı olaraq məlumatlar bir və ya daha çox daşıyıcıya köçürülür.
- ❖ Məlumat daşıyıcıları konteynerə yerləşdirilir, konteyner sıra ardıcıllığı ilə növbəti nömrə ilə nömrələndikdən sonra möhürlənir.
- ❖ Gün ərzində saat 14.00-dan sonra məlumatların köçürülməsi zərurəti yarandığı hallarda məlumat köçürülmüş daşıyıcılar barədə qeydlər növbəti iş günü jurnala daxil edilir və həmin iş gününə aid olan konteynerə yerləşdirilir.
- ❖ Hər gün saat 14.00-da konteyner möhürlənmiş vəziyyətdə jurnalda imza etdirilməklə Vergilər Nazirliyinin müvafiq əmri ilə təyin edilmiş məsul şəxsə təhvil verilir.
- ❖ Məsul şəxs Vergilər Nazirliyinin müvafiq əmri ilə müəyyən edilmiş məsul strukturun rəhbərinə konteynerin qəbul edilməsi ilə bağlı məlumat verdikdən sonra "İşçilərin xidməti zərurətlə əlaqədar idarədən getmələrinin və gəlmələrinin qeydiyyatı kitabı"nda müvafiq qeyd aparır.
- ❖ Məsul şəxs konteyneri Vergilər Nazirliyinin xüsusi təyinatlı avtomaşını vasitəsilə nazirliyin mühafizə xidmətinin silahlı əməkdaşlarının müşayəti ilə arxivə aparır.
- ❖ Xüsusi təyinatlı avtomaşının arxivə hərəkəti zamanı müəyyən olunmuş marşrutdan və qrafikdən kənarlaşması, nəzərdə tutulmayan məntəqələrdə dayanması, habelə avtomaşında kənar şəxslərin və yüklərin daşınması qadağandır. Xüsusi təyinatlı avtomaşının hərəkəti texniki səbəbdən mümkün olmazsa, konteynerin mühafizəsi təmin olunmalı və onun arxivə çatdırılması üçün şəraitə uyğun qərar qəbul edilməlidir.
- ❖ Məsul şəxs konteyneri arxivin müəyyən edilmiş daxili qaydası ilə arxivdə xüsusi ayrılmış seyfə qoyur və bu zaman seyfdə daşıyıcıların saxlama şəraitini və mövcud vəziyyətini yoxlayır. Saxlama vəziyyəti normativ tələblərə uyğun olmadıqda (rütubət, hərarət, toz və sair), bu barədə arxivin məsul işçisinə və Vergilər Nazirliyinin məsul strukturunun rəhbərinə rəsmi qaydada məlumat verir.
- ❖ Seyfin Vergilər Nazirliyinə aid olan açarı məsul strukturun rəhbərində saxlanılır. Məsul şəxs konteyneri arxivə aparanda açarı məsul strukturun rəhbərindən qəbul edir.
- ❖ Məsul şəxs Vergilər Nazirliyinə qayıtdıqdan sonra konteynerin arxivə təhvil verilməsi barədə məsul strukturun rəhbərinə məruzə edərək açarı ona qaytarır və "İşçilərin xidməti zərurətlə əlaqədar idarədən getmələrinin və gəlmələrinin qeydiyyatı kitabı"nda müvafiq qeyd aparır.

Məlumat daşıyıcıları arxivdən aşağıdakı hallarda geri götürülə bilər:

a) Məlumat daşıyıcılarının istismar müddəti bitdikdə yenilənmə məqsədilə;

b) Texniki səbəblərdən baş vermiş məlumat itkilərinin bərpa edilməsi məqsədilə:

c) Məlumat daşıyıcılarındakı informasiyanın tamlığının test olunması məqsədilə.

Məlumat daşıyıcıları arxivdən yalnız Vergilər Nazirliyinin rəhbərliyinin rəsmi icazəsi ilə geri götürülə bilər.

İcraçı təşkilatlarla qarşılıqlı fəaliyyət üzrə tələblər: Vergilər Nazirliyinin informasiya sisteminə səlahiyyət hüququ alan icraçı təşkilatlar və onların əməkdaşları kommersiya sirri təşkil edən məlumatların açıqlanmasına görə Azərbaycan Respublikasının qanunvericiliyinə uyğun olaraq məsuliyyət daşıyırlar.

