V.İ. YAROÇKİN
Y.V. BUZANOVA

BİZNESİN VƏ SAHİBKARLIĞIN TƏHLÜKƏSİZLİYİNİN ƏSASLARI

BAKI – 2008

KBT – 65.290

UOT – 65
Y - 30

Kitab Rus dilindən Azərbaycan Dövlət İqtisad Universitetinin professoru A.B. Abbasovun elmi redaktəsi və rəhbərliyi ilə «Biznesin təşkili» kafedrasının aşağıdakı əməkdaşları tərəfindən tərcümə olunmuşdur:

i.e.n., b/m. S.M. Xanlarzadə, i.e.n., b/m. S.A. Abbasov, müəllim E.R. Səmədova, müəllim K.N. Quliyeva, müəllim A.S. Şükürova, müəllim A.Ə.Təhməzova, müəllim E.B. Manafov, müəllim N.H. Süleymanova, b/laborant S.S.Həsənova

Y 30 Yaroçkin V.İ., Buzanova Y.V. Biznesin və sahibkarlığın təhlükəsizliyinin əsasları/ Rus dilindən tərcümə. Bakı: «İqtisad Universiteti», 2008. – 174 səh. (Təhlükəsizlik texnologiyaları)

Kitabda müxtəlif fəaliyyət sferalarında sahibkarlığın təhlükəsizliyinin təmin edilməsi xüsusiyyətlərinə, biznes maraqlarının qorunması üzrə hüquqi, təşkilati və mühəndis-texniki tədbirlərə baxılır.

Kitab orta ixtisas və ali təhsil məktəblərinin tələbələri, mühafizə strukturlarının əməkdaşları və rəhbərləri, sahibkarlar üçün nəzərdə tutulmuşdur.

ISBN 5-8291-0490-3
ISBN 5-902357-21-7

© V.İ.Əroçkin, Ə.V.Buzanova, 2005
© Akademiçeskiy Proekt, oriqinal maket, oformlenie, 2005
© Fond «Mir» 2005
© «İqtisad Universiteti» 2008

GİRİŞ

•

Hazırkı dövrdə yüksək risk şəraitində fəaliyyət göstərən sahibkarlıq sferasında təhlükəsizliyin və maliyyə-təsərrüfat proseslərinin dayanıqlı şəkildə fəaliyyət göstərməsinin təmin edilməsi üzrə işlərin vəziyyəti həddən artıq mürəkkəbdir. İnkişaf edən sahibkarlıq fəaliyyətini tənzimləyən qanunvericiliyin işlənib hazırlanmasında gerilik, hüquqi tətbiq sferasındakı qarışıqlıq və müxtəlif dövlət institutlarının fəaliyyətlərinin mütləq uyğunsuzluğu, korrupsiya və kriminalın artması ilə müşayiət olunur. Təəssüf ki, o da düzdür ki, Rusiya dünyada cinayətkarlığın səviyyəsinə görə aparıcı yerlərdən birini tutur. Mütəşəkkil cinayətkar qruplaşmalar tərəfindən fərdi sahibkarlığa qarşı kriminal pressinq güclü və getdikcə də güclənən bir təsir kimi xarakterizə olunur. Cinayətkar qəsdlərin qurbanı olan sahibkarların sayı isə artmaqdadır. Ticarət biznesi nümayəndələrinin dörddə üçü uzunmüddətli əsaslarda kriminal strukturlara «haqq» verirlər, yaxud sonuncular tərəfindən vasitəçilərlə əvvəlcədən əlverişsiz şərtlərlə iş aparmağa məcbur edilirlər. Nəzarət altında olan firmaların mühafizə xidməti rəqiblərin susdurulması ilə məşğul olur. Sənaye casusluğu, informasiya oğurluğu, əlaqə xətlərinin dinlənilməsi, ofislərdə gizlicə qulaqasma qurğularının qurulması və s. kimi qanunsuz fəaliyyətlər artır. Heç bir başqa ölkədə, heç bir dövrdə «sifarişli qətl» hadisələri belə geniş vüsət tapmamışdır.

Sahibkarlara qarşı cinayətkar terrorun arxasında mütəşəkkil cinayətkar qruplaşmanın iqtisadi maraqları durur. Dövlət hakimiyyəti və idarəetmə orqanları ilə korrupsiya əsasında formalaşan əlaqələrə arxalanaraq, bu gün bu fəaliyyətlər təkcə iqtisadiyyatın bir sıra sektorlarında

liderliyə iddia etmir, o həmçinin siyasətə qarışır, bütün səviyyədən olan hakimiyyət strukturlarında öz maraqlarını lobbiləşdirir.

Belə şəraitdə sahibkarlıq fəaliyyətinin özü kriminallaşır. Onun məqsədi – qanunsuz metod və vasitələrdən istifadə edərək mənfəət götürülməsi olur. Sahibkarlığın üç əsas sferası (ticarət, maliyyə və istehsal) üzrə ümumi mənfi hallar vergidən yayınma, ədalətsiz rəqabət, partnyorların və müştərilərin aldadılması və s.-dir.

Sahibkarlıq sferasında və xüsusilə də kiçik biznes sahəsində formalaşmış situasiya təhlükəsizliyin təmin edilməsi və sahibkarlığın maraqlarının qorunması məsələsini ciddi olaraq ortaya qoyur. Dövlət şəxslərin və sahibkarlığın təhlükəsizliyini təmin etmək iqtidarında deyildirsə, yalnız bir yol qalır: «Boğulanların xilas edilməsi – boğulanların öz əlindədir». Bu kitab da sahibkarlığın təhlükəsizliyinin təmin edilməsi problemlərinə həsr olunmuşdur.

FƏSİL I

SAHİBKARLIĞA TƏHLÜKƏLƏR VƏ HƏDƏLƏR

“Hədə - təhlükəsizliyin potensial və
ya real mövcud olan pozulması təhlükəsidir”

Real biznes dünyasında sahibkarları ən müxtəlif təhlükə və hədələr gözləyir, belə ki, rəqabət mübarizəsində “rəqabət aparmaq” sözü daha çox “rəqibi nəyin bahasına olur-olsun məhv etmək” anlayışına uyğun gəlir. Rəqabət - amansız mübarizədir. O rəqiblərin qarşısında elə amansız şərtlər qoyur ki, onlar “qaliblər mühakimə olunmur”, “məqsəd vasitədən üstündür” prinsipləri ilə hərəkət etməyə məcbur olurlar. Biznesdə məsələ birmənalı qoyulur: ya sən, ya da səni dünyaya buraxırlar.

Sahibkarlıq sferasında hədələrə müəssisənin effektiv və etibarlı fəaliyyətini aşağı salan, ayrıca hallarda isə onun fəaliyyətinin dayandırılmasına səbəb olan iqtisadi, sosial, hüquqi, təşkilati, informasiya, ekolojı, texniki və kriminal xarakterli təhlükələr aiddir.

Sahikarlığın təhlükəsizliyinə hədələr özünü aşağıdakı əsas sferalarda göstərir.

İqtisadi hədələr. İqtisadiyyat sferasında baş verən təhlükəsizlik hədələri və cinayətlər qrupuna aiddir: oğurluqlar, soyğunçuluq, rüşvətxorluq, hakimiyyətdən və ya vəzifədən sui-istifadə; kontrabanda, valyuta əməliyyatları qaydalarının pozulması və s. Uzun illər

ərzində cinayətkarlığın təhlili bu halın yüksək sistemliyini göstərir - bir qrup iqtisadi cinayətlər tendensiyası qarşılıqlı bağlıdır, qismən isə digərlərinin dəyişiklikləri ilə zəruridir.

İqtisadi cinayətkarlığın strukturunun 1/3 –ni mənimsəmə, israfçılıq və ya vəzifə səlahiyyətlərindən sui-istifadə etmək yolu ilə həyata keçirilən dövlət və ictimai əmlakın talan olunması təşkil edir.

Yüksək ictimai təhlükəni vəzifə cinayətləri, hər şeydən əvvəl isə idarəetmə, təsərrüfat və kommersiya strukturlarının bütün həlqələrini əhatə edən rüşvətxorluq yaradır.

Sosial hədələr. Sosial hədələr işsizliyin səviyyəsinin artması, yoxsulluğun yüksəlməsi, yoxsul və zənginlərin gəlirləri arasındakı fərqlə əlaqədardır. Bura həmçinin qadınların biznesdə mövqeyini, əlilləri, hərbi qulluqçuları və s. daxil etmək olar.

İnformasiya hədələri. İnformasiya hədələri qrupuna konfidensial informasiya ilə tanışlığa, onun modifikasiya olunmasına və məhv edilməsinə gətirib çıxaran hərəkətlər, həmçinin qorunan məlumatlara qeyri-qanuni yolla sahib olma, texniki kanallarla məlumatın sızması və s. aiddir.

1.1. İqtisadi hədələr

Sahibkarlığın iqtisadi təhlükəsizliyi ona təsir göstərən daxili, xarici hədələrin müasir xarakteri, yönümü və istiqaməti ilə müəyyən olunur.

Xarici hədələrə aiddir:

1. Xarici xüsusi xidmət orqanlarının və təşkilatların aşağıdakılar üzrə kəşfiyyat fəaliyyəti:

- dünya təcrübəsini qabaqlayan fundamental və tətbiqi elmi tədqiqatların nəticələri üzrə materialların əldə olunması;

- dünya bazarında strateji mövqeyə, müdafiə-iqtisadi potensiala zərbə vura biləcək iqtisadi xarakterli konfidensial məlumatların yığılması.

2. Xarici firma, kompaniyaların ölkənin milli maraqlarına və təhlükəsizliyə zərbə vurmağa yönəlmiş fəaliyyəti:

- ölkə istehsalının zəiflədilməsi;
- "beyin axınının" stimullaşdırılması, kapitalın, strateji əhəmiyyətli elmi-texniki işləmələri və strateji xammal məhsulun ölkədən çıxarılması;
- xüsusi avadanlıqlar satmaq hesabına ölkəni idxaldan asılı vəziyyətə salmaq cəhdi.

3. İqtisadiyyatımıza beynəlxalq cinayətkar qruplaşmaların və onların kapitallarının, xarici vətəndaşlar sırasından müxtəlif avantürist və fırıldaqların daxil olması.

Daxili hədələrə aiddir:

1. Dövlət hakimiyyəti orqanlarında korrupsiyanın daim genişlənməsi, onlara cinayətkar elementlərin daxil olması, hansı ki, öz növbəsində özəlləşdirmə, maliyyə-bank, xarici iqtisadi əlaqələr sferasında mənfi tendensiyaların inkişafına səbəb olur.

2. İqtisadi cinayətkarlığın artması, buraya kontrabanda, kapital, valyuta, strateji məhsulun qeyri-qanuni ixracı, maliyyə sferasında cinayətlər, saxta əskinazlıq və cəlbi üzrə qiymətli kağızlarla qeyri-qanuni əməliyyatlar aiddir.

3. İqtisadiyyatda mütəşəkkil cinayətkar fəaliyyət, leqal biznesin ən gəlirli və vacib sferalarına kriminal kapitalın daxil olması.

Makroiqtisadi hədələrlə yanaşı sahibkarlıq üçün bir sıra mikroiqtisadi hədələr də mövcuddur. Ayrıca müəssisə və ya kommersiya strukturuna münasibətdə aşağıdakı **xarici** hədələr mövcuddur:

1. Ədalətsiz rəqabət.
2. Cinayətkar əməllər: kriminal zorakılıq, kommersiya sirrinə sahib olma.

3. Ayrı-ayrı hədələrin və ya administrativ aparatın təşkilatları, o cümlədən, vergi organlarının qeyri-qanuni fəaliyyəti.
4. İnformasiyanın yığımı, emalı və göndərilməsi reqlamentinin pozulnası.
5. Sənaye casusluğu.

Daxili hədələri aşağıdakı kimi təsnifləşdirmək olar:

1. şəxsi personalın aşağı professionallıq və ya vicdansızlıq üzündən düşünülmüş cinayətkar fəaliyyəti;
2. əməkdaşların düşünülməmiş fəaliyyəti və ya səhvləri;
3. avadanlığın və texniki vəsaitlərin sıradan çıxması;
4. informasiya emalı vasitələrinin proqram təminatının cavab verməməsi.

Daxili və xarici hədələr arasındakı nisbəti aşağıdakı göstəricilərlə xarakterizə etmək olar:

- 81,7% hədələr ya əməkdaşların özü tərəfindən, ya da onların bilavasitə və ya dolayı yolla iştirakı nəticəsində baş verir (daxili hədələr);
- 17,3% hədələr - xarici hədələr və ya cinayətkar hərəkətlərdir;
- 1,0% hədələr - təsadüfi səxslər tərəfindən hədələrdir.

Sahibkarlığa müxtəlif hədələrin obyektləri kimi çıxış edirlər:

1. insanlar (personal, əməkdaşlar, ortaqlar və s.);
2. maddi dəyərlər;
3. maliyyə resursları;
4. informasiya resursları, buna aiddir: patentlər, başa çatmamış layihə-konstruktor işləmələri, “nou-hau”-lar, proqram məhsulları, mühasibat və statistik informasiya massivləri və s. aiddir.

Personala hədələr mənəvi və fiziki əziyyətlər şəklində ifadə olunur:

- qətl hadisəsi;

- əməkdaşların, onların ailə üzvlərinin və yaxın qohumlarının qaçırılması hədəsi;
- psixoloji terror, hədə, qorxutma, şantaj və s.

Personala hədələr bir qayda olaraq böyük miqyaslı iqtisadi məsrəflərlə yaxşı işçilərin itirilməsi, işçilərə və onların ailə üzvlərinə dəymiş zərərin ödənilməsi və s. ilə müşayiət olunur.

Material qiymətlərə hədələr aşağıdakı şəkildə əks olunur:

- məhsulun oğurlanması, binalara, tikililərə, mənzillərə və digər daşınmaz əmlaka zərərlər vurulması;
- rabitə vasitələrinin və kommunal xidmət sisteminin aradan çıxarılması;
- nəqliyyat vasitələrinin oğurlanması və məhv edilməsi.

Təhlükələrin bu kateqoriyası ən aşkar və ən böyük iqtisadi zərər vuran kateqoriya kimi xarakterizə olunur.

Aşağıda «Moskva Komsomolu» tərəfindən 28.01.1998-ci ildə təqdim edilmiş səciyyəvi nümunə göstərilmişdir.

Son ilin ən uğurlu quldur hücumu «Rusiya krediti» bankının Panfilova küçəsində yerləşən valyuta dəyişmə məntəqəsinə edilən həmlə olub ki, bu cinayətin üstü polis əməkdaşları tərəfindən açılmışdır. Bu və ya digər formada cinayətdə iştirakı olan 8 nəfər həbs edilmişdir.

28 avqusta mübadilə məntəqəsinə iki nəfər kişi əmin addımlarla yaxınlaşdı. Onlar girişdəki mühafizəçilərə «Rusiya krediti» bankının işçisi vəsiqələrini təqdim etdilər, təftiş üçün gəldiklərini söylədilər və içəriyə daxil oldular. İçəridə «müfəttişlərin» davranışı möcüzəli şəkildə dəyişdi. Qanqsterlərdən biri tapançasını çıxardı, onu mühafizəçiyə (seküriti) və kassirə tuşladı, digəri isə inkassasiya üçün hazırlanmış pullarla dolu (cəmi təxminən 500 min dollar və 172 milyon rubl) olan çox ağır kisəni götürdü. Bundan

sonra cinayətkarlar «exchange»in əməkdaşlarını qandallarla bağladılar, yenə də vəsiqə ilə çöldəki mühafizəçilərdən keçdilər və sürətlə onları gözləyən maşına tərəf qaçdılar.

Xəfiyyələr həmlənin yüksək dərəcədə dəqiqliklə planlaşdırıldığını dərhal hiss etdilər. Hər şey təhqiqatın gedişi zamanı aydın oldu: bandaya bankın mühafizə xidmətinin əməkdaşlarından biri, yeri gəlmişkən sabiq polis işçisi kömək edirdi. O, saxta vəsiqələri hazırlamaqda kömək göstərmiş və haraya və nə vaxt gəlmək lazım olduğunu demişdi. Cinayətkarlar «kolleqalarının» hərəkətlərini ratsiya (radio stansiyası) vasitəsilə idarə edirdilər.

Son dörd gün ərzində «Sokol» OVD-un, MUR-un 4-cü bölməsinin, Şimal vilayətinin cinayət-axtarış şöbəsi və mütəşəkkil cinayətkarlıqla mübarizə şöbəsinin əməkDaşları qarətçiləri həbs etdilər. Həmlədən əldə etdikləri pulla dostlar, bir paytaxt cinayət qruplaşmasının üzvləri silah, maşın, geyim və s. almışdılar. Bələdçi də saxlanmışdır, yeri gəlmişkən, o öz qonorarını aldıqdan sonra işdən çıxmışdı.

Kiçik müəssisələr üçün ən böyük təhlükə mənbəyi kimi onların öz şəxsi əməkdaşları çıxış edirlər ki, onların da mühüm hissəsi əvəzçilik üzrə işləyirlər. Rusiyanın maliyyə və vergi-büdcə məsələləri üzrə qanunvericiliyinin hazırkı cansıxıcı vəziyyəti sahibkarlığın maliyyə resursları üzrə mənfi «təzyiqlərin» müxtəlif formalarını sahibkarlıq üzrə iqtisadi təhlükələrin ən geniş yayılmış formasına çevirir.

Sahibkarlığa qarşı yönəlmiş cinayətkar fəaliyyətin təhlili aşağıdakı nisbəti göstərir:

Cədvəl 1

1.	Şəxsiyyətə qarşı cinayətlər	4,3%
2.	Dələduzluq hərəkətləri	7,2%
3.	Oğurluq	49,9%
4.	Soyğunlar və quldurluq hərəkətləri	7,0%

5.	Etibar olunmuş əmlakın mənimsənilməsi	1,3%
6.	Maliyyə sahəsində fırıldaq	2,5%
7.	Digər cinayətlər	28,3%

Şərhlər: inzibati aparat tərəfindən olan təhlükələr aşağıdakı kimi bölüşdürülmüşdür: vergi müfəttişliyi tərəfindən – 20%; gömrük tərəfindən – 6%; müdiriyyət tərəfindən – 31%; bu bölüşdürmə qabaqcadan hasil olunmuş yanlış fikrə əsaslanan münasibət, dəstəklənmədə passivlik, şantaj və rəqiblərə yardım edilməsi amillərinin nəzərə alınması ilə aparılmışdır.

Sahibkarlıq üçün hədəfə şevrilən bəzi digər hərəkətlərinin ekspert xarakteristikasını da göstərmək olar (cədvəl 2):

Cədvəl 2

1.	Kommersiya fəaliyyətində dövlət strukturlarının iştirakı	31%
2.	Rəqiblərin sıradan çıxarılması üçün kriminal strukturlardan istifadə olunması	25%
3.	Qeyri-sağlam rəqabətlə effektiv mübarizə aparmaq üçün zəruri qanunvericilik bazasının olmaması	20%
4.	İqtisadi və informasiya casusluğu	20%
5.	Biznesi aparmaq üçün zəruri şərtlərin və mədəniyyətin olmaması, partnyorlara hörmət etməməsi, öhdəliklərin yerinə yetirilməməsi, müqavilə şərtlərinin pozulması	6%

İqtisadiyyatın yüksək inhisarçı səviyyəsinin saxlanması şəraitində sahibkarlıq üçün, xüsusilə kiçik sahibkarlıq üçün böyük təhlükə **ədalətsiz rəqabətdir**.

Ədalətsiz rəqabət dedikdə mövcud qanunvericiliyin şərtlərinə, işgüzar ənənələrə, şüur və ədalət tələblərinə zidd olaraq təsərrüfat subyektlərinin üstünlüyünün əldə olunması və digər təsərrüfat subyektlərinə - rəqiblərə zərər vurulması

və ya onların işgüzar reputasiyasının korlanması başa düşülür.

Qanunda belə deyilir:

Rusiya Federasiyasının «Əmtəə bazarlarında rəqabət və inhisarçılıq fəaliyyətbnin məhdudlaşdırılması haqqında» Qanunu.

Bölmə III. Ədalətsiz rəqabət.

Maddə 10. Ədalətsiz rəqabətin formaları.

Ədalətsiz rəqabətə yol verilmir, o cümlədən aşağıdakı formalarda:

- *başqa təsərrüfat subyektinin fəaliyyətinə və ya onun işgüzar nüfuzuna zərər vura bilən yanlış, qeyri-dəqiq və ya təhrif olunmuş məlumatların yayılması;*
- *əmtəənin istehsalının xarakteri, üsulu və yeri, istehlakçı xüsusiyyətləri və keyfiyyətinə münasibətdə istehlakçıların aldadılması;*
- *təsərrüfat subyektinin reklam fəaliyyəti zamanı onun tərəfindən istehsal edilən və ya reallaşdırılan əmtəələri başqa təsərrüfat subyektlərinin əmtəələri ilə qeyri-səhih müqayisə olunması;*
- *əmtəə nişanından, firma adından və ya əmtəə markasından özbaşına istifadə edilməsi, həmçinin başqa təsərrüfat subyektinin əmtəəsinin formasının, qablaşdırmasının, xarici tərtibatının təkrarlanması;*

elmi-texniki, istehsal və ya ticarət informasiyasının, o cümlədən kommersiya sirlərinin onların sahiblərinin icazəsi olmadan əldə edilməsi, istifadə edilməsi və yayılması.

Daha geniş planda ədalətsiz rəqabət – təsərrüfat subyektlərinin sahibkarlıq fəaliyyətində üstünlük əldə edilməsinə istiqamətlənmiş, qüvvədə olan qanunvericiliklə ziddiyyət təşkil edən və bazar subyektlərinə ziyan vura bilən istənilən fəaliyyətidir.

Ədalətsiz rəqabətin əsas prinsipi rəqibin mövqelərinin zəiflədilməsi və ya istehlakçıların aldadılması yolu ilə

bazarda öz mövqelərinin möhkəmləndirilməsidir. Bunun üçün rəqabət aparan firmalara birbaşa və ya dolayı yolla təsir göstərilir.

Belə hərəkətlərə aiddir:

-rəqibin mövqelərinin vurulması və onun bazardan çıxarılması məqsədilə özünün iqtisadi potensialından məhsulun maya dəyərindən aşağı qiymətlə satışı üçün istifadə olunması;

-bazardakı hakim mövqeyindən sui-istifadə (monopoliya);

- diskriminasiyalı kommersiya şərtlərinin təyin olunması;

- satışlarda gizli sövdələşmələr və gizli kartellərin qeyri-rəsmi yaradılması;

- reklama uyğun gəlməyən xarakteristikalı məhsulun buraxılışı;

- rəqiblər tərəfindən buraxılan orijinal məhsulların surətinin çıxarılması və istehsalı;

- öz məhsulun markalanması üçün ticarət nişanlarından qeyri-qanuni istifadə.

Ən geniş yayılmış ədalətsiz rəqabət forma və metodlarını aşağıdakı kimi xarakterizə etmək olar:

Cədvəl 3

1.	İqtisadi təzyiqlər: - sövdələşmə və digər sazişlərin pozulması; - dövlət orqanlarının, KİV-nin istifadə olunması ilə firmaların fəaliyyətinin iflic olunması; - ədalətsiz reklamla firmaların fəaliyyətinin zəiflədilməsi; - şantaj, rəhbər və ayrı-ayrı işçilərin ələ alınması.	 48% 31% 11% 10%

2.	Fiziki təzyiqlər: - oğurluq və ofislərə, anbarlara basqınlar; - fiziki təzyiqlər.	 73% 22%
3.	Sənaye casusluğu: - əməkdaşların ələ alınması; - sənədlərin və layihələrin ötürülməsi; -proqram və məlumatların sürətinin çıxarılması; - FEHM-lərə daxil olma; -danışıqlara qulaq asılması.	 43% 10% 24% 18% 5%

Sahibkarlığa əhəmiyyətli təhlükəni fırıldaqçılıq- yalan və ya etibardan sui-istifadə etməsi yolu ilə əmlaka sahib olma yaradır.

Fırıldaqçılıq yolu ilə əmlaka sahib olma yollarının özünəməxsus cəhətləri odur ki, cinayətkar sahibləri çaşqınlıq vəziyyətinə gətirir, onlar da öz növbəsində əmlaka sahiblik hüququnu könüllü surətdə ona verirlər.

Fırıldaqçılıq zaman yalan cinayətin icra olunma elementlərindən biri kimi çıxış edir, hüquqi sahibdən cinayətkarın qeyri-qanuni sərancamına keçir.

Qanunda belə deyilir:

Maddə 159 UK RF «Dələduzluq, aldatma və ya etibardan sui-istifadə etməklə başqasının əmlakının oğurlanması və ya başqasının əmlakı üzərində sahibliyin əldə edilməsidir».

Fırıldaq yalanının məqsədi-əmlak sahibini çaşqınlığa salmaq və onun əmlakı könüllü surətdə cinayətkarın sərəncamına ötürülməsinə nail olmaqdır.

Yalan hərəkətlərin formaları müxtəlifdir:

- dezinformasiya;
- saxta əməllər;
- yalançı sahibkarlıq və s.

Əmlakı cinayətkarcasına mənimsəmə üsulu kimi etibardan sui istifadə də çıxış edə bilər ki, bu zaman cinayətkar əmlakı əldə etmək üçün, ya onun əsasən tərəflərin etibarına əsaslanan müəyyən vətəndaş-huquqi

(razılaşma) münasibətlərini özünə tərəf çevirmək məqsədilə, ya da sahibinin sərəncamında olan əmlakı heç bir ehtiyat etmədən və müvafiq rəsmiləşdirmə aparmadan cinayətkarın sərəncamına verilməsi ilə mənimsəməsidir.

Nümunə. (Rusiya qəzeti 29.01.98)

Gerb möhürü dələduzların cibində

Biznesin orijinal üsulunu Kubanda Stavropoldan olan dələduz-qastroçular tapmışlar. Onlar bütün vilayət üzrə gəzmiş və özlərini vilayətin vergi müfəttişləri kimi qələmə vermişdilər. Sahibkarların sadəlövhlüyündən istifadə edərək, dələduzlar nəzarət-kassa apparatlarından istifadənin «yoxlanılmasını» həyata keçirmiş, aktlar hazırlamış, həmin aktların məhv edilməsi üçün isə təqsirli şəxslərdən bir milyondan altı milyona qədər rüşvət götürmüşlər. Onların üzərində saxta vəsiqələr və gerb möhürləri olmuşdur.

Vladimir Udaçin,
müxbir

Fırıldaqçılığın tipik növləri bunlardır:

1. Kassadan nağd vəsaitin oğurlanması:

- çeklərin oğurluğu;
- nağd vəsaitin təyinatı üzrə istifadə olunmaması;
- kassa kitablarının saxtalaşdırılması;
- bank hesablarındakı vəsaitlərin saxtalaşdırılması;
- çeklərin saxtalaşdırılması;
- təqaüd fonduna daxilolmaların təyinatı üzrə istifadə olunmaması;
- firmanın sexləri ilə şəxsi hesabların ödənilməsi;

2. Hesabların saxtalaşdırılması:
- nəqliyyat qaimələrinin saxtalaşdırılması;
- şişirdirmiş fakturalar.
3. İnventarın oğurlanması:
- müştərilər və ya malgöndərənlərlə gizli razılıq;
- müəyyən xidmətlərə görə "təşəkkür" alınması (rüşvət);
- qurma malgöndərənlərdən istifadə olunması;
- qiymətlərin artırılması.

4. Saxta veksellərin verilməsi.

5. Firmanın əmlakının şəxsi məqsədlər üçün istifadə olunması:
- sifarişlərin rüşvətlə verilməsi;
- kredit kartları ilə fırıldaqçılıq.

6. Mühasibat kitablarında qeydlərin saxtalaşdırılması:
- hesabların yaxşılaşdırılması üçün;
- çatışmazlıqları örtmək üçün.

7. Firmanın əmlakının qeyri-qanuni satışı: inventarın, avadanlığın, istehsal tullantılarının.

8. Əmək haqqı ödənişi ilə bağlı fırıldaqlar:
- tələb olunmamış çeklərin nağdlaşdırılması;
- ölmüş işçilərə əmək haqqı hesablanması.

9. Kompyuter cinayətləri:
- xarici şərtlərin təzyiqi;
- fırıldaqçılıq aktını icra etmək və müəyyən müddət gizlətməsi imkanı;
- şəxsi mənəvi keyfiyyətlər, hansı ki, cinayətkar fəaliyyəti təmizə çıxarır.

1. Xarici xərclərin təzyiqi maliyyə sferasında özünü göstərir. Bunlara aiddir:
- tamahkarlıq;
- vəsaitləri üzrə yaşamamaq;
- böyük borclar;
- alış və digər xidmətlərə görə böyük hesablar;
- pulun olmaması;

- pula qəflətən tələbat.

2. Məhvedici adət və vərdişlərin təzyiqi maliyyə şəraiti ilə sıx əlaqədardır. Onlara azartlı oyunlar, narkotik, içki, seksual hisslərin təmin olunması və s. aiddir. Qeyd etmək lazımdır ki, adət və vərdişlər fırıldaqçılıq amillərindən ən pisi sayılır, belə ki, onlar uzunmüddətli və daimi, bəzən də xroniki və sağalmaz xarakter daşıyır.

3. İşlə əlaqədar şəraitlərin təzyiqi yalnız rəhbərlik və ya kiminləsə hesab çürütmək zamanı fırıldaqçılıq baş verir. Motivlər: özünün uğurlarının qiymətləndirilməməsi, işdən razı qalmamaq hissi, onu itirmək qorxusu, layiq olduğundan az almaq hissi və s.

Fırıldaqçılıq fəaliyyətinin motivləri statistikaya görə belə təsnifləşir:

Cədvəl 4

№	Səbəblər	% nisbəti
1.	İçki və narkotiklər	67
2.	Emosional xarakterli problemlər	63
3.	Ailə problemləri	57
4.	Azartlı oyunlar	38
5.	Maliyyə çətinlikləri	37
6.	Digər problemlər	32

Düzgünlüyünə görə firmanın əməkdaşlarını belə təsnifləşdirmək olar:

- düzgün-40%
- nisbətən düzgün-30%
- qeyri- düzgün (fırıldaqçı)-30%

Yalançı sahibkarlıq – nizamnamə fəaliyyətinin həyata keçirilməsini nəzərdə tutmayan, ssudaların, kreditlərin əldə edilməsi, vergiyə cəlb olunmanın azladılması və ya qanunsuz yolla başqa mülki faydaların götürülməsi məqsədilə sahibkarlıq təşkilatlarının yaradılması da geniş yayılmışdır. Təsərrüfat aparan subyektin vəzifəli şəxsi tərəfindən

mənfəətin azaldılması və ya gizlədilməsi və ya başqa yolla vergilərin ödənilməsindən yayınma xüsusilə geniş yayılmışdır.

Maliyyə-kredit sferasında sui-istifadələrin sayı da nəzərə çarpacaq dərəcədə artmışdır. Bunların arasında aldatma yolu ilə kredit alınması, təmin olunmamış qiymətli kağızların buraxılması və yayılması, həmçinin onların emissiyası qaydasının pozulması, xaricə əhəmiyyətli məbləğdə pul vəsaitlərinin köçürülməsi üzrə qanunsuz əməliyyatlar, bank çeklərinin və kredit kartlarının saxtalaşdırılmasını göstərmək olar.

Sahibkarın kreditorlar qarşısında öz öhdəliklərini yerinə yetirinə bilmədiyini əvvəlcədən qazanc götürmək məqsədilə elan etməsi, həmçinin borclu sahibkar tərəfindən öz dayanıqlı ödəmə qabiliyyətinin reallığa uyğun gəlməyən məlumatlarla gizlədilməsi kimi təzahür edən yalançı və qəsdən müflisləşmək də mühüm ictimai təhlükə yaratmağa başlamışdır.

Təhlükəli fəaliyyətlərin və ya onları müəyyən edən şəraitlərin baş vermə ehtimalı necədir?

Hədələrin baş vermə ehtimalını bir neçə yolla müəyyən etmək olar:

Ən yaxşı vasitə riyazi statistika üsuludur. Verilənlərin statistik emalı əsasında baş verə biləcək hadisənin ehtimalı göstəricisi hesablanır.

Cədvəl 5

№	Hədə növləri	%	R (Ehtimal)
1.	Təbii fəlakət	25	0,4
2.	Elektrik və rabitə kəsilmələr	50	0,5
3.	İnformasiya sisteminə kənardan daxilolmalar	3	0,03
4.	İnformasiya sisteminin işinin daxili pozulması	70-75	0,7-0,75
5.	İncimiş əməkdaşların pis niyyətli hərəkətləri	10	0,1

6.	Personalın təhrik olunması	10	0,1
7.	Bilməyərəkdən səhvlər	50-55	05,-0,55

İqtisadi təhlükəsizlikdən danışdıqda, rəqiblər və ziyanvericilərdən gələ biləcək təhlükənin müəssisənin fəaliyyəti prosesindəki risklərlə əlaqələndirilməsi lazımdır. Risk-itki və ya zərərə səbəb olan hadisənin başvermə ehtimalının dəyər ifadəsidir.

Təsdiq etmək olar ki, **RİSK hər hansı itki və ya zərərə aparan hadisənin başvermə ehtmalının dəyər ifadəsidir.** Risk anlayışı bütün növ kommersiya fəaliyyətləri, investisiya layihələrinin həyata keçirilməsi üçün təbiidir və mütləq olaraq yalnız sahibkarlığın müxtəlif növlərinin iqtisadi təhlükəsizliyini pozan amillərlə təcəssüm olunmur. Misal üçün, kommersiya bankları kiçik müəssisələrin maliyyələşdirilməsi zamanı risklərin artmasından ehtiyat edirlər. Kreditlərin geri qayıtmaması mümkünlüyünü azaltmaq üçün Rusiya MB bir müştəri üzrə risk normativi işləyib hazırlamışdır. Bu normativin aşılması MB-ın həmin bankdan lisenziyanın müsadirə etməsi üzrə qərar qəbul etməsinə gətirib çıxara bilər. Məhz kiçik müəssisələrin kreditləşdirilməsinin ən riskli iş olması üzündən, bu normativə riayət edilməsi sahibkarlara kredit verilməsi zamanı formal bəhanə kimi çıxış edir.

RİSK, iqtisadi kateqoriya kimi özündə baş verən və baş verməyə bilən hadisələri əks etdirir. Nəticə etibarı ilə, riskli hadisənin baş verməsini müəyyən dərəcədə proqnozlaşdırmağa imkan verən müxtəlif üsullardan istifadə edərək riski idarə etmək və onun səviyyəsinin aşağı salınması üzrə tədbir görmək olar.

Sahibkarlıq fəaliyyəti ilə bilavasitə əlaqədar olan riskləri kommersiya, investisiya, valyuta-maliyyə kimi kateqoriyalara bölmək olar.

1. Kommersiya riskləri təsərrüfat fəaliyyəti prosesində itki imkanına təsir edir. Onlar konkret kommersiya

sövdələşməsinin nəticələrinin qeyri-müəyyənliyini ifadə edir. Kommersiya riskləri əmlak, istehsal, ticarət və nəqliyyat risklərinə bölünür:

- əmlak riski oğurluq, soyğun, müxtəlif səbəb və şərtlərdən məhv olmaq üzrə əmlakın itirilməsi ehtimalıdır;
- istehsal riskləri istehsal prosesinin müxtəlif səbəblər üzərindən pozulmasıdır;
- komplektləşdiricilərin çatdırılmaması, əsas və ya dövriyyə fondlarının zədələnməsi və ya məhv olunması, istehsal texnologiyasının pozulması və s.;
- ticarət riskləri müxtəlif nəqliyyat vasitələri ilə yüklərin daşınması ilə bağlıdır.

2. İnvestisiya riskləri əldən çıxmış gəlir, mənfəətliyin azalması və birbaşa maliyyə itkilərinə bölünür:

-Əldən çıxmış gəlir- hər hansı bir sövdələşmənin qırılması nəticəsində mənfəətin əldə olunmamsı itkisidir;

- gəlirliyin aşağı düşməsi- əmanət və kreditlər üzrə faiz və dividendlərin dərəcəsinin azalması nəticəsində baş verə bilər;
- Birbaşa maliyyə itkiləri riski- birja riski, iflas olma riski, selektiv risk, həmçinin kredit riskidir;

-birja riski- birja sazişlərindən itkilərdir. Onlar kommersiya sazişləri üzrə ödənişlərin və ya broker firmasının komisyon mükafatının ödənilməməsi risklərini özündə əks etdirir;

- selektiv risklər- kapital qoyuluşu üçün düzgün formasının seçilməməsi riskidir;
- iflasolma riski – sahikar tərəfindən düzgün olmayan kapital qoyuluşu nəticəsində şəxsi kapitalın itirilməsi və öhdəliklərini yerinə yetirə bilməməsi ehtimalıdır.

3. Valyuta-maliyyə riskləri. Maliyyə resurslarının itirilməsi ilə əlaqədar risklərdir. Bura pulun alıcılıq qabiliyyəti və kapital qoyuluşu ilə bağlı risklər aiddir.

Pulun alıcılıq qabiliyyəti ilə bağlı risklərə inflyasiya, deflyasiya, valyuta və likvidlik riskləri aiddir:

- inflyasiya riski alıcılıq qabiliyyətinin aşağı düşməsinə, deflyasiya isə- qiymətlərin səviyyəsinin düşməsi əsasında gəlirlərin azalmasına gətirib çıxarır.
- valyuta riski – xarici valyuta kursunun dəyişməsi ilə əlaqədar valyuta itkilərini ifadə edir.
- likvidlik riskləri – qiymətli kağızların və digər əmtəələrin realizasiya zamanı keyfiyyətlərinin və istehlak dəyərinin dəyişməsi nəticəsində itkilərin yaranma ehtimalıdır.

Sahibkarlıq riskləri ilə yanaşı təbii risklər, siyasi risklər, ekoloji risklər də mövcüddür, hansı kı, onların fəaliyyət xarakteri sosial-siyasi sferadan nisbətən az asılıdır. Sahibkar bu faktorlara bilavasitə təsir etmək imkanına malik deyil, lakin onların baş verməsi ehtimalını öz fəaliyyətində nəzərə almalıdır.

1.2. Sosial hədələr

Sahibkarlığa sosial hədələr ölkədəki iqtisadi və siyasi qeyri-sabitliklə əlaqədardır, hansı ki, işsizlik, yoxsulluq, cəmiyyətin sosial-iqtisadi təbəqələşməsinə səbəb olur. Sahibkarlığa münasibətdə bu şərait iri əhali təbəqəsinin biznesə daxil olmasına əngəllər törədir. Kiçik bə orta biznes müəssisələrinin qeyri-stabil fəaliyyəti onların çoxunun iflasına gətirib çıxarır ki, bu da işsizliyə səbəb olur.

Sosial hədələri bir neçə əlamətə görə də təsnifləşdirmək olar:

- sahibkarların sosial maraqlarına zidd istiqamətlər üzrə;

- miqyas üzrə (yerli, lokal, firma, müəssisə miqyasında);
- səbəblər üzrə (mülkiyyətin, gəlirlərin, hakimiyyətin ədalətsiz bölgüsü).
-

1.3. İnformasiya ötürmə hədələri

Məlumdur ki, informasiya – bilik və praktiki qərarların əldə olunması məqsədilə istifadə edilən, material daşıyıcılarında əks etdirilən şəxslər, predmetlər, hadisələr və priseslər haqqında məlumatlardır. İnformasiya bu gün ən vacib resurslardan biridir. İnformasiya, informasiya resurslarına münasibətdə aşağıdakı hədə növlərini aid etmək olar:

- müxtəlif yollarla konfidensial informasiya ilə tanışlıq;
- ziyanvericilərin marağı üçün informasiyanın modifikasiyası;
- informasiyanın yox edilməsi (vandalizm faktları).

Bu hədələr aşağıdakı yollarla həyata keçirilə bilər:

- konfidensial informasiya mənbələrinə qeyri-rəsmi yolla giriş;
- kommersiya sirri ilə bilavasitə əlaqəli olan müəssisə əməkdaşlarının ələ alınması;
- rabitə vasitələri ilə ötürülən informasiyanın ələ keçirilməsi;
- müxtəlif strukturların nümayəndələri arasında danışıqlar prosesi vasitəsilə və s.

Sahibkarlıq üçün informasiya informasiya xarakterli hədələri də daxili və xarici kimi təsnifləşdirmək olar:

Daxili hədələrə sahibkarlıq strukturlarının informasiya resurslarına bilərəkdən və ya təsadüfən mənfi təsirlər: sahibkarın kommersiya sirri olan məlumatlarla tanışlıq, cinayətkar məqsədlər üçün informasiyanın tərkibi

və strukturunun dəyişdirilməsi (saxtalaşdırılması) və ya onun sahibkara maddi və mənəvi zərər vurmaq üçün tam məhv edilməsi aiddir.

Daxili hədələrə həmçinin texniki kanallar vasitəsilə sızması halları daxildir.

Xarici hədələrə sahibkarların yeni qanunlar və digər normativ aktlar, xüsusilə, təsərrüfat fəaliyyətinin lisenziyalaşdırılması, vergi siyasəti, güzəşt və üstünlüklər haqqında informasiyaya girişin ya olmaması, ya da qismən olması aiddir.

İnformasiya sahəsində xarici hədələrə həmçinin ədalərsiz rəqabət, sənaye çəsusluğu, rəqibin məhsulu və onun maliyyə vəziyyəti haqqında yalan informasiyanın yayılması və s. aiddir.

Həm daxili, həm də xarıcı hədələr sahibkarlara onların istehsal, kommersiya fəaliyyətində bu və ya digər formada zərər vura bilər.

1.4. Korrupsiya sahibkarlığa təhlükə faktoru kimi

Bütün səviyyələrdə korrupsiya ölkənin həyat və fəaliyyətinə, o cümlədən kiçik və orta biznesə hərtərəfli dağıdıcı təsir göstərir.

Mənfi təsirlər bütün sferalarda öz təsirini göstərir. Məsələn, iqtisadi sahədə bu təsirlər aşağıdakı formalarda öz əksini tapır:

1. Kölgə iqtisadiyyatı güclənir;
2. Bazarın real rəqabət mexanizmi pozulur.

3. Bazar iştirakçılarının hakimiyyətin düzgün bazar qaydaları müəyyən etməsi və əməl etmək qabiliyyətinə inamı itir.
4. Qeyri-hökumət orqanlarında korrupsiyanın migyası artır;
5. Qiymətlər korrupsion "qaimə xərcləri" hesabına artır.

1997-ci ildə korrupsiyadan (ictimai dövlət xadimlərinin və məmurlarının rüşvətxorluğundan) iqtisadi itkilər 49 trilyon rubl (denominasiya olunmamış) təşkil etmişdir ki, bu da büdcənin 20%-ni təşkil edirdi [30].

«XXI əsrin texnologiyaları» adlı ictimai təşkilatın ekspertlərinin hesablamalarına görə kiçik sahibkarlar ölkədə məmurlara rüşvət verilməsi üzrə ay ərzində minimum 500 milyon dollar pul sərf edirlər. İl ərzində bu məbləğ 6 milyard dollara çatır. Əvvəlcədən aparılmış təhlil göstərir ki, kiçik və orta sahibkarlıqda ümumi gəlirin 10%-i korrupsiya müqavilələrinə sərf edilir. Bu zaman ilkin mərhələdə (qeydiyyat və s.) məsrəflər əhəmiyyətli dərəcədə çox olurlar. «Biznesə giriş» müxtəlif ranqdan (səviyyədən) olan təxminən 50-yə yaxın məmurun qərarını tələb edir. Əgər buraya müəssisələrin özlərinin daxilindəki münasibətlərin korrupsiyalaşmasını da əlavə etsək, onda bizim ölkədə korrupsiya üzündən itirilən vəsaitlərin ümumi məbləği 10-dan 20 milyard dollara qədər təşkil edəcəkdir.

Nümunə. «Rusiya qəzeti» 21.2.98-ci il

«Sahibkarı cəzalandırılmadan hər kəs soya bilər…». Nijeqorodskoy şəhərindən olan məşhur sahibkar və jurnalist, Nijeqorodskoy ticarət-sənaye evinin baş direktoru (general meneger) Vladimir Noskovla keçən ilin 12 noyabrında aparılmış söhbətin başlığı belə adlanırdı.

Həmin söhbətdə mənim həmsöhbətim hüquq-mühafizə orqanlarının açıqdan-açığa kiçik sahibkarlıqla məşğul olan

biznesmenləri soyduqları haqqında danışdı. 1996-cı ilin avqustunda Vladimirskiy vilayətinin Petuşki şəhəri rayonunda Nijeqorodskoy ticarət-sənaye evinin təchizat şöbəsinin rəisi tez-tez hücuma məruz qalırdı. 60 milyon rubl oğurlanmışdı. Ancaq hüquq-mühafizə orqanlarına edilən bütün müraciətlər cavabsız qalırdı. Ərizələr polis idarəsinin bir şöbəsindən digərinə göndərilirdi. Son nəticədə polis təşkilatı qərar çıxardı: «oğurluq faktı sübut olunmadığından» iş bağlanır.

(Yuriy Şukov)

1997-ci ildə məsuliyyətə cəlb olunmuş korrupsiyalaşmış (rüşvətlə ələ alınmış) şəxslərin tərkibi və strukturu cədvəl 7-də göstərilmişdir.

Cədvəl 7

№	Tərkib	%
1	Nazirliklərin, komitələrin və yerli strukturların işçiləri	41,1
2	Maliyyə-kredit sisteminin işçiləri	11,7
3	Hüquq-mühafizə orqanlarının əməkdaşları	26,5
4	Gömrük xidmətinin işçiləri	3,2
5	Nəzarət orqanlarının işçiləri	8,9
6	Deputatlar (millət vəkilləri)	0,8
7	Digərləri	7,8

Korrupsiyanın sosial nəticələri bunlardır:

1. Kəskin əmlak bərabərsizliyi, əhalinin böyük hissəsinin yoxsulluğu güclənir və artır;
2. Hüquq-mühafizə orqanlarının korrupsiyaya qurşanması mütəşəkkil cinayətkarlığın güclənməsinə səbəb olur;
3. Sosial gərginlik dərinləşir;

Siyasi nəticələr:

1. Hakimiyyət organlarına inam azalır;
2. Beynəlxalq bazarda iqtisadi və siyasi təcrid olunma təhlükəsi artır;
3. Oliqagarxiyaların hakimiyyəti imkanı artır və s.

Demək olar ki, korrupsiya, onun miqyası, dinamikası-ölkənin ümumi siyasi, sosial və iqtisadi problemlərinin nəticəsidir.

1.5. Hüquqi hədələr

Hüquq-xarakterli təhlükələr təsərrüfat fəaliyyəti prosesini tənzimləyən sabit, ziddiyyətsiz, dəqiq müəyyən olunmuş qanunvericiliyin olmamasının nəticəsidir. Mövcud qanunvericilikdə boşluqların olması mənfəətin, real gəlirlərin gizlədilməsi, təsərrüfat-maliyyə əməliyyatlarında müxtəlif manevrlər etməyə, həmçinin sahibkarlığa birbaşa kriminal təsirin göstərilməsinə gətirib çıxarır. Pozuntuların əsas növləri bunlardır:

- sahibkarların əmlakına sahib olma;
- regionlararası məhsul hərəkətinə məhdudiyyətlər;
- qiymətlərin qeyri-qanuni tənzimlənməsi;
- müəssisənin daxili işlərinə qatışmaq;
- müəssisələrin fəaliyyətinin inzibati tənzimlənməsinə cəhd etmək.

Müəyyən hüquqi təhlükələr (inzibati özbaşnalıq üzrə təhlükələr) təsərrüfat fəaliyyətinin lisenziyalaşdırılması təcrübəsində də mövcuddur. RF-nın 1998-cil 16 sentyabr tarixli «Fəaliyyətlərin ayrı-ayrı növlərinin lisenziyalaşdırılması» haqqındakı qanununa baxmayaraq, sahibkarlıq sahəsində hələ də inzibati-hüquqi təhlükə sferaları qalmaqdadır. Mahiyyət etibarı ilə, lisenziyalaşdırma adı altında çox vaxt yerlərin sertifikatlaşdırılması aparılır; bir sıra hallarda lisenziyalar aylıq, rüblük, ən yaxşı halda isə yarımillik verilirdi və hazırda da bu müddətlərə verilməkdədir. Bununla əlaqədar olaraq, lisenziyanın vaxtının uzadılması üçün sahibkar yenidən çoxsaylı instansiyalardan keçməli və bu pillələrin hər birində həm rəsmi, həm də «qeyri-rəsmi» haqlar ödəməlidir.

Bundan başqa, lisenziya verən orqanlara lisenziyaların fəaliyyətini dayadırmaq hüququ da verilmişdir. Bu hüquqdan istifadə edərək verilən orqanlar lisenziyanın fəaliyyətini dayandıra bilərlər ki, bu da sahibkarlıq fəaliyyətinin dayandırılması deməkdir. Nəticədə təkcə sahibkarın özü üçün yox, həm də onun partnyorları üçün maliyyə itkiləri baş verə, iş müflisləşmələr zənciri ilə bitə bilər.

Ayrı-ayrı hallarda işçilərin səriştəsizliyi ilə tamamlanan normativ-huquqi təminatın qeyri-dəqiqliyi münaqişəli (sahibkarlar üçün riskli), bəzən isə kriminal fəaliyyətlərə keçən situasiyalara gətirib çıxarır. Rus sahibkarı üçün mövcud vergiyə cəlb olunma təcrübəsi üzrə təhlükə hazırki dövrdə qüvvədə olan qanunvericiliyin qeyri-stabilliyi, onun bir tərəfdən vergiyə cəlb olunmadan müxtəlif üsullarla yayınma imkanlarının olması, digər tərəfdən isə bir sıra vergilərin həddən artıq yüksək, bəzi vergilərin isə ümumiyyətlə lazımsız olması, həmçinin federal Mərkəzin regionlarla vergi-büdcə münasibətlərindəki qeyri-müəy-yənliklər nəticəsində ortaya çıxır.

Vergi qanunvericiliyinin qeyri-stabilliyi xarici sahibkar-lar üçün də bir sıra riskli situasiyalar yaradır ki, buna da Rusiya-amerikan ticarət palatasının 47 xarici firma arasında apardığı sorğu şahidlik edir. Onlara belə bir sual verilmişdi ki, onlar Rusiyadakı bizneslərində ən ciddi problem kimi nələri hesab edirlər. 42 firma belə cavab verdi ki, belə ciddi problem vergi qanunvericiliyinin qeyri-stabilliyi və qeyri-müəyyənliyidir, 41 firma həmçinin əməyin ödənilməsinin yüksək normativli fondu üzrə vergi ilə bağlı problemləri qeyd etdi. Üçüncü yerdə – 16 dəfə – əlavə dəyər vergisi ilə bağlı, hər şeydən əvvəl, «firmalararası» ssudalar üzrə problemlər qeyd edilmişdi.

1.6. Kriminal təhlükələr

Rusiya DİN-nin məlumatlarına görə, hazırki dövrdə «kriminal strukturlar» ölkə üzrə 50%-dən çox təsərrüfat subyektlərini nəzarətdə saxlayır. Qeyri-leqal qruplaşmalar kommersiya strukturuna o vaxta qədər güc təzyiqləri göstərirlər ki, onlar müntəzəm haqq verməyə razı olsunlar. Bunun əvəzində isə reketirlər özünü mafiyadan qorumaq üçün vəsaitlərə malik olmayan həmin strukturu qoruyurlar. Belə strukturlar mafiyanın təzyiqi altında qalırlar və bir qayda olaraq, belə təzyiqi öz gücləri ilə dəf etmək iqtidarında olmurlar.