İcraçı təşkilatın əməkdaşlarına Vergilər Nazirliyinin informasiya resurslarına səlahiyyət hüquqlarının verilməsi müvafiq struktur vahidi ilə razılaşdırılmaqla həyata keçirilməlidir. İcraçı təşkilatın əməkdaşları tərəfindən aparılan əməliyyatlara müvafiq struktur vahidi tərəfindən nəzarət edilməlidir.

Qəza və ya fövqəladə halların nəticələrinin aradan qaldırılması üçün həyata keçirilən tədbirlər: Vergilər Nazirliyində fövqəladə hallar, qəzalar meydana çıxarkən Vergilər Nazirliyinin fasiləsiz fəaliyyətinin təmin edilməsi üçün informasiya texnologiyaları servislərinin və biznes-proseslərin bərpa edilməsini təmin edən aşağıdakı tədbirlər həyata keçirilməlidir:

1. *ehtiyat avadanlıqlardan və otaqlardan istifadə edilməklə Nazirliyin əsas binasında informasiya texnologiyaları servislərinin və biznes-proseslərin operativ qəza-bərpa imkanının təmin edilməsi;*
2. *Nazirliyin yaradılan və qaynar rejimdə saxlanan Ehtiyat Mərkəzdən istifadə etməklə əsas informasiya texnologiyaları servislərinin və biznes-proseslərin operativ bərpası imkanının təmin edilməsi.*

Qəzalardan sonra informasiya sistemlərinin tələb olunan müddətlərdə bərpası Vergilər Nazirliyinin müvafiq struktur vahidi tərəfindən təmin edilməlidir. Vergilər Nazirliyinin struktur vahidləri öz səlahiyyətləri daxilində zəruri tədbirləri həyata keçməlidirlər.

2.2. Vergi orqanlarında smartfon tipli, internetə çıxış imkanına və foto və video görüntüsünə malik olan mobil telefon cihazlarından, planşet və noutbuk tipli kompüterlərdən, foto və video görüntü, səs qeydə alan cihazlardan, xarici yaddaş qurğularından və elektron yaddaşa malik digər mobil cihazlardan istifadə

Vergi orqanlarının vəzifəli şəxslərinə, xidməti heyətinə və digər işçilərinə xidməti vəzifələrinin icrası ilə əlaqədar smartfon tipli, internetə çıxış imkanına və foto və video görüntüsünə malik olan mobil telefon cihazlarından, planşet və noutbuk tipli kompüterlərdən, foto və video görüntü, səs qeydə alan cihazlardan, xarici yaddaş qurğularından istifadə etmələri qadağan olunur.

Vergi orqanlarının vəzifəli şəxslərinin, xidməti heyətinin və digər işçilərinin yuxarıda göstərilmiş əşyalar ilə Vergilər Nazirliyinə və nazirliyin tabeliyində olan qurumların inzibati binalarına daxil olmalarına, eləcə də inzibati binalarda həmin əşyalardan istifadə etmələrinə yol verilmir. Nazirliyin tabeliyində olan qurumların əməkdaşları xidməti zərurətlə əlaqədar inzibati binalara planşet tipli kompüterlə daxil ola bilərlər. Vergilər Nazirliyində İctimaiyyətlə və

kütləvi informasiya vasitələri ilə əlaqələr və analitik informasiya sahəsində təhlil və təşkilati tədbirləri həyata keçirən müvafiq struktur vahidinin əməkdaşları inzibati binaya özləri ilə foto və video görüntü, səs qeydə alan cihazları gətirə bilərlər.

Vergi orqanlarının vəzifəli şəxsləri, xidməti heyəti, digər işçilər, o cümlədən Vergilər Nazirliyinə elektron informasiya sisteminin təmin edilməsi sahəsində podrat müqaviləsi ilə xidmət göstərən təşkilatların işçiləri və müvafiq xidmətlərin göstərilməsi (o cümlədən, elektron informasiya sisteminin təmin edilməsi sahəsində) üçün vergi orqanlarının inzibati binalarına müvəqqəti gələn şəxslər xidməti və digər zərurətlə əlaqədar olaraq inzibati binalara daxil olan zaman buraxılışa icazə vərəqələrini təqdim etməklə (göstərməklə) özləri ilə xarici yaddaş qurğularını, planşet və noutbuk tipli kompüterləri keçirə bilərlər. Buraxılışa icazə vərəqələrinin verilməsinə və ondan istifadəyə nəzarəti Vergilər Nazirliyinin aparatında daxili təhlükəsizlik sahəsində təşkilati və nəzarət tədbirlərini həyata keçirən müvafiq struktur vahid, digər struktur bölmələrdə isə daxili nəzarət qrupu həyata keçirir.