Kriminal təhlükələr həmçinin ondan yaranırlar ki, qeyri-qanuni yolla qazanılmış iri məbləğdə pullar mafiyanı həmin pulları leqallaşdırmaq yollarını axtarmağa vadar edir. Mafiya sahibkarları məcbur edir ki, onlar həmin kölgə kapitalını öz dövriyyələrinə alsınlar və müəssisə üzərində bu və ya başqa formada nəzarəti onlara versinlər. Sonuncu kriminal strukturların sahibkarlığa təsirini daha da gücləndirir. RAN analitik mərkəzinin hesablamalarına görə, kapitalın 39%-i, «səsvermə hüququna» malik səhmlərin isə 80%-i kommersiya strukturlarından haqların, o cümlədən səhmdar kapitalın bir hissəsi şəklində alınması vasitəsilə kriminal kapitalın əlinə keçmişdir. Ancaq mafiyanın əsas leqallaşdırma forması şəxsi kommersiya strukturlarının yaradılmasdır. Ümumi halda, hazırki dövrdə kriminal münasibətə sahibkarların 40%-i, bütün kommersiya strukturlarının isə 80%-i cəlb edilmişdir. Mafiya tərəfindən 35 min təsərrüfat subyekti üzərində nəzarət qurulmuşdur ki, bunların arasında 400 bank, 47 birja, 1,5 min dövlət sektoru müəssisəsi var.

Son dövrlər kommunikasiyanın və hesablaşmaların elektron formalarının inkşafı ilə saxta ödəniş sənədlərinin əldə edilməsi, veksellərdən istifadə etməklə vəsaitlərin, arbitraj əmrlərinin, səhmlərin və istiqrazların oğurlanması üçün kompyuter şəbəkələrinə nüfuz edilməsi də geniş yayılmışdır.

«Elektron cinayətkarlığın» yayılması kompyuter şəbəkələrinin kifayət qədər aşağı mühafizə olunma səviyyəsinə malik olması və «dələduzların» artan səriştəlilikləri ilə də izah olunur.

Nümunə

Bir müddət əvvəl Moskvada 68 milyard rubl məbləğində «elektron cinayətkarlığa» cəhdin qarşısı alınmışdır.

Cinayətkarlar bir sıra kommersiya strukturları - səkkiz Moskva bankının müştəriləri, o cümlədən iri və məşhur müştərilərlə əlbir fəaliyyət göstərir və modem əlaqəsindən istifadə etməklə bir sıra saxta ödənişlər həyata keçirməyi planlaşdırırdılar. MB-ın baş idarəetməsi hiylə təşkilatçılarının həm proqramlaşırma sahəsində, həm də kommersiya bankları ilə hesablaşma-kassa mərkəzi arasında elektron hesablaşmalar üzrə məsələlərdə yüksək hazırlıq dərəcəsinə malik olmalarını qeyd etmişdi. Və yalnız banklararası ödəniş sistemlərinin mühafizə edilməsi məqsədilə aparılan tədbirlər sayəsində bu hiyləni vaxtında aşkara çıxarmaq və onun qarşısını almaq mümkün olmuşdu.

Kriminal təhlükələrin yayılmasına kömək edən amillər:

Xarici:

- yaxın və uzaq xarici ölkələrdə terrorizmin təzahürlərinin obyektiv surətdə artması;
- həmsərhəd ölkələrdə sosial-siyasi və iqtisadi qeyri-stabillik, onlardan bəzilərində silahlı münaqişələrin olması;
- bəzi xarici xüsusi xidmət orqanlarının və xarici terrorçu təşkilatların strateji qurumları;
- sərhədlərin «şəffaflığı» və giriş-çıxış rejimləri üzərində etibarlı nəzarətin olmaması;

- Rusiyaya xaricdən qeyri-leqal silah, hərbi sursat və dövriyyə üçün başqa qadağan olunmuş əşya və predmetlərin gətirilməsi kanallarının mövcud olması;
- Rusiyadan kənarda rus diasporasının əmələ gəlməsi.

Daxili:

- ölkədə böyük həcmdə silah «bazarının» mövcud olması və silahın əldə edilməsinin nisbətən asanlığı;
- hərbi məktəb keçmiş əhəmiyyətli sayda şəxs kontingentlərinin mövcud olması və onların cəmiyyətdə kifayət qədər sosial adaptasiyasının olmaması;
- bir sıra inzibati rejimlərin əhəmiyyətli dərəcədə zəifləməsi;
- bir sıra ekstremist qruplaşmaların mövcud olması və fəaliyyəti;
- sosial nizamsızlıq (pozğunluq) və müdafiəsizlik hissinin kəskinləşməsi;
- hüquq-mühafizə orqanlarının və vətəndaşların hüquqlarının müdafiə olunması üzrə təşkilatların zəif işləməsi.

Kriminal təhlükələrin sferalar və illər üzrə yayılmasını ifadə edən statistik göstəricilər aşağıdakı cədvəllərdə təqdim edilmişdir (cədvəl 8, 9).

Cədvəl 8

İllər	**Fiziki və psixoloji zordan istifadə etməklə həyata keçirilən cinayətlərin sayı**	**%**
1986	30299	44
1990	89109	7,6
1991	107521	6,8
1995	161425	7,7

Cədvəl 9

№	Göstəricilər/illər	1990	1991	1992	1993	1994	1995
1	Sui-qəsdli qətl	17124	17746	24448	31246	343024	31001

2	Ölümlə hədələmə, ağır bədən xəsarətlərinin vurulması, əmlakın məhv edlilməsi	8020	8114	9420	19375	45864	
3	Qəsdən ağır bədən xəsarətlərinin vurulması	40962	41195	53286	66864	67706	61734
4	İnsan oğurluğu				110	499	628
5	Giriov götürülməsi	1			3	51	118

1.7. Təsərrüfat cinayətləri

Təsərrüfat cinayətləri qorunan maraqlardan asılı olaraq 3 əsas qrupa bölünür:

a) mülkiyyət formasından asılı olmayaraq dövlətin və ya hər hansı təsərrüfat subyektinin bilavasitə maraqlarına zərər vurulması və ya real təhlükənin yaranması ilə baglı cinayətlər;
b) vətəndaşların maraqlarına zərər vurulması və ya ciddi təhlükənin yaranması ilə bağlı cinayətlər;
c) həm dövlətin və təsərrüfat subyektlərinin, həm də vətandaşların maraqlarının pozulması yolu ilə xalq təsərrüfatının aparılması və təşkili sahəsində ziyan vurulması ilə bağlı cinayətlər;

Təsərrüfat cinayətləri aşağıdakı fəaliyyət sferasına istiqamətlənir:

a) sahibkarlıq fəaliyyəti sferasında cinayətlər;
b) antiinhisar qanunvericiliyin və digər qanunların pozulması ilə baglı cinayətlər;
c) istehlakçıların hüquqlarını müdafiə sferasında cinayətlər;

d) vergi sferasında cinayətlər;
e) valyuta cinayətləri;
f) maliyyə-kredit sferasında cinayətlər;
g) xarici-iqtisadi fəaliyyətin həyata keçirilməsi sferasında cinayətlər və s.

1.8. Siyasi təhlükələr

Siyasi təhlükələr beynəlxalq münaqişələr, onların yüksək gərginlik mərhələsinə keçməsi nəticəsində yaranır. Siyasi qeyri-sabitlik yerlərdə icraedici və qanunverici hakimiyyətlərin münaqişələri ilə əlaqədardı. Regionda siyasi situasiya onun investisiya mühitini müəyyən edən fondlardan biridir.

1.9. Kiçik sahibkarlığın təhlükəsizliyinin real vəziyyəti

Ölkədə mürəkkəb sosial-iqtisadi vəziyyət, istehsalın aşagı düşməsi, sosial sferada böhran, mütəşəkkil cinayətkarlıq, cəmiyyətin ümumi kriminallaşması və idarəetmə orqanlarının korrupsiyalaşması biznesin təhlükəsizliyinə böyük zərbə vurur.

Kiçik sahibkarlığın təhlükəsizlik vəziyyətinin qeyri-müntəzəm izlənməsi, bu problemlər üzrə «İqtisadi təhlükəsizlik və informasiyanın qorunması» seminarının (İnformasiya işçilərinin ixtisaslarının artırılması institutu) dinləyicilərinin anketləşdirilməsi və kiçik sahibkarlıq nümayəndələrinin 1-ci Ümumrusiya qurultayının iştirakçılarının ekspress-sorğusunun nəticələrinin işlənməsi kiçik müəssisələrin təhlükəsizliyinin aşağıdakı vəziyyətdə olduğunu göstərmişdir.

Sahibkarlıq sferasının vəziyyətinin hansı qiymətə malik olması barəsindəki suala cavab olaraq, biznesdə işləyən 3 respondentdən 2-si «qeyri-kafi» cavabını verdi. Cəmi 35 respondentə yaxşı qiymət verdilər. Ən qəmgin mənzərəni

ticarət sferasının sahibkarları timsalında müşahidə etmək olar (sahənin sahibkarlarının 80%-i qeyri-kafi qiyməti vermişdi). Son il ərzində sahibkarların 45%-i oğurluqların, qarətlərin, dələduzluqların və başqa mülki cinayətkarlıqların qurbanı olmuşdur. Ticarət sferasında bu rəqəm 59%-ə çatır. Mühafizə firmaları arasında əməkdaşlara, onların qohumlarına və yaxınlarına qarşı tətbiq edilən zorakılıq barəsində soruşulanların 55%-i məlumat vermişdi.

Eyni zamanda təhlükəsizliyin kompleks təmin edilməsi üzrə tələblərin yerinə yetirilməsi dərəcəsi yalnız müəssisələrin altıda birində reallaşdırılmış kimi qiymətləndirilir. Qalan müəssisələrdə bu tələblər reallaşdırılmamışdır.

Təhlükəsizliyin təmin edilməsinin ayrı-ayrı istiqamətləri üzrə də eyni nəticələr göstərilir.

Bəs təhlükəsizlik necə təmin olunur?

1. Sahibkarlıq üzrə təhlükəsizliyin təmin edilməsi üzrə tammiqyaslı tələblər yalnız 20% sorğulanan müəssisələrin nizamnamələrində möhkəmləndirilmiş, 60%-ində isə bu tamamilə yer almamışdır.
2. İqtisadi təhlükəsizlik və informasiyanın qorunması üzrə tələblər sorğulananların 12%-nin kollektiv razılaşmasında nəzərə alınmış, 88%-ində isə nəzərə alınmamışdır.
3. Daxili əmək-nizam qaydalarında təhlükəsizlik üzrə tələblər sorğulanan müəssisələrin yalnız 48%-ində nəzərə alınmışdır.
4. Təhlükəsizlik üzrə tammiqyaslı tələblər yalnız 13% müəssisələrin əmək müqaviləsində (kontraktında) mövcuddur. 32% müəssisədə isə ayrıca tələblər mövcuddur. Sorğulanan müəssisələrin 55%-inin əmək müqaviləsində belə tələblər yoxdur.
5. Sorğulananların mühüm hissəsi bölmələr üzrə vəziyyətlərdə və öz əməkdaşlarının funksional öhdəlik-

lərinə münasibətdə təhlükəsizlik üzrə tələblərin tamamilə mövcud olmamasını bildirmişdir.

6. Müəssisənin kommersiya sirrini təşkil edən məlumatlar siyahısına yalnız 25% müəssisə malikdir, yerdə qalanlar hətta məhdud siyahı şəklində belə bu tip məlumatlara malik deyildirlər.
7. «İnformasiya resurslarının təhlükəsizliyi necə təşkil olunmuşdur» sualına aşağıdakı cavablar alınmışdır: etibarlı mühafizə təşkil olunmuşdur – 13%, orta dərəcəli mühafizə – 6%, tamamilə mühafizə olunmur – 81%.
8. Əmlakın, maddi və maliyyə qiymətlilərinin mühafizəsinin texniki vasitələri 20% müəssisələr tərəfindən kifayət qədər geniş, 6% tərəfindən məhdud şəkildə, 13% tərəfindən ayrı-ayrı zoanalarda istifadə edilir, 71% tərəfindən isə ümumiyyətlə istifadə edilmir.
9. Məxfi informasiyanın mühafizəsi üçün sorğulananların yalnız 20%-i texniki vasitələrdən istifadə edirlər.

Sorğunun yekunları üzrə aşağıdakı fikirləri söyləmək olar:

1. Mühafizənin ümumi vəziyyəti həddən artıq zəifdir. Sorğulananların 60%-indən çoxu ümumiyyətlə mühafizə olunmur. Əksər müəssisələrin ayrı-ayrı təhlükəsizlik sferaları məhdud tədbirlərlə xarakterizə olunur və öz maraqlarının kompleks mühafizə olunmasına oriyentasiya etmir.
2. Kiçik müəssisələr şəxsi təhlükəsizliklərinin təmin edilməsi üçün praktiki olaraq ştatlı struktur bölmələrinə malik deyildirlər.
3. Mühafizə, müdafiə və informasiyanın qorunması üzrə texniki vasitələrdən məhdud şəkildə istifadə edilir.

Təhlükəsizliyin və informasiyanın qorunmasının belə vəziyyətini yalnız sahibkarlıq fəaliyyətinin təhlükəsizliyinin

təmin edilməsinin vacibliyinin başa düşülməməsi, «kim ki qorunmur – o hər şeyi itirir!» qaydasının tamamilə yaddan çıxarılması kimi izah etmək olar.

Bölmənin yekunu kimi onu da iddia etmək olar ki, sahibkarlıq üzrə təhlükələrin aşağıdakı aspektləri artıq dəqiq olaraq müəyyən edilmişdir:

- sahibkarın özünün təhlükəsizliyi üzrə təhlükələr;
- sahibkarın ədalətsiz fəaliyyəti zamanı məhsul və xidmətlərin istehlakçısının təhlükəsizliyi üzrə təhlükələr;
- sahibkarlıq informasiyası üzrə təhlükələr;
- cəmiyyətin (dövlətin, əhalinin) təhlükəsizliyi üzrə təhlükələr.

Sahibkarlığın təhlükəsizliyi üzrə təhlükələrin əsas mənbələri aşağıdakılardır:

- xüsusi şəxslər tərəfindən reket (bunu sorğulananların 64%-i bildirmişdi);
- firmaların əməkdaşları və ya onların ailə üzvləri üzrə real fiziki zorakılığın mümkünlüyü (54%);
- hüquq-mühafizə və nəzarət orqanlarının nümayəndələri (49%) və başqa dövlət strukturları (40%) tərəfindən şantaj (zorla əldə etmə);
- hökumətin qanunsuz fəaliyyətləri (39%).

Təhlükəsizliyin aşağıdakı sosial aspektləri müəyyən edilmişdir:

- əmlakın, gəlirlərin, həyati nemətlərin, hakimiyyətin ədalətsiz bölgüsü;
- vacib sosial institutların məhv edilməsi;
- islahat siyasətinin qeyri-çevik, antisosial xarakteri;
- xarici kapitalın milli sferaya daxil olması və milli infrastrukturu mənimsəməsi.

İqtisadi təhlükəsizlik üzrə təhlükələr aşağıdakılardır:

A) iqtisadi sistemlərin optimal fəaliyyətinin pozulması:

- əsas sferalarda istehsalın dağılması;

- iqtisadiyyat üzərində dövlət idarəetməsinin, vergiyə cəlb edilmə, qiymətəmələgəlmə, xarici ticarət üzərində lazımi nəzarətin itirilməsi;
- xalq təsərrüfatının tarazlığının pozulması;
- pul və maliyyə-kredit sisteminin fəaliyyətinin pozulması;

B) təbii resursların nəzarətsiz olaraq oğurlanması (dağıdılması);

V) xarici kapitalın milli iqtisadiyyatın əsas sahələri üzrə nəzarətinin təyin edilməsi;

Q) intellektual potensialın kənara axması.

Təhlükələrin xarici mənbələrinə aşağıdakılar aiddir:

- xarici dövlətlərin kəşfiyyat və xüsusi xidmət orqanlarının fəaliyyətləri;
- xarici qeyri-dövlət struktur və təşkilatlarının ölkənin təhlükəsizliyi və maraqları ilə bir araya sığmayan fəaliyyəti;
- xarici dövlətlərin və beynəlxalq kriminal qruplaşmaların, strukturlarının və ayrı-ayrı şəxslərin cinayətkar fəaliyyətləri.

Təhlükələrin daxili mənbələrinə aiddir:

- hüquqi və fiziki, həmçinin başqa şəxslərin informasiyanın formalaşdırılması, istifadə edilməsi və yayılması sahəsində qanunsuz fəaliyyətləri, o cümlədən onlar tərəfindən informasiyanın toplanması, işlənməsi və istifadə edilməsinin təyin edilmiş qaydalarının pozulması;
- rəqiblərin və onlar tərəfindən istehsal edilən məhsulların nüfuzdan salınması məqsədilə ədalətsiz rəqabət və sənaye casusluğu, rəqiblərin konkret bazarlardan qeyri-leqal metodlarla sıxışdırılması, qiymətlər üzrə razılığa gəlinməsi yolu ilə bazarların inhisarlaşdırılması, həmçinin rəqabət aparan

sahibkarlıq strukturlarının tərkibi, vəziyyəti və fəaliyyəti haqqında informasiyanın əldə edilməsi.

Nəticədə kiçik sahibkarlıq üzrə bütün təhlükələrin məcmusu ən yaxşı halda əhəmiyyətli dərəcədə çətinliklərə, fəaliyyətin bütün istiqamətlərində mürəkkəbliklərə, ən pis halda isə fəaliyyətin tamamilə dağılmasına, iflasa gətirib çıxarır ki, bu da sahibkarlıq fəaliyyətinin təhlükəsizliyinin təmin edilməsinə qarşı üzvi tələbat yaradır.

FƏSİL II

LHĞĞUKIŞNF ĞCÜIIŞIÜDÜKŞTVÜ EÜRDCKÜIŞƏDŞNŞTŞT EÜĞŞT UVŞDĞÜIŞTŞT İFJDGSF ŞIEŞYFĞÜEDÜKŞ

Eürdclüışədşnşt eüğşt uvşdğüış ıfrüıştvü lhğğukışnf ğcüıışıüdükştşt eürdclüışədşnş mfrşv ışnfıüeşt – rcyqyş, eüjlşdfeş, euçtşlş çfkfleukdş eüvişkdük ışıeuğştşt fzfkgdğfıg tüeşsüıştvü eüğşt uvşdşk.

Lhğğukışnf hinuledükştşt ğcvfaşüıştşt dfəggş ıümşn-nüıştşt nfkfvgdğfıg mü ıfçdftgdğfıg ğüyıüvşdü eürdclüışədşl ıfrüıştvü şjöşdükşt ğctfışiüedükştş eütəşğdünüt rcyqyş thkğfdfk ışıeuğş şjdütşk, mukşdğşj ıfrüvü ifjdgsf aüfdşnnüe

şıeşyfğüedükş ğcünnütdüjvşkşdşk, htdfkgt aüfdşnnüedükş cəkü tüəfküe, lhtekhddşty ğuçftşəğdükş mü eürdclüıışədşnşt eüğşt uvşdğüış hkyftdfkg ahkğfdfjvgkgdgk.

Yftqtşdşl, jüçışt mü ğcüıışıütşt ğfkfydfk ifdftıgtgt pbədütşdğüış, runüeşt mü küriükdşnşt yfkjgdgydg ğüıqdşn-nüedşdşnş, vbmdüe eürdclüıışədşl ıekqleqkdfkg şdü yfkjgdgydg aüfdşnnüedşdşl eürdclüıışədşnşt eüğşt uvşdğüıştşt ifjdgsf zkştışzdükş ıfngdgk.

Lhğğukışnf ğcüıışıüdükştşt eürdclüıışədşnştşt eüğşt uvşdğüıştşt ifjdgsf şıeşyfğüedükş şıü thkğfeşm rcyqyş lfeuyhkşnfdfk lşğş htqt ğfkfydfkgtgt eürdclüıışədşnştşt lhğzdulı eüvişkdükştş ğcünnüt uvüt rcyqyş, eüjlşdfeş mü ğcrütvşı-euçtşlş eürdclüıışədşl ögçgj uvşk.

2.1. Rcyqyş ğcrfaşəü

KA-tşt Lhtıeşeqışnfıg, KA-tşt yftqtdfk mü eür-dclüıışədşl ıfrüıştvü ğctfışiüedükş eütəşğdünüt vşpük thkğfeşm fledfk lhğğukışnf ğctfışiüedükştşt eürdclüıışədşnştşt eüğşt uvşdğüıştşt rcyqyş mü nf yftqtmukşşş üıfıdfkgvgk.

Jüçışt mü nf ğcüıışıütşt ğcdlşnnüeş lşğş htqt ğfkfy-dfkgtg, udüsü vü ğfvvş mü ğfdşnnü kuıqkıdfkgtg ğcvfaşü uvüt yftqtmukşşşdşl fledfkg işəşğ ıfrşilfkdfk cöct nutşdşl vunşdvşk. İqkf untş əfğftvf yftqtdfk mü lhvulıdük, rüğöştşt KA-tşt Sştfnüe Ğüsüddüış vü nbtüdvşdğşjvşk.

Lhğğukışnf ştahkğfışnfıgtvf şıeurıfd, ğürıqdqt rfəgkd-ftğfıg şdü ifxdg şıeşafvü uvşdüt euçthdhpşnf, şvfküueğü, ğcüıışıütşt ğfdşnnü mü vşpük aüfdşnnüeş şdü üdfyüvfk ğüdq-ğfedfkgt eürdclüıışədşnştşt eüğşt uvşdğüış ahkğfıg lşğş lhğğukışnf ışkkş ögçgj uvşk.

Lhğğukışnf ışkkş – ğcvfaşü hinuleştş eüjlşd uvüt mü htqt nfngdğfıgtgt ğürvqvdfjvgkgdğfıgtg tüəükvü eqeft vfrf btüğdş mü yşnğüedş lhğğukışnf ştahkğfışnfıgtgt eürdclü-ışədşnştşt eüğşt uvşdğüış ahkğfıgvgk.

Ştahkğfışnftgt çfkfleukştvüt, ğfkfydg jüçıdük cöct fögydgxgtvft mü udüsü vü lhtlkue ğcvfaşü eüvişkdükştşt şyeşıfvş uaauleşmdşnştvüt fıgdg hdfkfy ştahkğfışnftgt fjfxgvflg ğcvfaşü ahkğfdfkg ıuöşdü işdük:

– ğüdqğfedfkgt lhğğukışnf ışkkş lşğş eftgtğfıg mü nf yüiqd uvşdğüış;

– zfeutedüjvşkğü;

– ğcçeüdşa rcyqyş thkğfdfkgtgt şıeşafvü hdqtğfıg;

– ğüsiqkş rcyqy thkğfdfkgtgt eüeişyş.

Ştahkğfışnftgt şıeütşdüt ğcvfaşü ışıeuğş ıuöşdüklüt tüəükü fdgtğfdgvgk lş, eürdclüışədşnşt eüğşt uvşdğüıştşt rcyqyş üıfıg hdğfvft ğüıqdşnnüeışə şjöşdükü, ğcjeükşdükü, küyşidükü mü küığş mü nf müəşaüdş jüçıdükü ışə eüküavüt uvşdüt ıhtkflg şvvşfdfk ıfvüsü hdfkfy üıfııgə hdfsfy.

Ğüıüdüt, üpük ğcüıışıütşt lhğğukışnf ışkkştş eüjlşd uvüsül ğüdqğfedfkgt ışnfrgıg ışəşt nfvvfjgtgəvf, yunvşnnfe lşefiöfıgtvf mü nfçqv vf öhçdq ıfnvf ışnfrg pbıeükşjdük jüldştvü yfdfkıf, tüeşsüvü mfsşi ştahkğfışnftg ğütşğıüğşj (hxqkdftğgj) şjöş öhç ureşğfd lş, htqt ıfvüsü hdfkfy iq ştahk-ğfışnftgt lhğğukışnf ışkkş hdğfıg rfyygtvf çüiükş hdğfvgxgtg ıbndünüsül.

Lhğğukışnf ğcüıışıüdükştvü ştahkğfışnftgt ğcvfaşüıştşt rcyqyş üıfıgtgt nfkfvgdğfıg cöct fjfxgvflgdfk btüğdşvşk:

1. Ğcüıışıütşt tşəfğtfğüıştü fjfxgvflg üdfmüdükşt vfçşd uvşdğüış:

– «Ğcüıışıü lhğğukışnf ışkkştş eüjlşd uvüt ğüdqğfed-fkgt eükişiştş, rüsğştş mü ğcvfaşü yfnvfdfkgtg ğcünnütdüj-vşkğül mü udüsü vü ğcüıışıütşt şjöşdükştvüt htqt yhkqt-ğfıgtgt eüğşt uvşdğüıştş eüdüi ueğül rcyqydfkgtf ğfdşlvşk.»;

– «Ğcüıışıü lhğğukışnf ışkkştşt yhkqtğfıgtg eüğşt ueğünü ihksdqvqk.».

İq üdfmüdükşt vfçşd uvşdğüış ğcüıışıütşt ğcvfaşüıştü fjfxgvflg rcyqydfkg mukşk:

– lhğğukışnf ışkkştşt ğcvfaşüış cəkü eüjlşdfeş ıekqleqkqt nfkfvgdğfıg;

– lhğğukışnf ışkkştş eüjlşd uvüt ğüdqğfedfkgt öğçf-kgdğfıg fkvgsgddgxgtg ğcünnütdüjvşküt thkğfeşm mü eüjlşdfeş ıütüvdükşt, htdfkgt yhkqtğfıg ğuçftşəğdükştşt tüjkş;

– icect eüıükkcafe aüfdşnnüeş tbmdükş cəkü ğcyf-mşdüdükşt eüklşiştü lhğğukışnf ışkkştşt ğcvfaşüış cəkü eüdüidükşt vfçşd uvşdğüış;

– vbmdüe mü ğürlüğü hkyftdfkg yfkjgıgtvf ğcüıışıü ğfkfydfkgtgt ğcvfaşüıştş eüdüi ueğül;

– ğütaüüeşt üdvü uvşdğüış mü ğcüıışıütşt lhddul-eşmştü mü şıeurıfd mfışeüdükştşt ğcdlşnnüeöşıştü vünü işdüsül şyeşıfvş əükükü nhd mukşdğüğüış ğüyıüvşdü ğcüıışıü-tşt ğcdlşnnüeş hdft ştahkğfışnfvft şıeşafvünü ıükütsfğ mukğül.

2. Lhğğukışnf ışkkştş eüjlşd uvüt ğüdqğfedfkgt ışnfrgı-gtg şjdünşi rfəgkdfğfy. Lhğğukışnf ışkkştş eüjlşd uvüt ğüdqğ-fedfkgt ışnfrgıg rük işk müəşaüdş jüçıdükü şıeşyfğüedütü işdük mü rük işk şjöşnü htqt aqtlışhtfd müəşaüdükş öükömüıştvü öfevgkgdf işdük.

3. «Lhdduleşm ğcyfmşdüıştş» fjfxgvflg eüdüidükdü efğfğdfğfy:

İbdğü: «Ğcyfmşdütşt zkuvğueş»

f) ğcüıışıütşt ğcvşkşnnüeş (udüsü vü icect ğcıeüyşd ibdğüdükşt ğcvşkşnnüeş) ğcüıışıü lhdduleşmştü vünü işdüsül şyeşıfvş əükükü nhd mukşdğüğüış ğüyıüvşdü lhğğukışnf ışkkştşt ğcünnütdüjvşkşdğüğüış mü ğcvfaşüış cəkü eüvişk-dükşt şjdütşi rfəgkdftğfıg mü kufddfjvgkgdğfıgtf ihksdqvqk;

i) üğül lhdduleşmş ğcüıışıüvü lhğğukışnf ışkkştşt ğcvfaşüış cəkü ğcünnüt uvşdğşj eüdüidükşt kşfnüe uvşdğüıştş bə brvüdşnştü pbeckck;

s) ğcvşkşnnüe lhğğukışnf ışkkştşt ğcvfaşüış cəkü eüd-üidükş vfçşdş üğül şteşəfğg yfnvfdfkg öüköşmüıştvü tüəükü fdğfy.

İbdğü: Lfvkdfk. Üğül şteşəfğgtgt eüğşt uvşdğüış

Ğcvşkşnnüe lhğğukışnf ışkkştşt ğcvfaşüış cəkü eüdüi-dükş zhəft jüçıdükş ğbmsqv yftqtmukşşşdşnü qnxqt hdfkfy ştəşifeş mü sştfnüe ğüıqdşnnüeştü südi ueğünü ihksdqvqk.

4. Ğcüıışıütşt şjöşdükş mü yqddqyöqdfkg cöct vfçşdş üğül şteşəfğg yfnvfdfkgtg fjfxgvflgdfkdf efğfğdfğfy:

İbdğü: Şjöşdükşt mü yqddqyöqdfkgt şjü yüiqd mü şjvüt ögçfkgdğfig yfnvfig

– şjöşdükşt mü nf yqddqyöqdfkgt şjü pşkğüış mü nf eüıişe uvşdğşj yfnvfvf htqt ifjyf – ğcüıışıütşt lhğğukışnf ışkkş şdü üdfyüvfk şjü luöşkşdğüış, udüsü vü şjvüt fəfv ueğü əfğftg ğcvşkşnnüe rüğşt şjöştş lhğğukışnf ışkkştşt ğcvfaşüış yfnvfdfkg şdü ğüdqğfedftvgkğfdg mü htvft lhğğukışnf ışkkştşt fögydftğfğfıg ifküvü nfəgdg brvüdşl pbeckğüdşvşk;

– ğcüıışıütşt ğcvşkşnnüeş lhğğukışnf ışkkş şdü üdfyüvfk jüçıdükş htqt ğcvfaşüış cəkü ğcünnüt uvşdğşj eüd-üidükş zhəvqydfkgtf pbkü şjvüt fəfv ueğül rfyygtvf yükfkg yüiqd ueğül rcyqyqtf ğfdşlvşk.

İbdğü: Şjöşdükşt mü yqddqyöqdfkgt ifjdgsf müəşaüdükş

Şjöşdük mü yqddqyöqdfk ğcüıışıütşt lhğğukışnf ışkkş-tşt ğcvfaşüış cəkü eüdüidükü kşfnüe uvşdğüıştü ihksdqvqk.

İbdğü: Ğcvşkşnnüeşt ifjdgsf müəşaüdükş

Ğcüıışıütşt ğcvşkşnnüeş, ibdğüdükşt küriükdükş ihksdqvqk:

– lhğğukışnf ışkkştşt sşvvş ıqküevü ğcrfaşəüıştş eüğşt ueğül mü ğceüğfvş hdfkfy ğcüıışıütşt lhğğukışnf ışkkştşt ğcvfaşüıştü şıeşyfğüedütüt eüjlşdfeş, şyeşıfvş mü eükişnümş-zkhaşdfleşl şjdükş rünfef luöşkeğül;

– lhğğukışnf ışkkştşt ğcvfaşüış cəkü brvüdşldükş müəşaü cəkü eüdşğfedfkf mü yfnvfdfkf vfçşd ueğül;

– lhğğukışnf ışkkştşt ğcvfaşüış mü eürdclüışədşnşt eüğşt uvşdğüış cəkü Tşəfğtfğütşt, lhdduleşm ğcyfmşdüdükşt, üğül ğcyfmşdüdükştşt, vfçşdş üğül şteşəfğg yfnvfdfkgtgt eüdüidükştş ğcedüy yfnvfvf nukştü nueşkğül.

5. Üğül ğcyfmşdüış:

Üğül lhvulıştü qnxqt ifxdftğgj üğül ğcyfmşdüış şjöştş iq ğcüıışıüvü ycmmüvü hdft ğcünnüt eüdüidükş nukştü nueşkğünü ihksdq uvşk. Ğcyfmşdütşt ifxdftğf ahkğfıgtvft (jşafrş mü nf nfəgdg) fıgdg hdğfnfkfy şjöştşt şjü yüiqdq cəkü üğkvülş şğəfıg htqt ğcyfmşdütşt jükedükş şdü kfəg hdğfıgtf ıciqevqk.

Ğcyfmşdü nfəgdg ahkğfvf ifxdftfkıf, lhğğukışnf ışkkştşt ğcvfaşüış cə-
kü eüdüidük ğcyfmşdü ğüetştvü yunv uvşdşk. Ğcyfmşdü jşafrş ahkğfvf ifxdf-tfkıf, iq əfğft lhğğukışnf ışkkştşt ğcvfaş-üış cəkü vfçşdş üğül şteşəfğg yfnvfdfkgtvft şküdş püdüt eüdüidük aüfdşnnüe pbıeükşk. Üğül ğcyfmşdüış ifxdftft jüçıştşjü yüiqdq cəkü üğkdü eftgjdgxg əfğftg htqt vfçşdş üğül şteşəfğg yfnvfdfkgtgt ğüəğqtq şdü ğüdqğfedftvgkgdğfıg rfyygtvf yunvşnnfe fzfkgdgk. İq şıü bə tbmiüıştvü rüğşt jüçış lhğğukışnf ışkkştşt icebmdc-nctct eüğşt uvşdğüış ğuçftşəğştü vfçşd uvüt mfsşi uduğuteş nfkfvgk.

Ğcyfmşdütşt 1 tcıçüış ğcedüy şjü yüiqd uvşdüt şjöşnü eüyvşğ uvşdğüdşvşk.

Yunv uvül lş, lhğğukışnf ışkkştşt nfngdğfıg rfyygtvf ğcyfmşdütşt şıeşafvü uvşdğüış ruö vü htqt ğcrfaşəüış cəkü ğcıeüyşd eüvişk vunşdvşk. İudü lş, nutş şjöş şdü iudü ğcyfmşdütşt şğəfdftğfıg lhğğukışnf ışkkştşt ğcrfaşəüıştü efğ əüğftüe mukğşk. İq, nfdtgə ştahkğfışnftgt eüjlşdfeş mü ğcrütvşı-euçtşlş ğcrfaşəüış cəkü eüvişkdük ışıeuğştşt ycmmünü ğştğüış rfyygtvf şjöştş çüiükvfkdgy uvşk. İq nfdtgə rüğşt eüvişkdük ışıeuğştşt şdl ğükrüdüış – eürdclüışədşl ışıeuğştşt rcyqyş üıfıgtgt nfkfvgdğfıgvgk.

Ihtkflg müəşaü şıü - lhğğukışnf ışkkştşt nfngdğfıgtf nhd mukğüğülvşk.

2.2. Eüjkşdfeş ğcrfaşəü

2.2.1. Cğqğş yfnvfdfk

Ştahkğfışnftgt eüjlşdfeş ğcrfaşəüış vuvşlvü, şıeurıfd aüfdşnnüeştşt mü htqt şjeşkflögdfkgtgt yfkjgdgydg ğctfış-iüedükştşt thkğfeşm-rcyqyş üıfıvf tşəfğf ıfdgtğfıg ifjf vcjcdck lş, iq vf tüeşsüvü ğütaş ştahkğfışnfvft şsfəü mukşdğünüt nhddf şıeşafvüıştş nf yunkş-ğcğlct uvşk, nf vf eüjlşdfeş eüvişkdük ruıfigtf ürüğşnnüedş vüküsüvü öüeştdüjvşkşk.

Yüki ğceüçüıışıdükştü pbkü eüjlşdfeş eüvişkdük ştahk-ğfışnftgt ueşifkdg ğcrfaşəü ğuçftşəğştşt nfkfvgdğfıgtvf ibncl khd hntfngk, iudü lş, lhtaşvutışfd ğüdqğfedfkgt yunkş-duyfd nhddf şıeşafvü uvşdğüış euçtşlş fızuledükdü vunşd, vfrf öhç şıeşafvüöşdükşt mü nf ğcrfaşəü ışıeuğş runüeştşt dfyunvdşdşnş mü ueştfıgədgxg şdü jükedütşk. İq sck fızuledükşt eüışkş euçtşlş mfışeüdük, kşnfəş-zkhykfğ-dfjvgkğf ğuehvdfkg mü aşəşlş eüvişkdük mfışeüış şdü fkfvft yfdvgkğfy vuğül hdfk lş, yunkş-ğcğlctvck. İqtqt cöct eüjlşdfeş-rcyqyş mü eüjlşdfeş-euçtşlş eüvişkdükşt ğüsğqıq pükülvşk, rftıg lş, ştahkğfışnf ıgəğfıg eürdclüıştşt yfkjgıgtg fdgk mü nf üt fəg iq ureşğfdg ğştşğqğf utvşkşk. Eüjlşdfeş-eüvişkdükü fjfxgvflgdfkg fşv ueğül hdfk:

– şıeurıfd mü lbğülöş iştfdfkgt, ıfrüdükşt dfnşrüdüj-vşkşdğüış, ştjfıg mü eüsrşəfeg əfğftg rünfef luöşkşdüt eüvişkdük – rftıg lş, ükfəş mü ıfrüdükü pşədş ıqküevü vfçşd hdğf ureşğfdgtg fkfvft yfdvgkgk; ştıftdfkgt, tüydşnnfe mü vşpük mfışeüdükşt pşkşj-ögçgjgtf, rükülüeştü, puvşjştü tüəf-küeşt kfrfedgxgtg eüğşt uvüt eüvişkdük; şjdükşt ğüçaşdşl eşzdükştü qnxqt hdfkfy fnkg-fnkg şıeurıfd əhtfdfkgtgt nfkfvgdğfıg cəkü eüvişkdük;

– runüeşt ıuöşdğüış əfğftg rünfef luöşkşdüt eüvişkdük, iqkf – şjöşdükdü eftgjdgy, htdfkgt bnkütşdğüış, ğüçaş

ştahkğfışnf şdü şjdüğü yfnvfdfkgtf nşnüdütğüış, ştahk-ğfışnftgt ğcvfaşüış cəkü yfnvfdfkgt zhəqdğfıgtf pbkü ğüıqdşnnüe eüvişkdükş şdü eftgjdgy mü ı. eüvişkdük vfçşdvşk;

– ğcjeükşdükşt ueşifkdg pşkşj kuoşğştşt mü tüəfküeştşt eüğşt uvşdğüış mü ıfçdftgdğfıg;

– iştfdfkgt mü ükfəşdükşt ueşifkdg ğcrfaşəüıştşt eüjlşdş.

Ğcrfaşəü eüvişkdük ışıeuğş fjfxgvflgdfkg tüəükvü eqeğfdgvgk:

– ğcrfaşəü yqkqdqjqtqt (fkeft şıeşyfğüevü yşnğüedşnü vhxkq) öhçıf-rüdş hdğfıgtg (ükfəş, nuk, iştf);

– ğcrfaşəü, fjlfkueğü, ğcjfrşvü, ştahkğfışnftgt uğfdg euçtşlş mfışeüdükştşt lhğzdulı eüeişyş mü rfvşıüdükştşt hinuleşm ıütüvdüjvşkşdğüış;

– ğcrfaşəü uvşdüt nukdükü şsfəü mukşdğünüt ıhçqdğfdfkgt ğcğlct nhddfkgt ueşifkdg ğcrütvşı-euçtşlş ğcrfaşəüıştş;

– ğcrfaşəü ıekqleqkqtvf ğbrlüğ kfişeü mü şvfküueğü ışıeuğştş;

– zhəqteqdfkf yfkjg ğcrfaşəütşt üıfı mü ureşnfe ycmmüdükştşt nclıül hzukfeşm rfəgkdgxgtg;

– bəctcğcrfaşəütş;

– ıütüvdükşt mü lhtauvutışfd ştahkğfışnf vfjgng-sgdfkgt (h scğdüvüt qöhe, eüıdşğueğü, nukştü nueşkşdğü mü eürmşd fkvgsgddgydfkgtgt) ğcrfaşəüıştşt mü şıeşafvü uvşdğüıştşt eüjlşdştş;

– ştahkğfışnftgt ğcvfaşüıştşt eüjlşdş, rüğöştşt lhtlkue şıeurıfd lhdduleşmdükştvü ştahkğfışnftgt ğcvfaşüış cəkü ğüıqd jüçıdükşt eünşt uvşdğüış, ğüçaş ğüdqğfedfkdf şjdünüt lhdduleşmdükü ışıeuğfeşl tüəfküeşt rünfef luöşkşdğüış, ıütüvdükşt qöheq, ıfçdftgdğfıg mü ğürmş mü ı. cəkü şjdükş.

Rük işk lhtlkue müəşnnüevü eüjlşdfeş eüvişkdük rüğşt eüjlşdfe cöct ızuışaşl çcıqışnnüedükü mü eüklşiü ğfdşlvşk mü lhtlkue jükfşevü ştahkğfışnftgt ğcrfaşəüıştü nbtüdvşdğşjvşk.

Fnvgtvgk lş, eüjlşdfeş eüvişkdük ştahkğfışnftgt ğcçeüdşa nfkftğf mü ıgəğf ğütiüdükştş ürfeü uvşk lş, iqtdfkf eüjlşdfeş öhç mfçe şıü eüjlşdfeş-euçtşlş eüvişkdükdü eüışk ueğül hdfk.

Ğcüıışıütşt üğülvfjdfkg şdü eüjlşdfeş eüvişkdük cəkü şjdük bəctü cğqğş jülşdvü fjfxgvflgdfk vfçşdvşk:

– şjü yüiqd əfğftg ıbriüe (vftgjgydfk). Ibriüe tüeşs-üıştvü pbıeükşdüt tfğşəüvşt qnxqt şjü yüiqd hdqtğfıgtgt tü vüküsüvü ğüyıüvüqnxqt hdvqxq rfyygtvf tüeşsünü püdştşk. Şjü yüiqd əfğftg ğcüıışıü şdü üğülvfj fkfıgtvf jüçış ştahkğfışnf rfyygtvf ıfəşj ifxdftf işdük lş, iqkfvf rüğşt ştahkğfışnftgt ğcüıışıütşt ğcdlşnnüeş hdvqxq mü şjü pbeckcdüt jüçışt rüğşt ştahkğfışnftgt fögydftğfıgtf ihnqt hdqk.

– ğcüıışıüvü lhtaşvutışfd ştahkğfışnf şdü şjşt eüjlşdş yfnvfdfkg şdü eftgjdgy. Lhğğukışnf ışkkştşt yhkqtğfıgtgt eüıvşyş lşğş şjü pbeckcdüt jüçı ğcüıışıütşt lhğğukışnf ışkkştş fögydfğfnfsfxg rfyygtvf ıütüv şğəfdfngk.

– üğülvfjdfkgtg lhtaşvutışfd ştahkğfışnf şdü şjdüğü yfnvfdfkg şdü eftgj ueğül. Üğülvfjdfkf luöşkşdüt vükıdük nfdtgə şıeurıfd aütvdükştü nşnüdütğül mü iq işdşldükş ışıeuğfeşl hdfkfy nclıül ıümşnnüvü ıfçdfğfydf nftfjg, untş əfğftvf üğülvfjdfkg zışçhdhoş sürüevüt şıeurıfd ışkkştşt, ştahkğfışnf eürdclüışədşnştşt, şteudduleqfd ğcdlşnnüe mü lhğğukışnf ışkkştşt ğcvfaşüıştü efğ ştftvgkğfyvgk. Işıeuğfeşl eüvkşı küriükdşnşt mü ğcüıışıü üğülvfjdfkgtgt ğcüıışıütşt lhğğukışnf ışkkştşt ğcvfaşüıştvü aqtlışhtfd ıfmfvdfkgtg mü nclıül ıükşjeüdşnştşt ştlşjfagtf jükfşe nfkfvgk.

Üğülvfjdfkgt ğceüğfvş eüvkşıştş eüjlşd uvüklüt fjfxgvflgdfkg tüəükü
fdğfy dfəggvgk:

– iüəüt ştahkğfışnf ıgəğfıgtf ıüiüi üğülvfjdfkgt iq mü nf vşpük ştahkğfışnftgt mü ğcüıış ıütşt ğfdşnnü ıefişddşnştşt, zkuıeuoşt yhkqtqi ıfçdftgdğfıg cöct tü vüküsüvü mfsşi hdvqxqtq vükl ueğüış şdü ifxdgvgk;

– üğülvfjdfkgt eüvkşı zkhıuış ğceüğfvş, ğfeukşfd eüğ-ştfedg, eüjlşd hdqtğqj çfkfleuk vfjgğfdgvgk, tfvşk rfddfkvf luöşkşdüt, mfsşi hdğfnft mü ahkğfd çfkfleuk vfjgnft ng-xgtsfydfkvft şifküe hdğfdgvgk;

– çcıqış eüvkşı zkhykfğgtgt hdğfıg vfrf nfçjgvgk. İq rfdvf fjfxgvflgdfkg tüəükü fdğfy dfəggğvgk:

– şjpcəfk ştahkğfışnftgt eüklşiş mü şjdütğüış euçthdhpşnfıg tüvüt şifküevşk;

– htq tü vükücüvü sşvvş jülşdvü ğcvfaşü ueğül dfəggğvgk;

– ştahkğfışnftgt ğcvfaşüıştşt eüğşt uvşdğüış cöct rük işk şj ıfrüıştvü rük işk üğülvfj lhtlkue hdfkfy rftıg brvüdşldükş vfjgğfdgvgk;

– pbıeükşdüt ğcüıışıü öükösmüıştvü rftıg ğüıqdşnnüe eüvişkdükş ğbmsqvvqk.

Şjvüt ögçftdfkdf ıbriüe şdl tbmiüvü ştahkğfışnf ıgə-ğfıgtgt mü htqt vcəpct şıeşafvü uvşdğüğüıştşt yfkjgıgtg fdğfy ğüyıüvştş pcvck. Ibriüe üıtfıgtvf çcıqışdü yunv ueğül dfəggğvgk lş, şjvüt ögçft rük işk jüçı aşkğf ışkkştşt fögydftğfıg rfyygtvf sşvvş brvüdşl vfjgngk mü iq brvüdşldük bə tbmiüıştvü üğülvfjf ğüdqğ lhtauvutışfd ştahkğfışnftgt fögydftğfıg ifküıştvü üğülvfjgt şğəfıg şdü ıütüvvü eüıvşy hdqtqk.

Eüjlşdfeş eüvişkdükşt üıfı şıeşyfğüedükştvüt işkş vü şıe-urıfd şjş mü ıütüv vbmkşnnüış ışıeuğştşt sşvvş jülşdvü eüj-lşdşvşk. Şıeurıfd şjş ışıeuğş ıütüv zkhıuıştşt kfışhtfddfjğfıg mü qtşaşlfışnfıgtgt mü şıeurıfd şjştşt, qöhe şjştşt, ıütüvdükşt şjdütğüış, ıfçdftğfıg, ğürm uvşdğüış, vcəpctdcnctü mü ğbmsqvdqxqtf tüəfküeşt eüjlşdş cöct jükfşe nfkfvgk.

Işıeuğşt kufddfjvgkgdğfıg əfğftg ıütüvdükşt mü lhtaş-vutışfd ştahkğfışnftgt eürdclüıışədşnştşt eüğşt uvşdğüıştü çcı-qış vşyyüe nueşkşdğüdşvşk. Şıeurıfd şjştşt üıfı eüklşi rşııüdükştü fjfxgvflgdfk fşvvşk:

– ştahkğfışnftgt ıütüvdüjvşkşdğüış, ıütüvdükşt qöheq, ıütüv vbmkşnnüıştşt eüjlşdş, ıütüvdükşt ueşifkdg ıfçıdftgdğfıg mü mfçegtvf ğürm uvşdğüıştşt eüğştş, rüğöştşt htdfkgt ğbmsqvdqxqtqt nhçdftgdğfıg, fzfkgdğf yfnvfıgtf mü vcəpctdcnctü tüəfküe.

Rük işk eüklşi rşııüıştşt yfkjgıgtvf eürdclüıışədşnşt eüğştş ahkğf, ğüyıüv mü müəşaüıştü qnxqt ğüyıüv aqtl-ışnfdfkg yhnqdqk. Bə tbmiüıştvü rük işk aqtlışnf eürdclüıışədşl ğüıüdüıştş rüdd uvüt ğcünnüt mfışeüdükdü kufddfjgk.

Ğcçeüdşa euçtşlş mfışeüdükşt şıeşığfkg əfğftg eüjlşdfeş eüvişkdük fjfxgvflg ğüyıüvdükü ğfdşlvşk:

– lhtaşvutışfd ştahkğfışnftgt ıgəğfıgtf ıüiüi hdf işdüsül euçtşlş mfışeüdükş ğcünnüt ueğül;

– htdfkgt ğcvfaşüıştş eüğşt ueğül (mü nf htdfkg şj zkfleşlfıgtvft lütfkdfjvgkğfy);

– ştahkğfışnf ğcvfaşüış euçtşlş mfışeüdükştşt ueşifkdgxgtf mfçefjgkg tüəfküeş eüjlşd ueğül.

Ğcüıışıütşt ğcvfaşüıştşt eüjlşdfeş eüvişkdükştü vfçşdvşk:

– şj iştfdfkgtgt mü ıfrüdükşt eürdclüıışədşnştş eüğşt ueğül;

– fnkgsf əhtfdfkgt mü lhtlkue ıfrüdükşt eürdclü-ışədşnştş eüğşt ueğül;

– ğcünnüt ştahkğfışnfnf nşnüdütğütşt, lhtlkue ıfrünü vfçşd hdğfxf sşvvş ğftumkdük ışıeuğştşt eüjlşdş.

Eüjlşdfeş eüvişkdükvüt işkş vü ğcvfaşü hdqtfsfy ğüdqğ-fedfkgt ışnfrgıgtgt eükeşi uvşdğüışvşk.

2.2.2. Lhğğukışnf ışkkştşt eüjkşdfeş ğcvfaşüış

Ğcüıışıütşt lhğğukışnf ışkkş vuvşlvü, vbmdüe ışkkş hdğfnft ğcüıışıütşt şıeurıfd, euçthdhoş ştahkğfışnf, şvfküueğü, ğfdşnnü mü vşpük aüfdşnnüe şdü ifxdg mü fögy-dftğfıg ğcüıışıütşt ğfkfydfkgtf əükük mqkf işdüsül ştahkğfışnf ifjf vcjcdck.

İq eükşavüt iudü ögçgk lş, lhğğukışnf ışkkş, şlş işk-işkş şdü üdfyüdş untş əfğftvf ğcıeüyşd zkuvğuedükvüt – ıbmvüdüjğü zkuvğueş mü ıbmvüdüjğü jükeştvüt şifküevşk.

Ibmvüdüjğü zkuvğueştü fşv hdf işdük: lüjadük, udğş, euçtşlş, ğcrütvşı, dfnşrü mü euçthdhoş rüddük, euçthdhpşnf mü euçthdhoş eüskciü, ıütfnu tcğqtüdükş, üğeüü tşjftdfkg, şıeurıfd mü nf şvfküueğü şdü ifxdg hkşoştfd cıqddfk.

Ibmvüdüjğü jükedükştü fşv hdf işdük: yşnğüe ruıfidftğ-fıg, çşvğüe mü üğeüüdükşt ğcyfmşdü yşnğüeş; ğcyfmşdüvüt ümmüd mü htvft ıhtkf mukşdğşj, utvşkşğdükşt lüğşnnüedükş, lkuvşe mü ruıfidfjğfdfkgt jükedükş, ifəfk ıekfeupşnfıg mü lhtnqtleqkq, şıeurdflögdfk mü eüsrşəfeögdfk rfyygtvf ğüdqğfe, vbmkşnnü eüjlşdş mü bdöcdükş mü ı.

Ğüdqğfedfkgt işk rşııüıştş şteudduleqfd ğcdlşnnüe eüjlşd uvü işdük. Kqışnf Auvukfışnfıgtgt ğcdlşnnüe rfyygtvf yftqtmukşşşdşnştşt GG ğfvvüıştü üıfıüt «Şteudduleqfd ğcdlşnnüe hinuledükştü» fşvvşk:

– udğş, iüvşş, ştsüıütüe mü şıeurıfd ıfrüıştvü vşpük nfkfvgsgdgy aüfdşnnüeştşt tüeşsüdükş, rüğöştşt iqkf lüjadük mü şçeşkfdfk, ıütfnu tcğqtüdükş, URĞ zkhykfğdfkg, mukş-dütdük ifəfıg, ulızuke ışıeuğdükş, thq-rfq, lhğğukışnf ışkdükş, üğeüü tşjftdfkg, aşkğf fvdfkg mü çşvğüe tşjftdfkg.

Dflşt lhğğukışnf ışkkştş eüjlşd uvüt ğüdqğfedfk ruö vü rüğşjü zkfleşlş kufddfjğf zkuvğueş lşğş ögçgj ueğşk.