Uçot, qeydiyyat və xidmət strukturlarının vəzifəli şəxsləri istisna olmaqla, vergi orqanlarının vəzifəli şəxslərinin qəbuluna gələn şəxslərə Vergilər Nazirliyinin və nazirliyin tabeliyində olan qurumların inzibati binalarına istifadəsi məhdudlaşdırılan cihazlarla daxil olmasına yol verilmir. Qəbula gələn şəxslər üzərilərində olan istifadəsi məhdudlaşdırılan cihazları saxlanması üçün nəzərdə tutulmuş müvəqqəti saxlanc yerlərinə təhvil verdikdən sonra Vergilər Nazirliyinə və nazirliyin tabeliyində olan qurumların inzibati binalarına buraxılırlar.

Uçot, qeydiyyat və xidmət məsələləri ilə əlaqədar vergi orqanlarının vəzifəli şəxslərinin qəbuluna gələn şəxslərin üzərilərində olan istifadəsi məhdudlaşdırılan cihazları söndürdükdən sonra inzibati binalara daxil olmasına yol verilir.

İstifadəsi məhdudlaşdırılan cihazların müvəqqəti saxlanması üçün Vergilər Nazirliyinə və nazirliyin tabeliyində olan qurumların inzibati binalarının girişində müvəqqəti saxlanc yerləri yaradılır.

Qeyd: *Müvəqqəti saxlanc yeri azı* ***10 bölmədən*** *ibarət olmalı və bölmələr nömrələnməlidir.*

Müvəqqəti saxlanc yerlərinə təhvil verilmiş istifadəsi məhdudlaşdırılan cihazların mühafizəsini Vergilər Nazirliyinin və nazirliyin tabeliyində olan qurumların inzibati binalarının mühafizəsinə məsul şəxslər həyata keçirir.

İstifadəsi məhdudlaşdırılan cihazlar müvəqqəti saxlanc yerinə təhvil verilərkən cihaz sahibinə müvəqqəti saxlanc yerinin bölməsinin nömrəsi əks olunan saxlanc nömrəsi verilir. Müvəqqəti saxlanca götürülmüş istifadəsi məhdudlaşdırılan cihazlar təqdim edilmiş saxlanc nömrəsi əsasında sahibinə qaytarılır.

Vergi orqanlarının vəzifəli şəxslərinin qəbuluna gələn şəxslər tərəfindən, eləcə də Vergi orqanlarının vəzifəli şəxsləri, xidməti heyəti və digər işçiləri tərəfindən istifadəsi məhdudlaşdırılan cihazların Vergilər Nazirliyinin və nazirliyin tabeliyində olan qurumların inzibati binalarına keçirilməməsinə nəzarəti həmin inzibati binaların mühafizəsinə məsul şəxslər həyata keçirir.

Vergi orqanlarının vəzifəli şəxslərinin qəbuluna gələn və istifadəsi məhdudlaşdırılan cihazları könüllü olaraq müvəqqəti saxlanc yerinə təqdim etməkdən (eləcə də, uçot, qeydiyyat və xidmət məsələləri ilə əlaqədar vergi orqanlarının vəzifəli şəxslərinin qəbuluna gələn və istifadəsi məhdudlaşdırılan cihazları könüllü olaraq söndürməkdən) imtina edən şəxslərin Vergilər Nazirliyinin və nazirliyin tabeliyində olan qurumların inzibati binalarına daxil olmasına icazə verilmir və bu barədə dərhal müəyyən edilmiş formada akt tərtib edilir.

Bu qaydaların tələblərinə vergi orqanlarının vəzifəli şəxsləri, xidməti heyəti və digər işçiləri tərəfindən riayət edilməməsi əmək intizamının kobud pozulması hesab olunur və qanunvericiliklə nəzərdə tutulmuş intizam məsuliyyətinə

səbəb olur.