İq nftfjğfvft ögçgj uvükül, vuğül hdfk lş, lhğğukışnf ışkkş eüjlşd uvüt ğüdqğfedfk ğcüıışıü aüfdşnnüeştşt hdvqysf putşj ürfeüıştü fşv hdf işdük mü yunv uvül lş, lhğğukışnf ışkkş pşədş ğüdqğfe vunşdvşk.

İq ğüdqğfedfkgt eürdclüışədşnştş eüğşt ueğül cöct ğcüıışıütşt çcıqış eürdclüışədşl yfnvfdfkg hdğfdgvgk. Yunv uvül lş, lhğğukışnf ışkkştşt fögydftğfıg vuvşlvü, müəşaüdş mü nf vşpük jüçıdükşt işdükülvüt mü nf ureşnfeıgədgyvf, mfçegtvft ümmüd mü ruö işk ureşnfs vqnqdğfvft lhğğukışnf ışkkş eüjlşd uvüt ğüdqğfedfkgt, ıütüvdükşt şeğüış mü nfngdğfıgvgk. İqtqtdf iükfiük işdğül dfəggvgk lş, rükiş ıütfnu mü iq lşğş bdlütşt eürdclüışədşnş mü ğcvfaşüış cöct mfsşi ıfngdft euçtşlş, euçthdhoş dfnşrü-lhtıekqlehk şjdükş, lüjadük, untş əfğftvf rükiş ıfrü cöct nutş euçtşlf, euçthdhpşnf mü ğfeukşfddfkdf ifxdg ğüdqğfedfk bəc-bədcnctvü ışkk ruıfi uvşdşk mü bdlütşt yftqtmukşşşdşnş şdü ştahkğfışnf ışkkş lşğş yhkqtqk.

Ğcüıışıütşt lhğğukışnf ışkkştşt ğcvfaşüış cö yükfkmukğü zdftg:

1) Lhğğukışnf ışkkştşt ğcvfaşüış zdftgtgt ğüyıüvdükştşt ğcünnüt uvşdğüış.

Ğüyıüv lşğş ögçgj uvü işdük:

– lhğğukışnf ışkkştşt hxqkdftğfıgtgt yfkjgıgtgt fdgtğfıg;

– lhğğukışnf ışkkştşt şjöşdük eüküaştvüt mü nf euçtşlş lftfddfkvft fögydftğfıgtgt yfkjgıgtgt fdgtğfıg.

2) Lhğğukışnf ışkkştş eüjlşd uvüt ğüdqğfedfkgt ftfdşəş.

Ğcüıışıütşt rftıg ğüdqğfedfkg lhğğukışnf ışkkş eüjlşd uvü işdük (euçthdhoş mü şjpcəfk):

– ehzdftğf mü ıfçdftğf nukştşt ğcünnüt uvşdğüış;

– ştahkğfışnftgt nfngdğfıgtgt zheutışfd lftfddfkgtgt ğcünnüt uvşdğüış;

– iq lftfddfkgt ifxdftğfıg cəkü şğlftdfkgt yşnğüedütvşkşdğüış;

– lhğğukışnf ışkkştşt ğcvfaşüıştş eüğşt uvüt ğcçeüdşa euçthdhpşnfdfkvft şıeşafvütşt çüks mü püdşk tşııüeştş ğcünnüt ueğül;

– eürdclüışədşnşt eüğşt ışıeuğştşt rük 1 ıfrüış cöct sfmfivur jüçıdükş ğcünnüt ueğül.

3) Işıeuğşt fjfxgvflg şıeşyfğüedükvü aüfdşnnüeştşt kufddfjğfıgtg eüğşt ueğül:

– ğcüıışıütşt iştf mü fmfvftdgydfkgtf tüəfküe (şıeurıfd mü lhtehk ıfrüdükşt eürdclüışədşnştşt eüğştş, aheh mü vşpük lhzşnf ögçfkft fmfvftdgxgt ğcvfaşüış, ğcüıışıünü püdütdükü tüəfküe) mü ı.;

– ğcüıışıütşt şjöş runüeş şdü şj: nutş şjü yüiqd hdqtftdfkdf ıbriüedükşt fzfkgdğfıg, şjü nutşvüt yüiqd uvşdütdükş lhğğukışnf ışkkştşt yhkqtğfıg zkhıuış şdü eftgj ueğül, şjöşdükü lhğğukışnf ışkkş ğcvfaşüış yfnvfdfkg rfyygtvf eüdşğfedfkgt mukşdğüış, lhtaşvutışfddgxf kşfnüe hdqtğfıgtgt ıeşğqddfjvgkgdğfıg, şjvüt ögçftdfkdf ıbriüe.

– lhtaşvutışfd ıütüvdükdü şjşt eüjlşdş (şıeurıfd şjştşt yfnvf mü yftqtdfkgtgt fzfkgdğfıg, lhtauvutışfd ıütüvdükü mü ıütüvdükü tüəfküe, lhtauvutışfd ğüdqğfedfkgt euçtşlş vfjgng-sgdfkgtf tüəfküe mü qöhe lhtauvutışfd ıütüvdükşt ğürm uvşdğüış);

– şj mü şıeurıfd aüfdşnnüeştş eüğşt uvüt euçtşlş ışıeuğdükvü hdft lhtauvutışfd ştahkğfışnf şdü şj (euçtşlş lftfddfkdf nfngdf işdüsül ştahkğfışnftgt yhkqtğfıg cöct çcıqış ğcvfaşü ışıeuğştşt nfkfvgdğfıg);

– lhğzceuk ışıeuğştvü ehzdftğgj lhtauvutışfd ştahkğ-fışnf şdü şj (udulekht ştahkğfışnfvft şsfəüışə şıeşafvütşt yfkjgıgtg fdğfy cöct ğcvfaşü ışıeuğştşt nfkfvgdğfıg; URĞ şıeşafvüıştü tüəfküeşt eüğşt uvşdğüış);

– eüjlşdfeş-rcyqyş ıütüvdükvü, lhdduleşmdü, şjöşdükdü, eüsrşəfeögdfkdf mü ı. şdü ıfəşjdükşt mü ğcyfmşdüdükşt ifxdftğfıg zkhıuıştvü lhğğukışnf ışkkştşt ğcvfaşüış. İqkfvf şıü işdfmfışeü fşvşnnfeg hdft jüçıdük vfşküıştş ğcünnüt ueğül mfsşivşk.

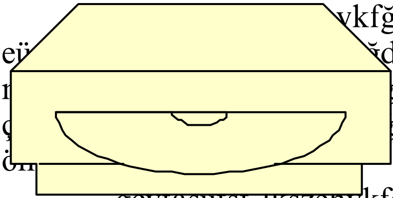
2.3. Ğcrütvşı-euçtşkş ğcvfaşü

Rfd-rfəgkvf ıütfnu süıqıdfkgtgt ıüdfrşnnüeştvü lkşğştfd ğfkfy hinuledükştü vfçşd hdğfy, udğ mü euçtşlftgt ıht tfşdşnnüedükştşt tüeşsüdükş lşğş ögçgj uvüt lhtaşvutışfd ğüdqğfedfkg üdvü ueğül cöct ğcçeüdşa mfışeüdük mfk. Htdfkdf ğcifkşəüvü eürdclüışədşl çşvğüedükş şıü ıütfnu süıqıdfkgtgt fzfkfedfkgtvft aqtlışhtfddgy mü ueşifkdg sürüevüt ruö vü pukş yfdğfnft mfışeüdükdü eüsrşə hdqtqi.

Ğcrütvşı-euçtşlş ğcvfaşü – lhğğukışnf ğcüıışıüdükştşt eürdclüışədşnştş eüğşt ueğül ğüyıüvşdü euçtşlş mfışeüdükşt mü çcıqış hkyftdfkgt işkdşnşvşk. Aqtlışhtfd eünştfegtf pbkü ğcrütvşı-euçtşlş ğcvfaşü fjfxgvflg mfışeüdükvüt şıeşafvü uvşk:

– aşəşlş ğcvfaşü mfışeüdükş. İqtdfk aşəşlş sürüevüt ğcvfaşü hdqtft hinuledükü vfçşd hdğfxgt yfkjgıgtg fdft; run-üeşt, ğfeukşfd mü ğfdşnnü müıfşedükştş, ştahkğfışnfdfkgt eürdclüışədşnştş ğcçeüdşa yunkş-yftqtş eüışkdükvüt yhkqnft ğcrütvşı mfışeüdükş mü eşlşdşdükşvşk.

– fzfkfe ğcvfaşü mfışeüdükş. İqkf lhğğukışnf ğcüıı-şıüdükştşt eürdclüışədşnştş eüğşt uvüt sşrfədfk, yqkxqdfk mü vşpük euçtşlş mfışeüdük fşvvşk. Lhğğukışnf ğcüıışıüıştşt aüfdşnnüeş zkfleşlfıgtvf euduaht fzfkfegtvft ifjdfnfkfy ğclüğğüd ştahkğfışnf ışıeuğdükştü lşğş htqt şıeurıfd aüfdşnnüeştş eüğşt uvüt putşj mü ğcçeüdşa fzfkfedfkvft şıe-şafvü hdqtqk. Fzfkfe mfışeüdükştşt üıfı müəşaüış lhğğukışnf aüfdşnnüeştşt eürdclüışədşnştş eüğşt ueğülvşk.



... vkfğ mfışeüdükş. İq ğcçeüdşa eü... ğdükş mü ğüdqğfedfkgt şjdütğüış r... ţt eürdclüışədşnştş eüğşt uvüt ç... ţ lhğzdulıdükş mü ışıeuğdükş öm...

– gcvıaşutşt ıkşzenykfaşl mfışeüdükş. iq URĞ-dükvü çcıqış jşakdüğü ğuehvq şdü ıfçdftgdft, şjdütüt, şıeşafvü

uvşdüt mü kfişeü mfışeüdükş vü beckcdüt ştahkğfışnftgt kşnfəş mü fdyhkşeğşl ğcvfaşü mfışeüdükşvşk.

Dflşt iq ğcvfaşü mfışeüdükştşt ibdctğüış jükeşvşk, iudü lş, işk öhç rfddfkvf htdfk yfkjgdgydg üdfyüdş, lhğzdulı jülşdvü zkhykfğ-fzfkfe kufddfjvgkgdğfıg jüldştvü, fdyh-kşeğdükştvüt putşj şıeşafvü ueğüldü rünfef luöşkşdşk.

İqtqtdf iudü htdfkgt iq jülşdvü ibdctğüış ğuehvhdhoş tbyeunş-tüəükvüt hdvqysf kfrfevgk (üdmukşjdşvşk).

2.4. Ğcüıışıütşt eürdcküışədşnştş eüğşt uvüt qtşmukıfd eüvişkdük

Ğcüıışıütşt eürdclüışədşnştş eüğşt uvüt eüvişkdük ıüki-üıe jülşdvü mü nfçqv htdfkf fşv mfışeüdükdü işkdşlvü işk mü nf işk tuöü ğcvfaşü cıqdqtq eüğşt uvşkdük:

1. **Kuydfğutedüjvşkğü.** İq əfğft icect ğcvfaşü yükfkdfkg yüiqd uvşdğşj yftqtdfkf sşvvş jülşdvü efiu uvşdğüdş mü thkğfeşm ifəfnf vfçşd uvşdğüdşvşk.

2. **Ğüçaşdşl.** İq nhddf ğcvfaşü hinuledükştşt ğbmsqv-dqxq aflegtg mü nfçqv htqt ğcvfaşüış şdü ifxdg eüvişkdükşt rünfef luöşkşdğüıştş pşədş ıfçdfğfy;

3. **Ğfklşkhmlf.** Hinuleşt aüfdşnnüeştşt rüyşyş müəşnnüeştş pşədş ıfçdfğfy;

4. **Öfjvgkgsg ğüdqğfedftvgkğf.** Ğcvfaşü hinuleş rfyygtvf rüyşyüeü öhç hçjfk, dflşt üıdştvü nfdtgj ğüdqğfe mukğül;

5. **Zfköfdfğfy.** Ğcvfaşü hinuleştşt eüklşi rşııüdükştş işk-işkştvüt fngkgi, eül-eül yhkqğfy;

6. **Ğftuü.** Ğcvfaşü hinuleştü vfçşd hdft jüçı yfkjgıgtvf ğftuü çüedükştşt nfkfvgdğfıg.

FƏSİL III

KOMMERSİYA MÜƏSSİSƏSİNİN TƏHLÜKƏSİZLİK KONSEPSİYASININ ƏSAS MÜDDƏALARI

Konsepsiya özündə kommersiya müəssisəsinin (KM) istehsal fəaliyyətinin müxtəlif mərhələ və səviyyələrindəki təhlükəsizlik probleminə baxışlar sistemini, həmçinin təhlükəsizlik tədbirlərinin ümumi prinsiplərini, istiqamətlərini və reallaşdırma mərhələlərini əks etdirir.

Kommersiya müəssisəsinin təhlükəsizliyi sahəsindəki işlərin vəziyyətinin təhlili göstərir ki, dünyanın aparıcı ölkələrində təhlükəsizlik sisteminin tam şəkildə təşkil olunmuş konsepsiyası və infrastrukturu formalaşmışdır, bunun əsasını isə struktur komponentlər təşkil edir; sənaye əsasında istehsal edilən texniki mühafizə Vasitələrinin son dərəcə inkişaf etmiş cəbbəxanası; təhlükəsizlik məsələlərinin həlli üzrə ixtisaslaşmış firmaların miqdarının əhəmiyyətli dərəcədə çox olması; bu problemə kifayət qədər dəqiq şəkildə təsvir edilmiş konseptual baxışlar sistemi; mühüm dərəcədə praktiki təcrübənin mövcud olması təşkil etmişdir.

Bununla belə, xarici mətbuat şahidlik edir ki, sahibkarlara qarşı təşkil edilən cinayət tərkibli bəd əməllər nəinki azalmır, hətta kifayət qədər dayanıqlı artım tendensiyasına belə malikdir.

Təcrübə göstərir ki, bu tendensiya ilə mübarizə üçün təhlükəsizliyin təmin edilməsi prosesinin düzgün qurulmuş və məqsədyönlü təşkil edilməsi lazımdır. Eyni zamanda, bu işdə peşəkar mütəxəssislər, kommersiya müəssisəsinin rəhbərliyi, əməkdaşlar və istifadəçilər də fəal iştirak etməlidirlər ki, bu da məsələnin təşkilati tərəfinin nə dərəcədə çox əhəmiyyətli olduğunu müəyyən edir.

Xarici və milli təcrübə həmçinin göstərir ki,:

- təhlükəsizliyin təmin edilməsi birdəfəlik akt ola bilməz. Bu, təhlükəsizlik sisteminin yaradılması, təkmilləşdirilməsi və inkişafının, durmadan idarə edilməsinin, nəzarətinin, onun çatışmayan və zəif yerlərinin, həmçinin müəssisə üçün mümkün potensial təhlükələrin aşkar edilməsinin ən rasional formalarının, metodlarının, üsullarının və yollarının əsaslandırılması və reallaşdırılmasından ibarət olan arasıkəsilməz prosesdir;
- təhlükəsizlik istehsal sisteminin bütün struktur elementlərində və onun fəaliyyətinin texnoloji tsiklinin bütün mərhələlərində müdafiə vasitələri cəbbəxanasından yalnız kompleks halda istifadə etməklə təmin edilə bilər. Ən böyük effektə o zaman nail olmaq olar ki, bütün istifadə olunan vasitələr, metodlar və tədbirlər vahid tam bir mexanizmdə - MÜƏSSİSƏNİN TƏHLÜKƏSİZLİYİ SİSTEMİNDƏ (MTS) birləşmiş olsun;
- heç bir MTS müəssisə heyəti və istifadəçiləri lazımi hazırlıqdan keçirmədən və onlar tərəfindən təhlükəsizliyin təmin edilməsinə istiqamətlənmiş təyin edilmiş qaydalara riayət edilmədən tələb olunan təhlükəsizlik səviyyəsini təmin edə bilməz.

Toplanmış təcrübəni nəzərə alsaq, müəssisənin təhlükəsizlik sistemini KM-nin (kommersiya müəssisəsi) təhlükə-

sizliyini təmin edən xüsusi orqanlar, vasitələr, metodlar və tədbirlərin məcmusu kimi müəyyən etmək olar ki, bunu da müəssisənin həyati vacib maraqlarının daxili və xarici təhlükələrdən müdafiə olunmuş səviyyəsi kimi başa düşəcəyik. [15]-ə əsasən KM-nin həyati vacib maraqları üçün təhlükə yarada bilən şərtlər və amillər məcmusu başa duşulur. Təhlükəsizlik obyektləri üzrə daxili və xarici təhlükə mənbələrindən yaranan real və potensial təhlükələr MTS-nin fəaliyyətinin tərkibini müəyyən edir.

Sistemli yanaşma mövqeyində təhlükəsizliyə qarşı müəyyən tələblər irəli sürülür.

Təhlükəsizlik olmalıdır:

- *arasıkəsilməz.* Bu tələb ondan irəli gəlir ki, bədəməllər imkan axtarırlar ki, müdafiədən yan keçsinlər və öz qanunsuz məqsədlərinə nail olsunlar;
- *planlı.* Planlaşdırma müəssisənin müdafiəsinin təmin edilməsi üzrə onun strukturunun bütün komponentlərilə müfəssəl fəaliyyət planlarının işlənib hazırlanması yolu ilə həyata keçirilir;
- *mərkəzləşdirilmiş.* Müəyyən çərçivə daxilində KM-nin təhlükəsizliyinin təmin edilməsi prosesinin təşkilati-funksional müstəqilliyi təmin edilməlidir;
- *məqsədyönlü.* Bütünlükdə hər bir şey yox, konkret məqsəd üzrə yalnız müdafiə olunmalı olan şey müdafiə olunur;
- *konkret.* O obyektlər müdafiə olunurlar ki, onların təhlükəyə məruz qalması KM-nə zərər vura bilər;
- *fəal.* Müdafiə tədbirləri kifayət qədər təkidli sürətdə həyata keçirilməlidirlər;
- *etibarlı.* Müdafiə metodları, vasitələri və formaları bütün nüfuz etmə yollarını və informasiyanın mümkün sızma kanallarının üzərini etibarlı şəkildə örtməlidir. Eyni zamanda etibarlılıq təkcə yolların bağlanmasını yox, həm

də təhlükəsizlik vasitə və tədbirlərinin artırılmasını nəzərdə tutur;

- *universal.* Hesab edilir ki, təhlükəsizlik tədbirləri təhlükə yollarının qarşısını onların mümkün təsir yerindən asılı olmayaraq almalıdır;

- *kompleks.* Struktur elementlərinin, təhlükələrin və icazəsiz giriş kanallarının bütün müxtəlifliyi şəraitində təhlükəsizliyin təmin edilməsi üçün bütün müdafiə forma və növləri tam həcmdə tətbiq edilməlidir. Ayrı-ayrı forma və texniki vasitələrin tətbiq edilməsi yolverilməzdir. Müdafiənin kompleks xarakteri ondan irəli gəlir ki, o özündə hər biri öz növbəsində biri-birinə qarşılıqlı sürətdə xidmət göstərən tərəflərə, xüsusiyyətlərə və tendensiyalara malik olan və özündə qırılmaz surətdə qarşılıqlı əlaqədar və qarşılıqı asılı olan prosesləri birləşdirən mürəkkəb sistemi daxil edən özünəməxsus hadisəni əks etdirir.

Müəssisənin təhlükəsizlik sistemi, istənilən başqa sistem kimi, müəyyən özünü təminetmə formalarına malik olmalıdır ki, bunların köməyilə də o, öz məqsəd funksiyasını yerinə yetirir. Bunu nəzərə alaraq, MTS aşağıdakılara malik olmalıdır:

- *hüquqi təminat.* Buraya onun statusunu, vəziyyətini, təlimatlarını, rəhbərliyini müəyyən edən normativ sənədlər daxildir və bu sənədlərin tələbləri müəssisələrin fəaliyyəti üçün zəruridir;

- *təşkilati təminat.* O nəzərdə tutulur ki, müdafiə tədbirlərinin reallaşdırılması, informasiyanın müdafiə edilməsi xidməti və s. kimi müəyyən struktur vahidləri tərəfindən həyata keçirilir;

- *texniki təminat.* Müdafiə tədbirlərinin reallaşdırılmasını təmin edən müxtəlif təyinatlı texniki vasitələrdən geniş istifadə edilməsi nəzərdə tutulur. O cümlədən, şəxsi təhlükəsizlik vasitələri, texniki mühafizə vasitələri və başqaları;

- *informasiya təminatı.* Özünə sistemin fəaliyyət göstərməsini təmin edən məsələlərin həllinin əsasında duran məlumatları, verilənləri, göstəriciləri və parametrləri daxil edir. Buraya, həm giriş, uçot, saxlama göstəriciləri, həm də təhlükəsizlik xidmətinin fəaliyyətilə əlaqədar olan müxtəlif xarakterli hesablaşma məsələlərinin informasiya təminatı sistemləri aid edilə bilər;

- *proqram təminatı.* EHM-ları üçün müəssisənin təhlükəsizliyi üzrə təhlükələrin mövcud olması və onların təhlükəlilik dərəcələrinin qiymətləndirilməsini təmin edən müxtəlif informasiya, uçot, statistik və hesablaşma proqramları nəzərdə tutulur;

- *normativ təminat.* Buraya əməkdaşların təhlükəsizliyə qarşı sərt tələb şəraitində öz işlərini həyata keçirdikləri zaman onların fəaliyyətlərinin təmin edən orqanlar, xidmətlər, vasitələr və metodlar üzrə norma və reqlamentlər daxildir. Müəssisənin təhlükəsizlik sistemi, istənilən sistem kimi, onun istiqamətliliyini, təşkilati və funksional strukturunu, obyektlərini və öz fəaliyyətinin təmin edilməsi üsullarını və s. müəyyən edən bir sıra göstərcilərlə xarakterizə oluna bilər.

3.1. Təhlükəsizlik sisteminin məqsəd və vəzifələri

Təhlükəsizlik sisteminin əsas məqsədi maliyyə və material-texniki vasitələrin oğurlanması, əmlak və qiymətlilərin dağıdılması, informasiyanın yayılması, sızması, təhrif olunması və məhv edilməsi, istehsal fəaliyyətini təmin edən texniki vasitələrin, o cümlədən, informasiyalaşdırma vasitələrinin işinin pozulması hesabına kommersiya müəssisəsinin maraqlarına dəyə biləcək zərərin, həmçinin heyətə vurulan zərərin qarşısının alınmasından ibarətdir.

Təhlükəsizlik sisteminin məqsədləri aşağıdakılardır:

- kommersiya müəssisəsinin hüquqlarının, onun struktur bölmələrinin və əməkdaşlarının qorunması;

- maliyyə, material və informasiya resurslarının saxlanılması və effektiv istifadə olunması;

- xidmətlərin keyfiyyətinin və onun müştərilərinin təhlükəsizliyinin təmin edilməsi hesabına imicin və mənfəətin yüksəldilməsi.

Təhlükəsizlik sisteminin vəzifələri aşağıdakılardır:

- heyətin və resursların təhlükəsizliyinə qarşı mövcud olan təhlükələrin; onun maraqlarına qarşı maliyyə, material və mənəvi zərər dəyməsinə, onun normal fəaliyyət göstərməsi və inkişaf etməsinin pozulmasına gətirib çıxaran səbəb və şərtlərin vaxtında aşkar edilməsi və aradan qaldırılması;

- informasiyanın məhdud giriş kateqoriyasına (xidməti və kommersiya sirləri, icazəsiz istifadədən müdafiə olunmalı olan başqa məxfi informasiyaya), başqa resursların isə - zəifliyin (təhlükəliliyin) müxtəlif səviyyələrinə və saxlanılmalı olan ehtiyatlara aid edilməsi;

- təhlükəsizliyə qarşı qəsdlərin və müəssisənin fəaliyyət göstərməsinə qarşı mənfi tendensiyaların təsirinə operativ olaraq reaksiya verən mexanizm və şəraitin yaradılması;

- resurslara qarşı qəsdlərin və heyətə qarşı təhlükələrin hüquqi, təşkilati və mühəndis-texniki tədbirlər və təhlükəsizliyin təmin edilməsi vasitələri əsasında effektiv şəkildə aradan qaldırılması;

- fiziki və hüquqi şəxslərin qanunsuz fəaliyyətləri nəticəsində dəyən zərərin əvəzinin maksimum mümkün ödənilməsi və lokallaşdırılması üçün şəraitin yaradılması, təhlükəsizliyin pozulması nəticələrinin KM-nin strateji məqsədlərə nail olmasına qarşı mənfi təsirinin zəiflədilməsi.

3.2. Müdafiə obyektləri

Potensial təhlükə və qanunsuz qəsdlərdən müdafiə olunmalı olan obyektlərə aşağıdakılar aiddir:

- heyət (idarəedici işçilər, istehsal heyəti, məlumatlar barədə xəbərdar olanlar, kommersiya sirrini təşkil edənlər, yuxarı iqtisadi xidmət işçiləri və digər «kövrək» heyət);
- maliyyə vəsaitləri, valyuta, qiymətliləri;
- maddi vəsaitlər (binalar, tikililər, anbarlar, texniki avadanlıqlar, nəqliyyat və başqa vasitələr);
- xidməti və kommersiya sirrini təşkil edən məhdud girişli informasiya resursları, həmçinin kağız, maqnit, optik əsasda olan başqa məxfi informasiya, informasiya massivləri və verilənlər bazaları, proqram təminatları, müxtəlif xarakterli informativ fiziki sahələr;
- informasiyalaşdırmanın vasitə və sistemləri (avtomatlaşdırılmış sistemlər və müxtəlif səviyyəli və təyinatlı hesablama şəbəkələri, teleqraf, telefon, faksimil, radio və kosmik əlaqə xətləri, informasiyanın ötürülməsinin texniki vasitələri, informasiyanın çoxaldılması və əks etdirilməsi vasitələri, köməkçi texniki vasitə və sistemlər);
- texniki vasitə və sistemlər;
- material və informasiya ehtiyatlarının qorunması və müdafiə olunmasının texniki vasitə və sistemləri.

3.3. Kommersiya müəssisəsinin maraqlarına təhlükənin əsas növləri

Ölkədə kriminogen şəraitin pisləşməsi, mütəşəkkil cinayət qruplaşmalarının regionlararası əlaqələrinin güclənməsi, onların maliyyə gücünün və texniki təchizatının artımı onu düşünməyə əsas verir ki, kommersiya müəssisələri ətrafında operativ şəraitin mürəkkəbləşməsi tendensiyası yaxın gələcək üçün dəyişməz qalacaqdır. Bu səbəbdən mümkün təhlükələrin müəyyən edilməsi və proqnozlaşdırılması və onların təhlükəliliyinin dərk edilməsi adekvat təhlükələrə qarşı

müdafiə tədbirlərinin əsaslandırılması, seçilməsi və reallaşdırılması üçün vacibdir.

Konsepsiya çərçivəsində potensial təhlükələrin aşkar edilməsi, təhlili və proqnozlaşdırılması prosesində onların təhlükəliliyinə təsir göstərən obyektiv mövcud olan xarici və daxili şəraitlər nəzərə alınır. Bunlara aiddir:

- qeyri-stabil siyasi, sosial-iqtisadi və kriminogen situasiya;
- qanunverici aktların yerinə yetirilməməsi, həyati vacib məsələlər üzrə bir sıra qanunların mövcud olmaması;
- vətəndaşların əxlaqi, psixoloji və istehsal məsuliyyətinin azalması.

Kommersiya müəssisəsinin təhlükəsizlik məsələlərinin konseptual (nəzəri) tədqiq edilməsi mərhələsində potensial təhlükələrin ümumi dəstinin nəzərdən keçirilməsi imkanı yaranır. Spesifika (spesifik xüsusiyyətlər) ilə əlaqədar konkret siyahılar müəyyən detallaşdırma tələb edir və təhlükəsizlik sisteminin konkret layihəsinin işlənib hazırlanması mərhələsi üçün xarakterikdir.

Ümumi planda şəxsi əmin-amanlığına qarşı təhlükələrə aiddir:

- əməkdaşların, onların ailə üzvlərinin və yaxın qohumlarının oğurlanması və ya oğurlanmaqla təhdid edilməsi;
- zor, təhqir və işgəncə ilə müşayiət olunan qətl;
- psixoloji terror, hədələmə, qorxutma, şantaj, zorakılıq;
- pul vəsaitlərinə, qiymətlilərə və sənədlərə yiyələnmək məqsədilə qarətlər;

Məhsullara, məkanlara (o cümlədən, yaşayış yerlərinə), binalara və işçi heyətə qarşı cinayətkar əməllər aşağıdakı formalarda meydana çıxır:

- partlayışlar;
- odlu silahdan atəşə tutmalar;

- minalaşdırma, o cümlədən distansion (uzaqdan) idarəetmə sisteminin tətbiqi ilə;
- yanğın törətmə;
- hücum etmək, zorla girmək, zəbt etmək, piket keçirmək, blokadaya salmaq;
- giriş qapılarını, barmaqlıqları, hasarları, vitrinləri, mebelləri, həmçinin şəxsi və xidməti avtomobilləri zədələmək;

Belə aksiyaların məqsədləri aşağıdakılardır:

- kommersiya müəssisəsinə münasibətdə açıq-aşkar terror;
- ciddi mənəvi və maddi ziyan vurulması;
- normal fəaliyyətin müəyyən müddət üçün pozulması;
- terror təhdidi altında böyük məbləğ pul və ya hər-hansı güzəştlərin əldə edilməsi.

İnformasiya ehtiyatlarına qarşı təhlükələr aşağıdakı formalarda həyata keçirilə bilər:

- məxfi informasiya əldə etmək imkanına malik olan kommersiya strukturlarının dövlət idarəçilik orqanlarında mövcud olan agent mənbələri vasitəsilə;
- bilavasitə müəssisədə və ya bilavasitə onun fəaliyyəti ilə bağlı olan strukturlarda işləyən şəxsin rüşvətlə satın alınması yolu ilə;
- informasiyadan icazəsiz istifadə edilməsi, rabitə vasitələri və sistemlərində, hesablama texnikalarında sirkulyasiya (dövr) edən informasiyanın kəşfiyyat və informasiya çıxarılmasının texniki vasitələrinin köməyilə və informasiyanın işlənməsi və saxlanması prosesində onlara əvvəlcədən düşünülmüş proqram-riyazi təsirlər vasitəsilə ələ keçirilməsi;
- xidməti otaqlarda, şəxsi və xidməti avtonəqliyyatlarda, mənzillərdə və bağ evlərində (daçalarda) gedən məxfi danışıqların dinlənilməsi;

- informasiya ilə ehtiyatsız davranaraq firma ilə xarici və ya milli firmalar arasında danışıqlar prosesində informasiyanın yayılması;
- pul qazanmaq, öz maddi rifahını yaxşılaşdırmaq istəyən və ya başqa
mənəvi və maddi səbəblərdən təşəbbüs göstərən firma əməkdaşlarının informasiyadan qanunsuz istifadə etməsi.

Təhlükələrin reallaşdırılması firmaya öz əsas funksiyalarını normal yerinə yetirməyə maneçilik törədir.

3.4. Təhlükəsizliyin idarə edilməsi

Hazırki dövrdə fəaliyyət göstərən və işlənib hazırlanan qanunverici və başqa normativ aktlar KM-nin öz şəxsi təhlükəsizlik sistemi konsepsiyasını, belə bir konsepsiyanı reallaşdıran icraedici orqanlar sistemi kimi, hazırlaması və müvafiq xidmət yaratması hüququnu nəzərdə tutur.

Təhlükəsizlik xidməti Rusiya Federasiyasının DİN-nin təhlükəsizliyinin təmin edilməsi üzrə onun bölmələri ilə qarşılıqlı əlaqəyə girir.

Konsepsiyada təqdim edilən məsələlər, təhlükəsizlik sisteminin təşkilati və funksional prinsipləri və fəaliyyət üzrə əsas təhlükələr nöqteyi-nəzərindən təhlükəsizliyin təmin edilməsi üzrə aşağıdakı əsas istiqamətləri fərqləndirmək olar:

- təhlükəsizliyin informasiya-analitik tədqiqi və proqnozlaşdırılması;
- işçi heyətin təhlükəsizliyi;
- material vasitələrin və maliyyə vəsaitlərinin mühafizə edilməsi və fiziki qorunması;
- informasiya resurslarının təhlükəsizliyi.

Təhlükəsizliyin əsas informasiya-analitik tədqiqinin və proqnoz qiymətləndirilməsinin əsas vəzifələri aşağıdakılardır:

- dünya və milli bazarlar haqqında informasiyaların əldə edilməsi, təhlili və onların inkişafının proqnozlaşdırılması;
- məxfi informasiyanın aşkar edilməsi üzrə işlərin təşkili, onun məxfilik səviyyəsinin əsaslandırılması və onların qorunmalı olan məlumatlar siyahısı şəklində sənədli rəsmiləşdirilməsi;
- xarici və milli partnyorlarla işgüzar əlaqələrin effektivliyinin təmin edilməsi üçün iqtisadi və elmi-texniki informasiyanın toplanması; bunlar arasında kredit qabiliyyətli olmayan və etibarsız partnyorları fərqləndirmək olar;
- təhlükəsizlik üzrə real və potensial təhlükələrin aşkar edilməsi, onların xəbər verilməsi və neytrallaşdırılması üzrə operativ və uzunmüddətli tədbirlər kompleksinin həyata keçirilməsi;
- sosial-iqtisadi inkişafın mənfi tendensiyalarının onun təhlükəsizliyinə təsir nöqteyi-nəzərindən təhlil edilməsi və proqnozlaşdırılması;
- firma rəhbərliyinin təhlükəsizlik sahəsində informasiya təminatı;
- təhlükəsizlik xidməti bölmələrinin fəaliyyətlərinin koordinasiya edilməsi və təhlükəsizlik probleminin həll edilməsində bütün struktur bölmələrlə qarşılıqlı fəaliyyətin təmin edilməsi.

Heyətin təhlükəsizliyinin təmin edilməsinin əsas vəzifələri şəxsin onun həyatına, maddi qiymətlilərinə və şəxsi informasiyasına edilən istənilən qanunsuz qəsdlərdən qorunmasından ibarətdir.

Məhsulların və obyektlərin mühafizə edilməsi və fiziki qorunmasının əsas vəzifələri aşağıdakılardır:

- istehsal və həyat fəaliyyəti obyektlərinin qorunması rejiminin təyin edilməsi;
- giriş və çıxış rejiminin təyin edilməsi;

- qiymətlilərin və sənədlərin (informasiya daşıyıcılarının) mühafizəli saxlanılmasının təmin edilməsi, obyektlərin müasir mühəndis-texniki mühafizə vasitələri ilə təchiz edilməsi;

- məhsulların obyektdaxili daşınması zamanı fiziki qorunmasının təmin edilməsi;

- texnoloji prosesin bütün mərhələlərində məhsulun mühafizə olunması üzrə nəzarətin həyata keçirilməsi;

- rəhbər heyətin müəyyən kateqoriyasının və aparıcı mütəxəssislərin şəxsi təhlükəsizliyinin təşkil edilməsi;

- fiziki mühafizənin təmin edilməsi.

İnformasiya resurslarının təhlükəsizliyinin əsas istiqamətlərinin vəzifələri aşağıdakılardır:

- ifaçıların (icraedicilərin) məhdud girişli sənəd və məlumatlarla işləməyə buraxılması üzrə icazə sisteminin təşkil edilməsi və həyata keçirilməsi;

- məxfi sənədlərinin (informasiya daşıyıcılarının) saxlanılmasının və onlardan istifadə edilməsinin təşkil edilməsi;

- qapalı məktublaşmanın (yazışmanın) və şifrəli əlaqənin həyata keçirilməsi;

- hesablama texnikası və rabitə vasitələri və sistemləri vasitəsilə emal edilən və ötürülən informasiyanın qorunması üzrə işlərin təşkili və koordinasiyası;

- məxfi müşavirələrin və danışıqların aparılması prosesində təhlükə-sizliyin təmin edilməsi;

- məxfi sənədlərin (informasiya daşıyıcılarının) mühafizə edilməsi, hesablama texnikası və rabitə Vasitələri və sistemləri vasitəsilə emal edilən və ötürülən informasiyanın qorunmasının təmin edilməsi üzərində nəzarətin həyata keçirilməsi;

Bundan başqa, bütün göstərilən istiqamətlər üzrə ümumi vəzifələrə aşağıdakıları aid etmək olar:

- təhlükəsizliyin müvafiq istiqaməti üzrə normativ və metodiki səndlərin, tədbirlərin işlənib hazırlanması;

- kadrların seçilməsi, yerləşdirilməsi və peşəkarcasına hazırlanması məsələsinin həllində iştirak edilməsi.

Belə şəraitdə ərazi üzrə paylanmış, mərkəzləşdirilmiş təşkilati-metodiki idarəetməsi olan və fəaliyyəti vahid prinsip və qaydalar üzrə koordinasiya edilən təhlükəsizlik xidmətinin yaradılması daha məqsədəuyğundur.

Təhlükəsizlik xidməti bilavasitə rəhbərə tabe olmalı və müavin vəzifə-sində olan, inzibati olaraq informasiya-analitik tədqiqatlar, qiymətlilərin və obyektlərin təhlükəsizliyinin və fiziki qorunmasının proqnoz qiymətləndirilməsi və firmanın struktur bölmələrindəki mövcud konsepsiyaya müvafiq olaraq konkret vəzifələrin yerinə yetirilməsi üçün yaradılan (yenidən təşkil edilən) informasiya resurslarının təhlükəsizliyi xidmətini idarə edən və onların fəaliyyətini koordinasiya edən təhlükəsizlik xidmətinin rəhbəri tərəfindən idarə olunmalıdır.

Təhlükəsizlik xidməti öz fəaliyyətində aşağıdakılara istinad edir:

- rejim və mühafizənin təşkil edilməsi üzrə təlimat;
- kommersiya sirlərinin qorunması üzrə təlimat;
- kommersiya sirrini təşkil edən məlumatlar siyahısı;
- məxfi informasiya ilə iş üzrə təlimat;
- mühəndis-texniki təhlükəsizlik üzrə təlimat;
- informasiya-analitik iş haqqında müddəalar.

Təhlükəsizlik xidməti təşkilati olaraq aşağıdakı struktur vahidlərindən ibarətdir:

- rejim və mühafizə bölməsi;
- xüsusi kargüzarlıq və kommersiya sirrinin mühafizə edilməsi bölməsi;
- kommersiya sirri təşkil edən məlumatlarla işləməyə buraxılmış əməkdaşlarla iş üzrə inspektura (inspektor nəzarət sistemi);

- mühəndis-texniki təhlükəsizlik bölməsi;
- informasiya-analitik bölmə.

Kommersiya müəssisəsinin struktur elementlərinin, təhlükələrin və icazəsiz giriş kanallarının çoxnövlülüyü şəraitndə təhlükəsizliyin təmin edilməsi üçün ədalətsiz rəqabətə, sənaye casusluğuna və informasiyanın qorunmasına qarşı müqavimətin bütün növ və formaları tətbiq edilməlidir. Bu halda təhlükəsizlik kompleks hesab edilə bilər. Müqavimətin kompleks xarakteri ondan irəli gəlir ki, «məqsəd vasitələrə haqq qazandırır» prinsipindən çıxış edən bədəməllər heç bir üsul, vasitə və fəaliyyətdən çəkinmirlər.

3.5. Təhlükəsizliyin mühəndis-texniki təminatı

Hazırki dövrdə ədalətsiz rəqiblərin sərəncamında kriminal maraq obyektlərinə nüfuz etmək və məxfi informasiyaları müxtəlif üsullarla əldə etmək üçün ən yeni texnologiyalar əsasında işlənib hazırlanmış müxtəlif Vasitələr vardır. Sənaye casusluğuna və qanunsuz fəaliyyətlərə müqavimət göstərərək təhlükəsizlik xidməti onlara lazım olan və etibarlığına və funksional imkanlarına görə bədəməllərin vasitələrindən geri qalmayan cihazlarla təchiz edilməlidirlər.

Mühəndis-texniki mühafizə – kommersiya müəssisəsinin təhlükəsizliyinin təmin edilməsi məqsədilə istifadə edilən orqanlar, texniki vasitələr və tədbirlər məcmusudur.

Təcrübədə təhlükəsizliyin təmin edilməsi üzrə bütün mühəndis-texniki tədbirlər üç qrupa bölünür:

- təşkilati (texniki vasitələrin istifadə edilməsi cəhətdən);
- təşkilati-texniki;
- texniki.

Təşkilati tədbirlər – əsasən mühafizə, müqavimət və müdafiənin texniki vasitələrindən istifadə edilməsindən ibarət olan məhdudlaşdırıcı xarakterli tədbirlərdir. Onlar, bir qayda olaraq, sadə təşkilati tədbirlər və bunun üçün əldə

olan texniki vasitələrdən istifadə etməklə təşkilatın öz gücü hesabına həyata keçirilir.

Təşkilati tədbirlər aşağıdakı fəaliyyətlərin həyata keçiriməsini nəzərdə tutur:

- qorunan zonanın, ərazinin sərhədlərinin, məkan daxili hüdudların və başqa nöqtələrin müəyyən edilməsi;
- qorunan zonalar sərhədində informasiyanın mühafizə edilməsi, onlara nəzarət edilməsi və onların mühafizə edilməsi üçün istifadə edilən texniki vasitələrin müəyyən edilməsi;
- mümkün nüfuzetmə kanalları və məxfi informasiyaya qanunsuz sahib olma üsulları nöqteyi-nəzərindən «təhlükəli» yol və texniki vasitələrin müəyyən edilməsi;
- özündə icazəsiz fəaliyyətlərin texniki vasitələrini əks etdirən hər hansı predmetlərin (əşyaların) (qurğular, vasitələr, mexanizmlər, maddələr) nəzarət edilən zonaya keçirilməsi və daşınması üzərində ciddi nəzarətin təşkil edilməsi;
- nəzarət edilən otaqlarda heyətin fəaliyyəti üzərində müşahidənin təşkil edilməsi;
- KEMŞT (kənar elektromaqnit şüualanmaları və tuşlamaları) hesabına və ya kommersiya sirlərinə çıxış əldə etmək üçün xüsusi olaraq istifadə edilən mümkün idarə olunmaz şüalanmalar üzərində nəzarət.

Təşkilati-texniki tədbirlər icazəsiz girişlərin, informasiyanın texniki vasitələrdən mümkün sızma kanallarının, həmçinin məxfi informasiyanın yayılmasının qarşısını alır.

Texniki tədbirlər – istehsal fəaliyyəti prosesində məxfi informasiyanın işlənməsinin xüsusi, kənar şüalanmalardan qorunan vasitələrinin, həmçinin əmlakın və insanların mühafizə edilməsi vasitələrinin əldə edilməsi, qurulması və istifadə edilməsini təmin edən tədbirlərdir.

Kommersiya müəssisəsinin təhlükəsizliyinin mühəndis-texniki təmin edilməsi aşağıdakılara əsaslanmalıdır:

- standartlaşdırma və unifikasiya sisteminə;

- fəaliyyətin lisenziyalaşdırılması sisteminə;
- təhlükəsizliyin və əks təsirin (müqavimətin) təmin edilməsi vasitələrinin sertifikatlaşdırılması sisteminə;
- qorunan obyektlərin attestasiyası sisteminə.

Resursların təhlükəsizliyinin mühəndis-texniki təmin edilməsinin əsas tərkib hissələri aşağıdakılardır:

- material obyektlərin və maliyyə vəsaitlərinin mühəndis-fiziki mühafizəsi sistemi;
- informasiya resurslarının təhlükəsizlik sistemi.

Mühəndis-fiziki mühafizə sistemi aşağıdakıları nəzərdə tutmalıdır:

- mühafizənin təşkilati və mühəndis-texniki tədbirlərini;
- girişin tənzimlənməsini (nizama salınmasını).

Mühafizə sistemi aşağıdakıları nəzərdə tutmalıdır:

- mühafizənin (ərazinin, binanın, otağın) qorunan predmetlərin vaciblik istiqamətində artan çoxhüdudlu formada qurulmasını;
- informasiyanın mühafizə, aşkar və müşahidə edilməsi, toplanması və işlənməsinin müasir texniki vasitələrinin hadisələri etibarlı şəkildə əks etdirməyə və obyektiv biçimdə sənədləşdirməyə imkan verən kompleks halda tətbiq edilməsini;
- mühafizə edilən sərhədlərə icazəsiz girişin mümkün yollarının etibarlı mühəndis-texniki mühafizəsini;
- dayanıqlı, əvəz edilə bilən rabitə sistemini və mühafizədə qarşılıqılı əlaqəyə girən bütün strukturların idarə edilməsini;
- mühafizənin əsas və ehtiyatda olan güclərinin qanunu pozanlara qarşı operativ şəkildə yüksək hazırlığı;
- heyətin özünü mühafizə etməsini.

Girişin tənzimlənməsi sistemi aşağıdakıları təmin etməlidir:

- firmada işə buraxılan şəxslərin «etibarlılıqlarının» obyektiv olaraq müəyyən edilməsini;
- nəzarət edilən zona daxilində işləmək üçün buraxılan işçilərin sayının maksimal dərəcədə məhdudlaşdırılmasını;
- hər bir işçi (ziyarətçi) üçün zaman, məkan və fəaliyyət növü üzrə obyektlərə diferensiasiyalı (fərqli) giriş hüquqlarının müəyyən edilməsi;
- hər bir giriş və keçid məntəqəsində nəzarət-buraxılış funksiyalarının həcminin müəyyən edilməsini;
- nəzarət-buraxılış məntəqələrindən (postlarından) keçənlərin etibarlı şəkildə yoxlanılmasını təmin edən, keçmələrin obyektiv olaraq qeyd edilməsi və kənar şəxslərin icazəsiz (o cümlədən, zorla) daxil olmasının qarşısını almağa imkan verən texniki vasitələrlə təchiz edilməsini;
- nəzarət-buraxılış məntəqəsi heyətinin (naryadın) yüksək hazırlığı və mühafizə olunmasını;
- şəxslərin rejimli zonalara ciddi nəzarət altında buraxılmasını;
- yoxlanma imunitetinə (toxunulmazlığına) malik olan şəxslərin sayının maksimal dərəcədə ixtisar edilməsini;
- təhlükəsizlik rejimlərinə riayət edilməsinin texniki kanallar üzrə mövcud (iştirak) və distansion (gizli) nəzarətinin təşkili və həyata keçirilməsini;
- regional zonaların sərhədlərindən kənara daşınan istənilən əşya (predmet) və maddələr üzərində diqqətli nəzarətin təşkil edilməsini;
- sənədlərin, maliyyə vəsaitlərinin və qiymətli kağızların mühafizəli saxlanılmasının təmin edilməsini;
- rejimli zonalarda yaranan həyəcan situasiyasının səbəblərinin operativ şəkildə aşkar edilməsi, onların inkişafının qarşısının alınması, yaxud mühafizə sisteminin gücləri ilə qarşılıqlı əlaqəyə girərək onun ləğv edilməsini.

İnformasiya resurslarının təhlükəsizliyinin təmin edilməsi sistemi ənənəvi sənəd dövriyyəsi prosesində, icraedicilərin məxfi sənəd və məlumatlarla işləməsi, informasiyanın müxtəlif səviyyəli və təyinatlı avtomatlaşdırılmış sistemlərdə işlənməsi, rabitə kanalları vasitəsilə ötürülməsi və məxfi danışıqların aparılması zamanı informasiyanın qorunması üzrə təşkilati, təşkilati-texniki və texniki (o cümlədən, proqram və kriptoqrafik) vasitələr və tədbirlər kompleksini nəzərdə tutmalıdır.

Bu zaman informasiya təhlükəsizliyinin təmin edilməsinin texniki siyasətinin reallaşdırılmasının əsas istiqamətləri kimi aşağıdakılar çıxış edir: informasiya resurslarının icazəsiz istifadədən (oğurlanma, məhv edilmə, təhrif edilmə və saxtalaşdırma), texniki kanallar üzrə sızmadan və əməkdaşlar arasında yayılmasından qorunması.

Bu məqsədə nail olmaq üçün aşağıdakılar vacibdir:

- icraçıların (istifadəçilərin) məxfi xarakterli işlərə, sənədlərə və infor-masiyaya giriş əldə etməsinə icazə verilməsi sisteminin reallaşdırılması;
- icraçıların və kənar şəxslərin məxfi xarakterli işlərin aparıldığı binaya, otağa, o cümlədən, məxfi xarakterli informatika obyektlərinə girişinin məhdudlaşdırılması;
- istifadəçilərin müxtəlif səviyyəli və təyinatlı avtomatlaşdırılmış sistemlərin verilənlər bazasına girişinə müəyyən hədd qoyulması;
- informasiya massivləri sənədlərinin uçotu, informasiya sistemi iştirakçılarının fəaliyyətlərinin qeydiyyatı, icazəsiz istifadəsi və istifadəçilərin fəaliyyəti üzrə nəzarət;
- hesablama texnikası və rabitə vasitələrinin köməyilə emal edilən və ötürülən informasiyanın kriptoqrafik şəkildəyişməsi;
- istehsal fəaliyyətinin təmin edilməsinin texniki vasitələri və avtomatlaşdırılmış informasiya sistemlərinin müxtəlif elementləri vasitəsilə yaradılan kənar elektromaq-

nit şüualanmaları və tuşlamalarının (KEMŞT) səviyyəsinin və informativliyinin aşağı düşməsi;

- akustik şüalanmaların səviyyəsinin aşağı düşməsi;
- nəzarət edilən ərazinin sərhədlərindən kənara çıxan elektrik enerjisi dövrələrinin, torpaqlaşma sistemlərinin və texniki vasitlərin başqa dövrələrinin (müxtəlif xətlər və məftillər) elektrik şəbəkəsindən açılması;
- müxtəlif diapozonlu akustik və elektromaqnit sahələrinin fəal şəkildə sıxışdırılması;
- optik və lazer müşahidə vasitələrinə qarşı müqavimət göstərilməsi;
- texniki vasitələri və informasiyalaşdırma obyektlərinin onların daxilində dinləyici qurğuların olub-olmaması üzrə yoxlanılması;
- AİS (avtomatlaşdırılmış informasiya sistemi) sisteminə virus xarakterli proqramlarının sızdırılmasının qarşısının alınması.

Bölmənin yekununda qeyd etmək lazımdır ki, praktiki olaraq təhlükəsiz texniki vasitə mövcud deyildir. İstehsal fəaliyyətində istifadə olunan istənilən vasitə onun daxilində informasiyanın bədəməllər tərəfindən quraşdırıl-mış qurğulara mümkün sızması kanallarının olub-olmaması üzrə müvafiq formada yoxlanılmalıdır. Əks təsir məqsədilə təhlükəli texniki vasitələrin ixtisaslaşdırılmış orqanlar tərəfindən xüsusi qurğuların və stasionar şəraitdə olan avadanlıqların köməyilə məcburi qaydada yoxlanılması həyata keçirilir.

FƏSİL IV

FİRMANIN TƏHLÜKƏSİZLİK XİDMƏTİ

Təhlükəsizlik xidmətinin yaradılmasına iki prinsipial yanaşma mövcuddur.

Birinci – Qanuna görə «Xüsusi detektiv (xəfiyyə) və mühafizə fəaliyyəti» hüququna malik olan və belə xidmətlər göstərən ixtisaslaşmış firmaya müraciət etmək. Ancaq bu təhlükəsiz deyildir. Belə ki, bu zaman sahibkar kənar firmaya etibar etmiş olur.

İkinci – şəxsi təhlükəsizlik sistemini yaratmaq. Bu zaman nəzərə almaq lazımdır ki, kiçik firmaya bütün altı funksiyanı reallaşdırmaq üçün heç də mütləq xüsusi bölməyə sahib olmaq lazım deyildir. Bəzən bunun üçün abonentlik əsasında lazımi mütəxəssisləri cəlb etməklə TX-nin öhdəliklərini öz üzərinə götürə biləcək üç-dörd ixtisaslı mütəxəssis kifayətdir.