2.3. İş yerlərindən təhlükəsiz istifadənin təmin edilməsi

Vergi orqanlarında konfidensial məlumatların elektron ötürülməsi və alınması yalnız şifrələnmiş kanallar (VPN kanallar, https protokolundan istifadə etməklə) vasitəsi ilə həyata keçirilir.

Vergi orqanlarının əməkdaşları elektron fayllardan və kağız daşıyıcısında olan məlumatlardan elə istifadə etməlidirlər ki, məlumatların təhlükəsizliyi təmin edilsin.

Vergi orqanlarının əməkdaşları öz xidməti otağında kommersiya (vergi) sirri təşkil edən məlumatların əks olunduğu sənədləri (qovluqları) hər kəsin görə biləcəyi yerdə saxlamamalı və onların məxfiliyinin qorunması üçün bütün mümkün vasitələrdən istifadə etməlidirlər.

Vergi orqanlarının əməkdaşları iş vaxtı ərzində və yaxud iş gününün sonu xidməti otağını tərk edən zaman iş masasını səliqəliyə salmalı, masanın üstündə xidməti fəaliyyət ilə əlaqədar yalnız zəruri əşyaları (kitablar, ofis ləvazimatları) saxlamalı, habelə informasiya təhlükəsizliyinin təmin edilməsi məqsədi ilə kommersiya (vergi) sirri təşkil edən məlumatların əks olunduğu və ya olunmadığı sənədlərin (qovluqların) masanın üstündə saxlanılmasına yol verməməlidir. Bu zaman kommersiya (vergi) sirri təşkil edən məlumatların əks olunduğu sənədlər (qovluqlar) seyflərə və ya kilidlə bağlanması mümkün olan dolablara, kommersiya (vergi) sirri hesab edilməyən digər sənədlər (qovluqlar) isə kilidlə bağlanması mümkün olan dolablara qoyulmalıdır.

Vergi orqanlarının əməkdaşları tərəfindən kommersiya (vergi) sirri təşkil edən məlumatların əks olunduğu sənədlər (qovluqlar) istifadə edildikdən sonra, onların əsilləri aiddiyyəti struktur vahidə təhvil verilməli, surətləri isə bərpa olunmasını istisna edən üsullarla (doğranılma və ya başqa üsullarla) məhv edilməlidir.

III. Vergilər Nazirliyinin informasiya təhlükəsizliyi sahəsində sertifikatlaşması

Ötən illər ərzində Vergilər Nazirliyi tərəfindən AVİS-də məlumat təhlükəsizliyinin, vergi orqanlarında dövlət, peşə və kommersiya sirrinin qorunması məqsədilə bir sıra zəruri tədbirlər həyata keçirilmişdir.


BS Cert.

AZS Milli Sertifikatlaşdırma Sistemi
Azərbaycan Respublikası
Standartlaşdırma, Metrologiya və Patent üzrə Dövlət Komitəsi
yanında Dövlət Akkreditasiya Xidməti
AZS National Certification System
State Accreditation Service under the State Committee on Standartization, Metrology and Patent of Azerbaijan Republic

"BS CERT" MMC İdarəetmə Sistemlərinin Sertifikatlaşdırılması üzrə Orqan
The certification body on management systems of the "BS CERT" LTD
VÖEN: 2002693391

Akkreditasiya attestatı № AZ 031/11.1/09.0510.01.13
Verilmə tarixi : 20 Sentyabr 2013-cü il

Accreditation certificate № AZ 031/11.1/09.0510.01.13
Issue date : 20 September 2013

Blank № 005

Uyğunluq Sertifikatı
Certificate of conformity
Azərbaycan Respublikasının Vergilər Nazirliyi

ISO/IEC 27001:2013
"İnformasiya Təhlükəsizliyinin İdarəetmə Sistemləri"
beynəlxalq standartının
TƏLƏBLƏRİNƏ UYĞUNDUR

Qeydiyyat № AZ 031120200052015
Register №
Qeydiyyat tarixi 10.08.2015
Register date
Qüvvədə olma müddəti 10.08.2018
validation date
"BS CERT" MMC-nin
İdarəetmə Sistemlərinin Sertifikatlaşdırılması üzrə Orqanın rəhbəri
Director of the certification body on management systems of the "BS CERT" LTD
İmza :
M.Y. SALIMZADƏ SƏLİM SƏTTAR oğlu
İdarəetmə sisteminin ümumi qeydiyyat hesab nömrəsi: № 005
General registration number of the management system № 005

Vergilər Nazirliyi bu sahədə görülən işlərin nəticəsi olaraq beynəlxalq standartın alınması ilə bağlı sertifikasiyanı keçərək 2015-ci ilin avqustun 10-da 3 il müddətinə informasiya təhlükəsizliyi sahəsində yüksək səviyyəli İSO/İEC 27001:2013 uyğunluq sertifikatına layiq görülmüşdür.

Məlumat üçün bildiririk ki, informasiya təhlükəsizliyinin idarəetmə sistemi mühüm əhəmiyyət kəsb edən informasiya aktivlərinin qorunması istiqamətində idarəolunan yanaşmadır və bu yanaşma İSO/İEC 27001:2013 "İnformasiya təhlükəsizliyinin idarəetmə sistemləri" beynəlxalq standartının tətbiqi ilə həyata keçirilir. Bu standart ilk dəfə olaraq informasiya təhlükəsizliyi sahəsində müvafiq sertifikatlaşdırma aparan dünyanın ən tanınmış institutlardan biri - Britaniya Standartlar İnstitutu tərəfindən 1995-ci ildə təsdiq olunub.

İSO/İEC 27001:2013 "İnformasiya təhlükəsizliyinin

idarəetmə sistemləri" beynəlxalq standartı dünyada informasiya təhlükəsizliyi sahəsində ən yüksək və ən çətin sertifikasiya prosesinə malik olan standartdır və Vergilər Nazirliyi respublikamızda mərkəzi icra hakimiyyəti orqanları arasında bu institutun sertifikatını alan yeganə dövlət qurumudur.

IV. Nəzarət sualları

1. İnformasiya texnologiyaları sahəsində yaranan təhlükələr əsasən təhlükənin hansı növünə aid edilir?
2. İnformasiyanın mühafizəsi tədbirləri dedikdə nə başa düşülür?
3. Əldə olunmasına görə informasiya neçə növə ayrılır və hansılardır?
4. Məlumatların dövlət sirrinə aid edilməsi, istifadəsi qaydaları və mühafizəsi hansı Qanunvericilik aktı ilə müəyyən edilir?
5. Xidməti informasiya xarici informasiya daşıyıcılarında saxlanıla bilərmi?
6. Vergi orqanlarında konfidensial (əldə olunmasına məhdudiyyət qoyulan) məlumatların elektron ötürülməsi və alınması hansı yolla həyata keçirilir?
7. AVİS-ə daxil edilmiş məlumatlar əsasında istifadəçilərin müxtəlif növ hesabatları əldə etməsinə imkan verən proqram-texniki altsistem necə adlanır?
8. İnformasiyanin saxlanması və ötürülməsi üçün istifadə olunan xarici informasiya daşıyıcıları hansılardır?
9. Server və şəbəkə avadanlığı harada yerləşdirilməlidir?
10. Vergi orqanlarının vəzifəli şəxslərinə, xidməti heyətinə və digər işçilərinə xidməti vəzifələrinin icrası ilə əlaqədar, nələrdən istifadə etmələri qadağan olunur?
11. Müvəqqəti saxlanc yerləri hansı tələblərə cavab verməlidir?
12. İstifadəsi məhdudlaşdırılan cihazlar müvəqqəti saxlanc yerinə təhvil verilərkən cihaz sahibinə nə verilməlidir?
13. Vergi orqanlarının vəzifəli şəxslərinin qəbuluna gələn şəxslər tərəfindən, eləcə də Vergi orqanlarının vəzifəli şəxsləri, xidməti heyəti və digər işçiləri tərəfindən istifadəsi məhdudlaşdırılan cihazların Vergilər Nazirliyinin və Nazirliyin tabeliyində olan qurumların inzibati binalarına keçirilməməsinə nəzarət kim tərəfindən həyata keçirilir?
14. Vergilər Nazirliyinin hansı strukturunun vəzifəli şəxslərinin qəbuluna gələn şəxslərə həmin strukturun yerləşdiyi inzibati binaya istifadəsi məhdudlaşdırılan cihazlarla daxil olmasına yol verilir?
15. Vergi orqanlarının əməkdaşları iş gününün sonu xidməti otağını tərk edən zaman iş masasının üstündə xidməti fəaliyyət ilə əlaqədar olan hansı sənədləri (əşyaları) saxlamalıdır?