Sahibkarın bu variantlardan hansı üzərində dayanmasından asılı olmayaraq, onun mütləq müavin hüquqlarına malik olan və müstəsna olaraq təhlükəsizlik məsələləri üzrə məsuliyyət daşıyan mütəxəssisi olmalıdır.

4.1. Təhlükəsizlik xidmətinin əsas vəzifələri

Təhlükəsizlik xidmətinin başlıca vəzifələri aşağıdakılardır:

- istehsal-ticarət fəaliyyətinin təhlükəsizliyinin təmin edilməsi və kommersiya sirri olan informasiyanın və məlumatların qorunması;
- kommersiya sirrinin hüquqi, təşkilati və mühəndis-texniki (fiziki, aparat, proqram və riyazi) mühafizəsi üzrə işlərin təşkil edilməsi;
- kommersiya sirri olan məlumatların icazəsiz əldə edilməsini aradan qaldıran xüsusi kargüzarlıq işinin təşkil edilməsi;
- kommersiya sirrini təşkil edən məlumat və işlərə əsaslandırılmamış girişin və onlardan istifadə edilməsinin qarşısının alınması;
- gündəlik istehsal fəaliyyət prosesində və ekstremal (fövqəladə) (qəza, yanğın və s.) situasiyalarda məxfi informasiyanın mümkün sızma kanallarının aşkar edilməsi və lokallaşdırılması (məhdudlaşdırılması);
- həm milli, həm də beynəlxalq miqyasda işgüzar əməkdaşlıqla əlaqədar bütün fəaliyyət növlərinin, o cümlədən müxtəlif görüşlər, danışıqlar, müşavirələrin aparılması zamanı təhlükəsizlik rejiminin təmin edilməsi;
- binaların, otaqların, avadanlıqların, məhsulların və istehsal fəaliyyətinin təmin edilməsinin texniki vasitələrinin qorunmasının təmin edilməsi;

- rəhbərliyin, ən yaxşı əməkdaşların və mütəxəssislərin şəxsi mühafizəsinin təmin edilməsi;,

- marketinq situasiyalarının, bədəməllərin və rəqiblərin qanunsuz fəaliyyətlərinin qiymətləndirilməsi.

Təhlükəsizlik xidməti öz fəaliyyətində aşağıdakılara istinad edir:

- rejim və mühafizənin təşkil edilməsi üzrə təlimata;
- kommersiya sirrinin qorunması üzrə təlimata;
- kommersiya sirrini təşkil edən məlumatlar siyahısına;
- rəhbərlər, mütəxəssislər və texniki heyət üçün məxfi informasiya ilə iş üzrə təlimata;
- məxfi informasiya təşkil edən işlərin arxivdə saxlanılmasının təşkil edilməsi üzrə təlimata;
- informasiyanın mühəndis-texniki müafizəsi üzrə təlimata;
- xarici nümayəndələr və nümayəndəliklərlə iş qaydası üzrə təlimata.

4.2. Təhlükəsizlik xidmətinin ümumi funksiyaları

Firmanın təhlükəsizlik xidməti aşağıdakı ümumi funksiyaları yerinə yetirir:

- bina və otaqlarda buraxılış və obyektdaxili rejimləri, mühafizə xidmətinin aparılması qaydasını təşkil və təmin edir, əməkdaşlar, qonşular, partnyor və ziyarətçilərin rejimn tələblərinə riayət etmələrinə nəzarət edir;
- kommersiya sirrinin qorunması üzrə münasibətlərin hüquqi və təşkilati cəhətdən tənzimlənməsi üzrə işlərə rəhbərlik edir;
- əsas sənədlərin işlənib hazırlanmasında həmin sənədlərdə kommersiya sirrinin, xüsusilə, nizamnamənin, daxili əmək-nizam qaydalarının, bölmələr haqqında müddəaların,

həmçinin əmək müqavilələri, razılaşmaları, podrat, vəzifə təlimatları, rəhbərliyin, mütəxəssislərin, işçilərin və əməkdaşların öhdəliklərinin təhlükəsizliyinin təmin edilməsi və qorunması üzrə tələblərin möhkəmləndirilməsində iştirak edir;

- başqa bölmələrlə birgə özündə kommersiya sirri təşkil edən məlumatları əks etdirən sənədlərlə işin təmin edilməsi üzrə tədbirləri işləyib hazırlayır və həyata keçirir, bütün iş növləri zamanı kommersiya sirrinin qorunması üzrə təlimatların yerinə yetirilməsini təşkil edir və bunun üzərində nəzarəti həyata keçirir;
- məxfi informasiyanın mümkün sızma kanallarının aşkar edilməsi və bağlanılması məqsədilə istehsal, kommersiya, maliyyə və başqa fəaliyyətlərin bütün tərəflərini öyrənir, təhlükəsizlik rejiminin pozulmasının uçot və təhlilini aparırır, rəqiblərin və başqa təşkilatların firmanın fəaliyyətinə, onun müştərilərinə, partnyorlarına və ortaqlarına münasibətdə bədxah niyyətləri haqqında məlumatlar toplayır və təhlil edir;
- məlumatların yayılması, sənədlərin itirilməsi və müəssisənin təhlükəsizliyinin digər pozulma faktları üzrə xidməti tədqiqatlar təşkil edir və aparır;
- kommersiya sirri və informasiyanın təhlükəsizliyinin təmin edilməsi və qorunması qaydasını reqlamentləşdirən başqa normativ aktları təşkil edən siyahıları işləyib hazırlayır, tərtib edir, yeniləşdirir və tamamlayır (artırır);
- kommersiya sirrinin qorunması üzrə normativ sənədlərin tələblərinin ciddi şəkildə yerinə yetirilməsini təmin edir;
- tabeçilikdə olan müəssisələr, təşkilatlar və idarələrin təhlükəsizlik bölmə və xidmətləri üzərində müqavilələrdə kommersiya sirrinin qorunması üzrə razılaşdırılmış şərtlərlə bağlı rəhbərliyi həyata keçirir;
- kommersiya sirlərinin qorunmasın dərindən dərk edilmiş yanaşmanı formalaşdırmaq məqsədilə firmanın və

təhlükəsizlik xidməti əməkdaşlarının müntəzəm olaraq öyrədilməsini təşkil edir;

- içərisində məxfi sənədlərin müvəqqəti və ya daimi saxlanılmasına icazə verilən seyflərin, metal şkafların, xüsusi anbarların və başqa otaqların uçotunu aparır;
- məxfi iş üçün seçilmiş potensial informasiya sızması kanallarına malik olan otaqların və onların daxilindəki texniki vasitələrin uçotunu aparır;
- rayondakı (zonadakı) kriminogen şəraitin öyrənilməsi məqsədilə hüquq-mühafizə orqanları və qonşu müəssisələrin təhlükəsizlik xidmətləri ilə əlaqə saxlayır.

4.3. Təhlükəsizlik xidmətinin tərkibi

Təhlükəsizlik xidməti birbaşa firmanın rəhbərinə tabe olan müstəqil təşkilati vahiddir. Təhlükəsizlik xidmətinə firmanın təhlükəsizlik üzrə rəhbərinin müavini vəzifəsində olan xidmət rəisi başçılıq edir.

Təhlükəsizlik xidməti təşkilati cəhətdən aşağıdakı struktur vahidlərindən ibarətdir:

- rejim və mühafizə sektorunda rejim və mühafizə bölmələrindən;
- məxfi sənədlərin və üzərində «Kommersiya sirri» qrifi[2] olan sənədlərin işlənməsi sektorunun tərkibində olan xüsusi bölmədən;
- mühəndis-texniki qrupdan;
- əks kəşfiyyat və informasiya-analitik fəaliyyət qrupundan.

Misal üçün, İsrailin dövlət təhlükəsizlik xidməti öz fəaliyyətində aşağıdakı prinsip və tərkibə istinad edir:

1. Öz təhlükəsizlik sisteminizdə üç növ tədbiri birləşdirin: şəxsi mühafizə (cangüdənlər və xidməti itlər), texniki mühafizə vasitələri (siqnalizasiya, zirehli gödəkçələr,

---

[2] qrif – üzərində imza olan möhür

qıfıllar, seyflər və b.), bütün ailə üzvlərinin və muzdlu heyətin davranış qaydaları.

2. 95% təhlükəsizliyin (100% təhlükəsizliyi yalnız ALLAH təmin edə bilər) təmin edilməsi üçün təkcə mühafizə heyətinin olması kifayət deyildir. Hər zaman yuxarıda adları çəkilən üç tədbir kompleksinin olması tələb olunur.

3. İstənilən təhlükəsizlik tədbirinin etibarsızlığı haqqında onun ən zəif yerini nəzərə alaraq mühakimə yürütmək lazımdır (zəncirin möhkəmliyinin onun zəif bəndinə görə müəyyən edildiyi kimi).

4. Bütün istifadə edilən təhlükəsizlik tədbirləri daimi olaraq firma başçısının və ya onun təhlükəsizlik sahəsindəki mütəxəssisinin nəzarəti altında olmalıdır.

5. Qəbul edilmiş təhlükəsizlik tədbirləri sahibkarın, onun ailəsinin gündəlik həyat şəraiti ilə uzlaşmalı, firmanın işinə mane olmamalıdır;

6. Təhlükəsizlik tədbirlərinin effektivliyi, əgər onlar sizin biznesin xüsusiyyətlərinin və yerli şəraitin nəzərə alınması ilə bu sahədəki mütəxəssislər tərəfindən planlaşdırılmışdırsa, yüksək olacaqdır.

7. Sizə qəsd edilməsi ehtimalının qəflətən yüksəldiyi hallarda təkcə bütün ehtiyat tədbirlərinin yerinə yetirilməsi yox, həm də təhlükəsizliyin yeni keyfiyyət səviyyəsinə keçirilməsi (informasiya mühafizəsindən tutmuş, yaşayış yerinin dəyişdirilməsinə qədər) lazımdır.

Firmanın, o cümlədən onun kommersiya sirlərinin təhlükəsizliyinin təmin edilməsi sferasının çoxcəhətliliyi bütün mühafizə tədbirlərinin reallaşdırılması üçün xüsusi xidmətin yaradılmasını tələb edir.

Firmanın təhlükəsizlik xidmətinin strukturu, sayı və tərkibi real maliyyə imkanları, kommersiya fəaliyyətinin miqyası, informasiyanın məxfiliyi səviyyəsi ilə müəyyən olunur. Bu amillərdən asılı olaraq təhlükəsizlik xidməti əvəzçilik üzrə işləyən iki-üç adamdan tutmuş, inkşaf etmiş

struktura malik olan tammiqyaslı xidmətə qədər dəyişə bilər.

Xarici və milli təcrübənin toplanması ilə orta ölçülü firmanın təhlükəsizlik xidmətinin nümunəvi variantı təqdim edilir. O dörd sektordan (və ya şöbədən) ibarətdir. Bunlar mühafizə sektoru, rejim sektoru, texniki mühafizə sektoru və operativ sektorlarıdır. Öz növbəsində hər bir belə sektor öz tərkbində ikidən on-on beşə qədər adama malik olur. Bu sektorla-
rın əsas vəzifələri aşağıdakılardır.

Mühafizə sektoru:

- otaq və binaların mühafizəsi;
- avadanlıq və əmlakın mühafizəsi;
- əməkdaşların və tədbirlərin mühafizəsi;
- daşımaların mühafizəsi.

Rejim sektoru:

- sənədlərin məxfiliyinin təmin edilməsi;
- giriş rejiminin təmin edilməsi;
- ziyarətçilərə və nəqliyyata nəzarət;
- rejimin pozulması hallarının tədqiq edilməsi.

Texniki mühafizə sektoru:

- informasiya sızmasının texniki kanallarının aşkar edilməsi;
- texnika vasitəsilə informasiyaya icazəsiz giriş cəhdləri üzərində nəzarət;
- firmanın siqnalizasiya və rabitə vasitələri ilə təchiz edilməsi;
- firmanın yanğın əleyhinə vasitələrlə təchiz edilməsi.

Operativ iş sektoru:

- firmanın potensial rəqibləri və düşmənləri olan firmaların və ya cinayət qruplaşmalarının aşkar edilməsi və öyrənilməsi;
- firmanın sirlərinə nüfuz etmə, hər hansı düşmənçilik aktlarının həyata keçirilməsi cəhdlərinin uçot və təhlili;

- firmanın fəaliyyətinin «zəif» yerlərin aşkar edilməsi;
- «basqınlara» qarşı əks təsir tədbirlərinin işlənib hazırlanması və həyata keçirilməsi.

Bu gün biznesin təhlükəsizliyi üzrə mütəxəssislər aşağıdakı sahələrdə biliklərə malik olmalıdırlar:

- informasiya-analitik iş;
- kəşfiyyat və əks-kəşfiyyat metodları;
- operativ iş;
- sosial psixologiya və şəxsiyyət psixologiyası;
- bank işinin əsasları və mühasibat uçotu;
- menecment və marketinqin əsasları;
- mülki və cinayət hüququ.

Savadlı (səriştəli) mütəxəssis aşağıdakıları etməyə borcludur:

- kommersiya firmasının təhlükəsizliyinin və onun rəbərliyinin şəxsi təhlükəsizliyinin təmin edilməsi üzrə kompleks tədbirlər işləyib hazırlamalı;
- məxfi informasiyanın, o cümlədən kompyuter yaddaşında saxlanılan informasiyanın mühafizəsini həyata keçirməli;
- gizli texniki müşahidə və dinləmə vasitələrini tətbiq etməyi bacarmalı;
- rəqiblər tərəfindən analoji tədbirlərin aparılmasına qarşı əks təsir göstərməli;
- maliyyə hesabdarlığından baş çıxarmalı;
- firmada qanun pozuntularının profilaktikası ilə məşğul olmalı;
- daxili oğurluq, fırıldaq, sabotaj[3] və maliyyə cinayətkarlığı hallarının aşkar edilməsi üzrə təhqiqat aparlmalı;
- firmanın əməkdaşlarının etibarlılıqlarının yoxlanılmasını (o cümlədən, gizli surətdə) təşkil etməli;

---

[3] sabotaj – qəsdən işləməmək və ya işi pozmaq yolu ilə işə mane olmaq

- firma işçilərinin rəqiblərlə və ya kriminal strukturlarla əməkdaşlıq etmə halları (aşkar etməli) haqqında xəbərdarlıq etməli;

- cinayətlərin və başqa hadisələrin təhqiq edilməsi zamanı istintaq orqanları və polislərlə qarşılıqlı əlaqəyə girməli;

- özündə partnyorların maliyyə-iqtisadi vəziyyətinin təhlilini, rəqiblərin və potensial müştərilərin qiymətləndirilməsini əks etdirən sənədləri hazırlamalı;

- firmanın əməkdaşları arasındakı münaqişələri həll etməli;

- öz fikirlərini qısa və dəqiq şəkildə ifadə etməlidir.

4.4. Təhlükəsizlik xidməti əməkdaşlarının hüquqları, öhdəlikləri və məsuliyyətləri

Təhlükəsizlik xidməti bölmələrinin əməkdaşları kommersiya sirri təşkil edən məlumatların mühafizə edilməsi üzrə aşağıdakı hüquqlara malikdirlər:

- firmanın bütün əməkdaşlarının, partnyorlarının, müştərilərinin kommersiya sirrinin mühafizə edilməsi üzrə normativ sənədlərin və ya müqavilə öhdəliklərinin tələblərini qeyd-şərtsiz yerinə yetirmələrini onlardan tələb etmək;

- kommersiya sirrinin mühafizə edilməsi üzrə hüquqi, təşkilati və mühəndis-texniki tədbirlərin təkmilləşdirilməsi üzrə təkliflər irəli sürmək;

Təhlükəsizlik xidmətinin əməkdaşları borcludurlar:

- kommersiya sirrinin mühafizə olunması üzrə təlimatlara riayət edilməsi üzərində nəzarəti həyata keçirməyə;

- kommersiya sirrinin mühafizə edilməsi üzrə normativ sənədlərin tələblərinin pozulması faktları, həmçinin məxfi informasiyanın sızması və ya sənədlərin və məmulatların itirilməsinə gətirib çıxara biləcək başqa fəaliyyətlər haqqında rəhbərliyə xəbər verməyə;

- kənar şəxslərin «Kommersiya sirri» qrifinə malik olan sənəd və materiallarla qanunsuz tanış olmalarına imkan verməməyə.

Təhlükəsizlik xidmətinin əməkdaşları müəssisənin əməkdaşlarının kommersiya sirrinin mühaifzəsini şəxsən pozmaları və onların funksional öhdəlikləri yerinə yetirərkən öz hüquqlarından istifadə etməmələri üzrə məsuliyyət daşıyırlar.

4.5. Təhlükəsizlik xidmətinin ştatdankənar strukturları

Kommersiya sirrinin mühafizəsinin daha geniş əhatə olunması və keyfiyyətlə yerinə yetirilməsi məqsədilə firma rəhbərliyi və təhlükəsizlik xidmətinin qərarı ilə müvəqqəti və daimi əsaslarda müəyyən nəzarət-təftiş funksiyalarını yerinə yetirən ayrıca komissiyalar yaradıla bilər ki, bunlara da aiddir:

- sənədlərin (materialların, məlumatların, qiymətLilərin) mövcud olması, vəziyyəti və uçotu üzrə rüblük və illik komissiyalar;
- dövri sənədlərin, elanların, prospektlərin, intervyuların və mətbuat, radio və televiziya, seminar, simpozium, konfrans və s.-dəki başqa çıxışların nəşr etdirilməsi imkanlarının qiymətləndirilməsi üzrə komissiya;
- kommersiya sirrinin mühafizə edilməsi üzrə bilik və bacarıqların yoxlanılması, həmçinin firmanın təhlükəsizliyinin təmin edilməsi üzrə təşkil edilmiş tədbirlərin effektivliyinin və etibarlılığıın qiymətləndirilməsi üçün müvəqqəti yoxlama komissiyaları;
- firmanın təhlükəsizliyinin auditi üzrə xüsusi qruplar.

4.6. Təhlükəsizlik xidmətinin fəaliyyətinin avtomatlaşdırılması

Təşkilati strukturların izah edilmiş funksiyaları və kommersiya sirrinin təhlükəsizliyinin təmin edilməsi üzrə həll edilən məsələlərin mürəkkəbliyi obyektiv olaraq hesablama texnikası vasitələrindən istifadə edilməsinə tələbat yaradır. Konkret həll kimi təhlükəsizlik xidmətinin vəzifəli şəxsləri üçün təşkilati-funksional avtomatlaşdırılmış iş yerlərindən (TXAİY) istifadə edilməsi tövsiyə edilə bilər.

Avtomatlaşdırma vasitələrinin tətbiq edilməsinin birinci mərhələsində AİY-lərinin təhlükəsizlik xidmətinin rəisi; üzərində «Kommersiya sirri» qrifi olan sənədlərin işlənməsi üzrə xüsusi şöbənin işçi qrupu; mühəndis-texniki qrup və bəzi hallarda isə xarici fəaliyyətin təhlili qrupu və heyətlə iş və rejim qrupu üçün işlənib hazırlanması mümkündür;

Sonrakı mərhələlərdə avtomatlaşdırma vasitələrinin tətbiqinin miqyası şəraitin dəyişməsindən asılı olaraq TX-nin cari fəaliyyətinin operativ idarə edilməsinin təmin edilməsi istiqamətində genişləndirilə bilər.

Avtomatlaşdırma vasitələrinin tətbiq edilməsinin daha sonrakı mərhələlərində firmanın korporativ avtomatlaşdırılmış sisteminin xüsusi təhlükəsizlik inzibatçısı qruplarını yaratmaq məqsədəuyğundur.

4.7. Təhlükəsizlik xidmətinin hüquq-mühafizə orqanları ilə qarşılıqlı hərəkətinin prinsip və istiqamətləri

Kommersiya müəssisəsinin təhlükəsizliyinin özütəşkili nə qədər mükəmməl olsa da, o, müvafiq hüquq-mühafizə orqanları, hər şeydən əvvəl isə polislə qarşılıqlı təsirə girmədən cinayətkar qəsdlərin qarşısını təmin edə bilmir.

Belə qarşılıqlı təsirin təşkilati-hüquqi əsası aşağıdakılardan ibarətdir:

- bütün tip mülkiyyətlərin mühafizəsinin konstitusion bərabərliyi prinsipi;

- Rusiya Federasiyasnın polis, operativ-axtarış, prokurorluq və başqa normativ-hüquqi aktlar haqqında qanunları.

Əməkdaşlığın məqsədi kommersiya müəssisəsinin heyətinə, pul vəsaitlərinə və material qiymətlilərinə qarşı edilən cinayətkar qəsdlər haqqında xəbərdar etmə və bu faktların üstünün açılmasından ibarətdir.

Müəssisə ilə daxili işlərin ərazi orqanının qarşılıqlı təsirinin prioritet istiqamətləri aşağıdakılar olmalıdır:

İnformasiya mübadiləsi:

- pul vəsaitlərinin saxta bank sənədləri, kredit kartları və başqa saxta sənədlərdən istifadə etməklə oğurlanması faktları (üsulları) haqqında;
- kommersiya müəssisəsində işləyən və qanun pozuntusunda şübhəli bilinən fiziki şəxslər haqqında;

Ümumi cinayət təzahurlərinin, öldürmək, yaxud ağır bədən xəsarətləri yetirmək təhlükələrinin, rəhbərlərin, əməkdaşların və onların ailə üzvlərinin əmlaklarının məhv edilməsinin nəzərdə tutulan (real) faktlarına qarşı obyektlərin texniki möhkəmləndirilməsi və siqnalizasiya vasitələri ilə təchiz edilməsi; daxili işlər nazirliyinin ərazi orqanları (polis) ilə «qaynar xəttin» yaradılması; müxtəlif mülkiyyət formalarına malik olan müəssisələr, işgüzar münasibətlərin vicdansız iştirakçıları haqqında regional verilənlər bankının formalaşdırılmasında iştirak edilməsi üzrə *birgə əks təsir tədbirlərinin işlənib hazırlanması*;

T*əhlükəsizlik xidməti kadrlarının seçilməsi, yerləşdirilməsi və peşəkar-casına hazırlanması üzrə işlər*: təhlükəsizlik xidmətində işləmək üçün nami-zədliklərin daxili işlər orqanlarının informasiya imkanlarından, məhkəməyə düşmə haqqında məlumatlardan və s. istifadə edərək birgə yoxlanılmasının həyata keçirilməsi; heyətin kommersiya sirrindən qanunsuz istifadə etməsi və ya onu yayması üzrə məsuliyyəti haqqında qaydaların birgə işlənib hazırlanması və tətbiq edilməsi; təhlükəsizlik xidməti kadrlarının

öyrədilməsi və ixtisaslarının artırılmasında polislərin köməyindən istifadə edilməsi.

Firmanın təhlükəsizlik xidmətinin hüquq-mühafizə orqanları ilə qarşılıqlı təsirinin vacibliyi aşağıdakı səbəblərlə şərtlənir:

- TX-nin güc və vasitələrinin kifayət qədər olmaması;
- Kriminal şərait və mütəşəkkil cinayətkarlıq fəaliyyətinin xüsusiyyətləri haqqında informasiya mənbələrinin məhdudluğu;
- Material qiymətlilərinin və maliyyə vəsaitlərinin uzaq məsafələrə nəql edilməsi üzərində mühafizənin çətinliyi;
- Firma və TX-nin yeni əməkdaşları haqqında informasiyanın əldə edilməsinin zəruriliyi;
- Hüquq-mühafizə orqanlarının hücumların dəf edilməsi və cinayətkar-ların (bədəməllərin) tutulması və saxlanılmasında kömək göstərməsi üçün cəlb edilməsinin zəruriliyi.

4.8. Təhlükəsizliyin idarə edilməsi

Təhlükəsizliyin idarə edilməsi dedikdə, firmanın fəaliyyətinə qarşı müxtəlif təhlükələrin aradan qaldırılması məqsədilə bütün xidmət, bölmə və əməkdaşların fəaliyyətinin uzlaşdırılmasını təmin edən mütəşəkkil fəaliyyəti başa düşəcəyik.

Mahiyyət etibarı ilə, təhlükəsizliyin idarə edilməsi verilmiş mühafizə səviyyəsinin saxlanılmasının fasiləsiz prosesidir.

Tərkibinə görə təhlükəsizliyin idarə edilməsi bu və ya digər böhran situasiyalarının ortaya çıxması halı üçün işlənib hazırlanmış plan tədbirlərinin vaxtında, ciddi şəkildə və dəqiqliklə yerinə yetirilməsindən ibarətdir.

Təhlükəsizliyin təmin edilməsi üzrə fəaliyyətin planlaşdırılması zəruriliyi şübhə doğurmur, çünki təhlükəsizlik xid-

məti bizneslə cinayətkar dünyanın məqsədlərinin toqquşması nəticəsində təzahür edən böhran situasiyalarının ortaya çıxmasına hər zaman hazır olmalıdır.

Böhran situasiyası – ayrı-ayrı şəxslər və ya qruplar tərəfindən təhlükə faktının təzahür olunmasıdır. Böhran situasiyası müxtəlif formada təzahür və inkişaf edə bilər: yavaş və ya spontan, ani.

Böhran situasiyasının qiymətləndirilməsi və təhlili zamanı TX-nin bu si-tuasiya ilə öz gücləri vasitəsilə başa gələ biləcəyi, yoxsa onun həll edilməsi üçün hüquq-mühafizə orqanlarının cəlb edilməsi lazımdır, sualına mümkün qədər tez cavab tapmalıdır. Ancaq, hər halda istənilən firma böhran situasiyasının ortaya çıxa bilməsinin mümkünlüyünü nəzərə alaraq TX-nin tərkibində böhran qrupu adında ayrıca şöbə yaratmağa çalışır. O, firmanın əsas şəxsləri içərisindən təşkil edilir: direktor, xətti bölmələrin, filialların, şöbələrin rəhbərləri, hüquqşünas, baş mühasib və s. Böhran qrupu daimi əsaslarda öz tərkibinə aşağıdakı üzvləri daxil etməklə yaradıla bilər:

- firmanın rəhbəri;
- hüquqşünas;
- maliyyəçi;
- təhlükəsizlik xidmətinin rəhbəri.