V. Müstəqil öyrənmə üçün tapşırıqlar

1. Dövlət və kommersiya sirri hesab edilən məlumatlar;
2. Kommerisya sirri və məxfi məlumat xarakterli informasiya mübadiləsi təhlükəsizliyinin təmin olumasının optimal yolları nələrdir;
3. Bütün informasiya təhlükəsizlik tədbirlərinin nazirlik üçün əhəmiyyəti nədir;
4. Korporativ elektron poçtun və "BigAnt" proqram təminatının istifadəsinin üstünlüyü nədir;
5. "İncə Müştəri"nin istifadəsinə nə üçün zərurət yaranmışdır;
6. Aparat və departamentlər ƏVİ-lər arası məlumat mübadiləsi üçün rabitə kabelləri nə səbəbə məhz optik kabellərdir;

7. Bütün informasiya təhlükəsizlik tədbirlərinin nazirlik üçün yekun əhəmiyyəti nədir.

VI. İzahlı lüğət

Avtomatlaşdırılmış Vergi İnformasiya Sistemi– vahid məlumat bazasının və tətbiqi proqram təminatının çalışdığı mərkəzi serverlərdən, istifadəçilərin və vergi ödəyicilərinin mərkəzi serverlərə bağlanaraq işləməsini təmin edən şəbəkə avadanlıqlarından ibarət iri proqram-texniki kompleksdir və mərkəzi bazada toplanmış məlumatları emal edərək müxtəlif hesabatların alınmasına, təhlillərin aparılmasına imkan verən sistemdir.

"Hesabat-axtarış"(SAR) altsistemi– AVİS-ə daxil edilmiş məlumatlar əsasında istifadəçilərin müxtəlif növ hesabatları əldə etməsinə imkan verən proqram-texniki altsistemdir.

Konteyner – məlumat daşıyıcıların daşınması və saxlanılması üçün istifadə edilən daşıyıcının qabaritinə uyğun xüsusi qutu.

Arxiv - məlumatların surətlərinin daşıyıcılarının saxlanması üçün Azərbaycan Respublikasının Vergilər Nazirliyi tərəfindən müəyyən edilən və əsas mərkəzin yerləşdiyi binadan kənarda olan yer.

VI. Ədəbiyyat

1. Azərbaycan Respublikasının Vergi Məcəlləsi
2. İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında Azərbaycan Respublikasinin Qanunu
3. Dövlət Sirri haqqında Azərbaycan Respublikasinin Qanunu
4. "Avtomatlaşdırılmış İnformasiya Sistemində məlumat təhlükəsizliyinin təmin edilməsi ilə bağlı Qaydalar"ın təsdiq edilməsi barədə vergilər nazirinin 2 fevral 2014-cü il tarixli 1417040100771200 nömrəli əmri
5. "Azərbaycan Respublikası Vergilər Nazirliyində İnformasiya azadlığı ilə bağlı daxili icraat" Qaydaları haqqında Azərbaycan Respublikası vergilər nazirinin 22 may 2013-cü il tarixli 1317040100504000 nömrəli əmri
6. Azərbaycan Respublikası vergilər nazirinin 16.09.2014-cü il tarixli 1417040101320900 nömrəli Əmri ilə təsdiq edilmiş "Vergi orqanlarında smartfon tipli, internetə çıxış imkanına və foto və video görüntüsünə malik olan mobil telefon cihazlarından, planşet və noutbuk tipli kompüterlərdən, foto və video görüntü, səs qeydə alan cihazlardan, xarici yaddaş qurğularından və elektron yaddaşa malik digər mobil cihazlardan istifadə qaydaları"
7. Azərbaycan Respublikası vergilər nazirinin 01.08.2014-cü il tarixli 1417040101035000 nömrəli Əmri ilə təsdiq edilmiş "Vergi orqanlarında məlumaların təhlükəsizliyinin qorunması və iş yerlərindən təhlükəsiz istifadənin təmin edilməsi Qaydaları"
8. İSO/İEC 27001:2013 "İnformasiya təhlükəsizliyinin idarəetmə sistemlər beynəlxalq standartı.