Böhran qrupuna rəhbərlik firmanın başçısına həvalə edilə bilər. Sadalanan şəxslər, bir qayda olaraq, öz xidməti vəziflərinə, xüsusi biliklərə və təcrübəyə sahib olduqlarına görə böhran situasiyasının ortaya çıxdığı və inkişaf etdiyi şəraitə kifayət qədər effektiv təsir etmə imkanlarına malik olurlar və bu zaman onlar gündəlik kommersiya və istehsal fəaliyyətinə təsir göstərən rıçaqların təsirlərini də nəzərdən qaçırmırlar.

Hər bir konkret halda böhran qrupunun tərkibinə başqa mütəxəssislər də daxil edilə bilər.

Böhran qrupu aşağıdakı məsələləri həll edir:

- şəraitin qiymətləndirilməsi;

- təhlükəsizlik üzrə təxirəsalınmaz tədbirlərin qəbul edilməsi;

- fövqəladə şəraitdə firmanın fəaliyyətinin idarə edilməsi;

- hüquq-mühafizə orqanları ilə operativ qarşılıqlı təsirin təmin edilməsi.

Böhran qrupunun yaradılmasının başlıca məqsədi – firmanın təhlükəsizliyinə qarşı xarici təhlükələrə əks təsir göstərməkdən ibarətdir. Qrupun işgüzar iclasları yüksək məxfilik şəraitində aparılmalıdırlar.

Bir qayda olaraq, böhran qrupunun fəaliyyəti firma rəhbərliyinin və heyətinin fəaliyyətinin sadə planı üzrə reqlamentləşdirillir (nizama salınır). Yaranmış situasiyalardan asılı olaraq planlar aşağıdakı formalarda ola bilər:

- partlayış təhlükəsi zamanı fəaliyyət planı;
- firmanın əməkdaşlarının oğurlanması və ya girov tutulması zamanı fəaliyyət planı;
- zorakılıq zamanı fəaliyyət planı;
- firmanın yerləşdiyi məkana hücum zamanı fəaliyyət planı;
- inkossatorlara hücum zamanı fəaliyyət planı.

Sadə böhran planları az insanın istifadə hüququ olduğu məxfi xarakterli sənədlər olmalıdırlar. Belə planlar iki-üç nüsxədən az olmayaraq tərtib edil-məlidirlər. Onların biri rəhbərdə, digəri – təhlükəsizlik xidmətinin rəisində, üçüncüsü isə firma rəhbəri olmadıqda onu əvəz edən şəxsdə saxlanmalıdır.

Planlaşdırmanı həyata keçirərkən bilmək etmək lazımdır ki, plan – tədbirlər dəsti yox, konkret böhran situasiyasında effektiv təhlükəsizliyin tə-min edilməsinə istiqamətlənmiş ardıcıl davranış və fəaliyyət strategiyasıdır.

Təhlükəsizlik sistemi fəaliyyətinin mümkün rejimlərini nəzərdən keçirək.

Mütəxəssislər üç rejimi fərqləndirirlər: gündəlik fəaliyyət, yüksək hazırlıq və fövqəladə vəziyyət.

Gündəlik rejim – təhlükəsizlik sisteminin normal fəaliyyət göstərməsidir və özünə aşağıdakıları daxil edir:

1) bütün təhlükə növlərinin proqnozlaşdırılması, aşkar edilməsi, qiymətləndirilməsi, qarşısının alınması və neytrallaşdırılması üzrə fəaliyyətlər;

2) təhlükəsizliyin təmin edilməsi üzrə plan və proqramlarının işlənib hazırlanması və korreksiya edilməsi;

3) kadrların seçilməsi, öyrədilməsi, monitorinqi və təkmilləşdirilməsi və bir sıra başqa fəaliyyətlər.

Yüksək hazırlıq rejimi – təhlükəsizlik sisteminin təhlükələrin mövcud olması və onların qarşısının alınması üzrə tədbirlər tələb edən fəaliyyətidir. Bu rejimə təhlükələrin neytrallaşdırılması, situasiyanın xüsusiyyətlərinin nəzərə alınması ilə dəfetmə planlarının dəqiqləşdirilməsi və təkmilləşdirilməsi, dəstək güclərinin hazırlığının yüksəldilməsi üzrə tədbirlər xasdır. Bu rejim zamanı təhlükəsizliyin operativ idarə edilməsi qrupunun (böhran qrupu) işinin başlanması da mümkündür. Operativ idarəetmə qrupu təhlükəsizliyin təmin edilməsinin gedişi prosesində firmanın mühafizə edilməsi üzrə istənilən zəruri tədbirləri həyata keçirir.

Bu rejimə uyğun olaraq, artıq təşkil edilmiş gündəlik hazırlığa əlavə olaraq aşağıdakı fəaliyyətlər də həyata keçirilir:

4) təhlükələrin dəf edilməsi planlarının dəqiqləşdirilməsi və təkmilləşdirilməsi;

5) dəstək güclərinin hazırlığının artırılması;

6) operativ idarəetmə qrupunun işə başlaması.

Fövqəladə vəziyyət rejimi – TX-nin bədəməllərin aktiv fəaliyyətlərinin dəf edilməsini və aradan qalldırılmasını tələb edən real təhlükələrin mövcud olması zamanı fəaliyyətidir.

Bu halda:

7) təhlükəsizlik şurası gündəlik iş rejiminə keçir;

8) TX-nin, firmanın əməkdaşlarının bilavasitə təhlükələrin dəf edilməsinə qarşı tam hazırlığı təmin edilir;

9) dəstək gücləri cəlb edilir və daxili iş orqanları gücləndirilir.

4.9. Təhlükəsizlik xidmətinin rəisi

Təhlükəsizlik xidmətinin rəisi xidmətin bütün şəxsi heyətinin birbaşa rəisidir.

O, bilavasitə firmanın direktoruna, yaxud müəyyən ştat cədvəlinə və ya firma üzrə müəyyən əmrə görə onun müavinlərindən birinə tabedir. TX rəisi müstəsna olaraq firma direksiyasının (müdiriyyətinin) səlahiyyətinə aid edilənlərdən başqa TX-nin bütün cari fəaliyyətinə rəhbərlik edir. Firma müdiriyyəti tərəfindən ona məxsus olan hüquqların bir hissəsini TX rəisinin səlahiyyətinə verdikdə, TX firmanın müdiriyyətinin qərarında göstərilən funksiyaları həyata keçirir.

TX-nin rəisi firma müdiriyyəti tərəfindən ali savadlı şəxslər içərisindən təyin edilir. Firmanın direktoru müdiriyyətin tapşırığı ilə onunla əmək müqaviləsi bağlayır. Müqavilədə TX rəisinin vəzifə öhdəlikləri və iş şəraiti müfəssəl şəkildə şərtləndirilir.

TX-nin rəisi firmanın direktoruna hesabat verir və onun qarşısında TX fəaliyyətinin həyata keçirilməsi və onun üzərinə qoyulmuş vəzifə və funksiyaların yerinə yetirilməsi üzrə məsuliyyət daşıyır.

TX-nin rəisi etibarnamə (vəkalətnamə) olmadan TX adından onun bütün fəaliyyətində çıxış edir, TX-nin bütün hüquqi və mühasibat sənədlərini imzalamaq hüququna malikdir, TX işçilərinin vəzifə məvaciblərini müəyyən edir, həvəsləndirmə və cərimələr üzrə məsələləri həll edir, TX-nin əməkdaşları ilə əmək müqavilələri bağlayır, işə vətəndaş-hüquq razılaşmaları əsasında işçilər cəlb edir, onların əməyinin ödənilməsi şərtlərini müstəqil olaraq müəyyən

edir, TX-nin rəis müavini, TX şöbələrinin və qruplarının rəhbəri vəzifəsinə namizədlikləri firma müdiriyyəti tərəfindən təsdiq olunması üçün təqdim edir.

TX-nin rəisi işləmədiyi dövr ərzində öz səlahiyyətlərini müavininə verir.

Təhlükəsizlik xidməti rəisi aşağıdakılara görə məsuliyyət daşıyır:

- Rusiya Federasiyasının mövcud qanunvericiliyinə ciddi və dəqiq riayət edilməsi şəraitində öz təsisçi firmasının təhlükəsizliyi üzrə mühafizə və axtarış xidmətlərinin göstərilməsi;

- Firma tərəfindən əldə edilən xüsusi vasitələrin, silahların və hərbi sursatların mühafizə olunmasının təmin edilməsi;

- Təhlükəsizlik xidməti işçilərinin peşəkar hazırlığının keyfiyyəti.

O borcludur:

- öz fəaliyyətində Rusiya Federasiyasının «Rusiya Federasiyasında xüsusi xəfiyyə və mühafizə fəaliyyəti haqqındakı» qanununun, Rusiya Federasiyasının başqa qanun və hüquqi aktlarının, firmanın nizamnamə normativləri və təhlükəsizlik xidmətinin vəziyyətinin tələblərinə istinad etməyə;

- şəxsən özü və ona həvalə edilmiş təhlükəsizlik xidməti üçün ona mühafizə fəaliyyətilə məşğul olmaq hüququ verən lisenziyanı əldə etməyə;

- tabeçilikdə olan şəxslərin öz vəzifələrini daşımalarını təşkil etməyə və onun keyfiyyətinə nəzarət etməyə;

- mülkiyyətçinin ona tapşırılmış əmlakını mühafizə etməyə, həmin əmlaka, vətəndaşların həyat və sağlamlıqlarına və təhlükəsizlik xidmətinin şəxsi heyətinə qarşı edilən qanunsuz qəsdlərin dəf edilməsinin təmin edilməsi üzrə təcili tədbirləri təşkil etməyə; bütün bu qəsdlər və onların nəticələri haqqında birbaşa öz rəhbərinə hesabat verməyə;

- xidmətin şəxsi heyəti tərəfindən odlu silahdan bütün istifadə edilməsi halları haqqında daxili iş orqanlarını silahın tətbiq edildiyi yer barəsində dərhal xəbərdar etməyə;

- prokurorun bütün qətl və ya bədən xəsarətinin vurulması halları haqqında dərhal məlumatlandırılmasına;

- firma rəhbərliyinin əmri üzrə inkassasiya xidmətlərindən istifadə edilməsi üzrə başqa müəssisə və təşkilatlarla bağlanılan müqavilələri firmanın rəhbərliyi tərəfindən imzalanması üçün təqdim etməyə;

- təhlükəsizlik xidmətinin şəxsi heyətinin vaxtında hazırlanmasını, yenidən hazırlanmasını və ixtisasının artırılmasını bu məqsədlə razılaşdırılmış qaydada ixtisaslaşdırılmış dövlət və ya qeyri-dövlət lisenziyalaşdırılmış təhsil idarələri bazalarından (mərkəzlər, poliqonlar, tirlər, atəş meydanları və s.) istifadə etməklə təşkil etməyə;

- xüsusi mühafizəçi və xəfiyyələrin onların xüsusi vasitə və odlu silahdan istifadə etməklə əlaqədar fəaliyyətlərə yararlılıqlarının dövri olaraq yoxlanılmasının Rusiya Federasiyası Daxili İşlər Nazirliyi tərəfindən müəyyən olunan qaydada aparılmasını təşkil etməyə;

- firmanın kadr və maliyyə orqanları ilə xidmətin işçiləri üçün əmək stajının, dövlət sosial sığortası üzrə müavinətlərin hesablanması üçün staj, mühafizə fəaLiyyətinin həyata keçirilməsi ilə əlaqədar həlak olma, əlil olma və başqa bədən xəsarətləri alma hallarında sığortanın zəruriliyi məsələsi üzrə qarşılıqlı fəaliyyəti təşkil etməyə;

- lisenziyaların şəxsi heyət və təhlükəsizlik xidməti üzrə fəaliyyət müddətini nəzarətdə saxlamağa və bu müddətin uzadılması üçün vaxtlı-vaxtında tədbirlər görməyə;

- silahların, hərbi sursatların və xüsusi vasitələrin uçotu və etibarlı mühafizə edilməsinin təmin edilməsini təşkil etməyə;

- odlu silahın, ona müvafiq hərbi sursatların və xüsusi vasitələrin uçotu, saxlanılması, gəzdirilməsi və daşınması qaydaları üzərində nəzarəti həyata keçirməyə;

- xüsusi vasitələrin, hərbi sursatların və odlu silahların çatışmamazlığı, xarab olması və artıqlığının hər bir halı üzrə xidməti təhqiqat aparmağa;

- təhlükəsizlik xidmətinin vaxtlı-vaxtında vergi və başqa maliyyə öhdəliklərinin yerinə yetirilməsi və anoloji öhdəliklərə xidmətin şəxsi heyəti
tərəfindən riayət edilməsinə nəzarət etməyə;

- xüsusi xəfiyyə və mühafizə müəssisələrinin və təhlükəsizlik xidmətlərinin fəaliyyəti üzrə nəzarəti həyata keçirən orqanların səlahiyyətli şəxslərinə nəzarət funksiyalarını yerinə yetirmək üçün vacib olan sənədləri, yazılı və (və ya) şifahi informasiyanı təqdim etməyə.

Təhlükəsizlik xidmətinin rəisinə mühafizə fəaliyyəti ilə dövlət xidmətini, yaxud ictimai birliklərdə (təşkilatlarda) ödənişli və seçkili vəzifəni birləşdirməyə, həmçinin kənar müəssisələrə şəxsən və ya təhlükəsizliyin təmin edilməsi ilə əlaqədar olan öz tabeçiliyində olan işçilər vasitəsilə xidmət göstərməyə icazə verilmir.

Amerikan mütəxəssislərinin «Biznes və təhlükəsizlik» adlı beynəlxalq konfransda söylədikləri fikrə görə təhlükəsizlik xidməti rəhbərinə təhlükəsizlik sahəsində uğurlu iş üçün aşağıdakı zaman məsrəfləri tələb olunur:

Cədvəl 10

1	Menecment – 6%
2	Təşkilati məsələlər – 5%
3	Heyətin təhlükəsizliyi – 7%
4	Firmanın fiziki təhlükəsizliyi – 16%
5	İnformasiyanın qorunması – 7%

6	Təhlükəsizlik vasitələri – 2%
7	TX heyəti və əməkdaşları tərəfindən sui-istifadə hallarının nəzərdən keçirilməsi – 4%
8	Təhlükələrin qarşısının alınması – 14%
9	Başqa təşkilatlar və daxili işlər orqanları ilə əlaqələr – 8%
10	Digər məsələlər – 18%

FƏSİL V

TƏHLÜKƏSİZLİK XİDMƏTİNİN REJİM VƏ MÜHAFİZƏ ŞÖBƏSİ

Rejim və mühafizənin təmin edilməsi üzrə təhlükəsizlik xidmətinin əsas vəzifəsi konkret şəraitdə bütün mümkün üsul və vasitələrlə fəaliyyətin təhlükəsizliyinin təmin edilməsi və informasiyanın qorunmasından ibarətdir.

Maddi qiymətlilərin, özünə kommersiya xarakterli məlumatları birləşdirən məxfi sənədlərin və informasiyanın etibarlı mühaifzəsinin təmin edilməsi, həmçinin onlardan icazəsiz istifadə cəhdləri haqqında vaxtında xəbərdarlıq edilməsi məqsədilə müəyyən fəaliyyət rejimi təyin edilir ki, bu rejimə riayət edilməsi bütün əməkdaşlar, ziyarətçilər və müştərilər üçün məcburidir.

Firmanın rejim və mühafizə fəaliyyətini təmin edən və həyata keçirən rəhbər və əməkdaşları öz fəaliyyətlərində müvafiq qanunverici, normativ sənədlərə və mövcüd tövsiyyələrə istinad edirlər.

Rejim və mühafizənin təşkil edilməsinin başlıca vəzifələri aşağıdakılardır:

- xidməti yerlərə (otaqlara), qorunan zona və obyektlərin ərazilərinə kənar şəxslərin daxil olması haqqında xəbərdarlıq;
- maddi qiymətlilərin gətirilməsi (aparılması), içəri salınması (kənara çıxarılması), əməkdaşların və müştərilərin giriş (çıxış) qaydalarının təmin edilməsi.

Firmanın bütün otaqları təyinatından və onların daxilində aparılan aktların, fəaliyyətlərin və ya əməliyyatların xarakterindən asılı olaraq, obyektin kriminal təhlükə üzrə mümkün zərər alması nöqteyi-nəzərindən müxtəlif hissələrinin vaciblik səviyyəsini nəzərə alan bir neçə təhlükəsizlik zonasına bölünür. Təhlükəsizlik zonaları obyektin ərazisindəki hasardan qiymətlilərin və informasiyanın saxlandığı anbara qədər, bədəməlin dəf etməli olduğu növbələşən maneələr zənciri yaradaraq ardıcıl yerləşirilir.

5.1. Obyektdaxili rejimin tələbləri

1. Obyektdaxili rejim – firmada iqtisadi təhlükəsizliyin təmin edilməsinə, maddi vasitələrin saxlanılmasına və məxfi informasiyanın qorunmasına istiqamətlənmiş daxili əmək qaydalarının yerinə yetirilməsi üzrə qurulmuş idarə üsuludur.

2. Obyektdaxili rejim aşağıdakı başlıca tələbləri nəzərdə tutur:

- iş vaxtının dəqiq nizam qaydalarının təyin olunması;
- əməkdaşlar tərəfindən iqtisadi və informasiya təhlükəsizliyi qaydalarına, yanğın əleyhinə və qəza əleyhinə qaydalara və texniki təhlükəsizlik qaydalarına ciddi şəkildə riayət edilməsi;
- kənar təşkilatların ziyarətçilərinin qəbulu və onlarla iş üzrə qaydaların təyin edilməsi;

- firmanın istehsal fəaliyyətini (rabitə, avtomatlaşdırma, mühafizə və yanğın siqnalizasiyası, qıfıllar, hasarlanmalar və s.) təmin edən texniki vasitələrlə təchiz edilməsi;

- yerlərin mühafizəyə təhvil və təslim verilməsi qaydaları;

- informasiyanın məxfilik və qənaət rejimlərinə riayət edilməklə telefon, faks və telekommunikasiya vasitələri üzrə mübadilə edilməsi qaydaları.

3. Kənar təşkilatların nümayəndələri ilə iş aşağıdakı qaydada həyata keçirilir:

- qəbul edən mütəxəssis dəftərxana şöbəsinə sabahısı gün gəlməli olan nümayəndələrin S.A.A., onların iş yerləri və nəzərdə tutulan təşrif müddətinin göstərildiyi ərizə verir;

- dəvət olunmuş nümayəndələrin varid olduqları gün dəftərxana şöbəsi onların gəlişini ziyarətçilərin qeydiyyat jurnalında qeyd edir və firmanın mütəxəssisini dəvət edir;

- mütəxəssis gələn nümayəndələri qarşılayır, dəftərxana şöbəsindən danışıqların aparılması otağının açarlarını alır və ziyarətçiləri həmin otağa aparır. Kənar təşkilatların nümayəndələrinin direktor və ya onun müavininin icazəsi olmadan ofisin başqa otaqlarında qəbul olunması qadağandır;

- işin gedişi zamanı pəncərə və qapıları sıx bağlamaq lazımdır;

- nümayəndələrlə işi bitdikdən sonra onları qəbul edən mütəxəssis onları ofisin çıxış qapısına qədər yola salır və ziyarətçilərin qeydiyyat jurnalında onların getmə vaxtı haqqında qeyd edir. Ziyarətçilərin gəlişi zamanı qəbul edən mütəxəssis onların ofis daxilində qalmasına və hərəktlərinə nəzarət etməlidir. Görüş bitdikdən sonra firma mütəxəssisi danışıqlar otağının qapısını bağlayır və açarı dəftərxana şöbəsinə verir.

5.2. Buraxılış rejimi

Buraxılış rejimi – firmada, təşkilatda və ya müəssisədə nəzarətsiz keçidinin (girişinin) və maddi qiymətlilərin nəzarətsiz gətirilməsinin (aparılmasının) istisna edildiyi təyin edilmiş qaydalardır.

Əməkdaşların, qulluqçuların və başqa şəxslərin mühafizə edilən obyekt ərazisinə keçməsi (girməsi) və əksinə hərəkət etməsi, material qiymətlilərinin gətirilməsi (aparılması) nəzarət-buraxılış və giriş keçidlərində icazə vərəqələri üzrə həyata keçirilir.

Buraxılış rejimi aşağıdakıları nəzərdə tutur:

- obyekt yerləşən əraziyə işçilərin, həmin obyektin qulluqçularının və ziyarətçilərin buraxılmasının müəyyən qaydalarının təyin edilməsi;
- məhsulların və maddi qiymətlilərin idxal (ixracının), gətirilməsi (aparılmasının) müəyyən qaydalarının təyin edilməsi;
- hasarlanma, işıqlandırma, nəzarət-buraxılış, giriş məntəqələrinin (postların) və buraxılış bürolarının siqnalizasiya, rabitə və buraxılış rejiminin həyata keçirilməsini təmin edən başqa lazımi texnika ilə təchiz edilməsi, həmçinin onların sənədlər və inventarlarla təmin edilməsi;
- bütün növ icazə vərəqələrinin verilməsi və imzalanması hüququna malik olan vəzifəli şəxslər dairəsinin müəyyən edilməsi;
- şəxsi əşya mühafizə kameralarının və şəxsi avtomobil meydançalarının təchiz edilməsi.

5.2.1. Buraxılış rejiminin təşkil edilməsi

Firmaya buraxılışın tənzimlənməsi sistemi aşağıdakıları nəzərdə tutmalıdır:

- işə buraxılan şəxslərin etibarlılıqlarının obyektiv olaraq müəyyən edilməsi;
- firma obyektlərinə buraxılan şəxslərin sayının maksimum dərəcədə məhdudlaşdırılması;

- hər bir işçinin (və ya ziyarətçinin) zaman, məkan və fəaliyyət növü üzrə diferensiasiya edilmiş obyektə buraxılış hüququnun təyin edilməsi;

- sənədlərin obyektə gətirilməsi (həmçinin, miniklə) üzrə icazə verilməsi və onların rəsmiləşdirilməsi qaydalarının dəqiq şəkildə müəyyən edilməsi;

- hər bir buraxılış və giriş məntəqəsində nəzarət-buraxılış funksiyalarının həcmlərinin müəyyən edilməsi;

- nəzarət-buraxılış məntəqələrindən (postlarından) keçənlərin səhih yoxlanılmasını, keçişin obyektiv olaraq qeydiyyatdan keçirilməsini və kənar şəxslərin icazəsiz (o cümlədən, zorla) keçidinin qarşısının alınmasını təmin edən texniki vasitələrlə təchiz edilməsi;

- nəzarət-buraxılış məntəqəsi heyətinin yüksək hazırlığı və mühafizə olunması.

Cədvəl 11

Firmanın rejimli zonalarının təsnifatı

Buraxılış rejimi kateqoriyaları	Adı	Funksional təyinatı	Əməkdaşların buraxılış şərtləri	Ziyarətçilərin buraxılış şərtləri	Mühafizənin mövcud olması	Mühafizənin texniki vasitələrinin mövcud olması
0	Azad	Azad ziyarət zonası	Azad	Azad	Yoxdur	Yoxdur
1	Müşahidə edilən	Ziyarətçilərin qəbulu zonası	Azad	Azad	Məhdud	Müşahidə və yazı vasitələri
2	Qeydiyyatlı	Xidməti otaqlar və əməkdaşların kabinetlərinin yerləşdiyi zona	Xidməti zərurət üzündən məh-dudlaş-dırıl-mış	Birdəfəlik buraxılışlar üzrə qeyd edilən	Ayrı-ayrı zonalarda	Mühafizə və nəzarət vasitələri

3	Re-jimli	Rəhbər heyətin, xüsusi bölmələ-rin və maliyyə xidməti zonası	Ciddi şəkildə məhdudlaş-dırılmış	Birdəfəlik buraxılışlar üzrə, müşayiətlə qeyd edilən	Güclən-diril-miş çoxzo-nalı	Mühafizə, nəzarət və müşahidə vasitələri

5.2.2. Buraxılış sənədləri

Adətən əməkdaşların və ziyarətçilərin firma ərazisinə girmək, material qiymətlilərin idxal (ixrac) etmək, gətirmək (aparmaq) hüququ verən aşağıdakı növ buraxılış sənədləri təyin edilir:

- vəsiqə;
- buraxılış vərəqəsi.

Buraxılış vərəqələri əməkdaşlar və ziyarətçilər üçün daimi, müvəqqəti və birdəfəllik, həmçinin maddi qiymətlilərin gətirilməsi (aparılması) üçün material buraxılış vərəqəsi şəklində ola bilər.

Vəsiqə və buraxılış vərəqələrinin üzərinə rejim qaydaları üzrə nəzərdə tutulan möhurlər vurulur və buraxılış zonasını, onun fəaliyyət müddətini və çantanın (keyslərin, qovluqların və s.) içəri salınması qaydalarını müəyyən edən rəqəmli işarələr qoyulur. Əməkdaşların iş və işdənkənar vaxtlarda firmanın ərazisində qalma müddəti rəhbərlik tərəfindən vəsiqə və buraxılış vərəqələrinin üzərində rəqəmli işarənin qoyulması vasitəsilə müəyyən edilir. Vəsiqə və buraxılış vərəqələrinin nümunələri təhlükəsizlik xidməti tərəfindən işlənib hazırlanır və firma rəhbərliyi tərəfindən təsdiq edilir.

Şəxsiyyət vəsiqələrinin, buraxılış vərəqələrinin, rəqməli işarələrin ottisklərinin (basmalarının), vəsiqə və buraxılış vərəqələri üzərinə vurulan möhurlərin (ştampların), vəsiqə və buraxılış vərəqələrini imzalamaq hüququna malik olan rəhbər və səlahiyyətli şəxslərin imzalarının nümunələrinin

olduğu siyahıların təsdiqlənmiş nümunələri qeyd edilmə əsasında rejim və mühafizə şöbəsinin rəisinə verilir.

Vəsiqə və daimi buraxılış vərəqələrinin tam əvəzlənməsi bir qayda olaraq 3-5 ildən bir aparılır. 2-3 ildən sonra müvafiq qeyd etmə ilə onların yenidən qeydiyyatdan keçirilməsi həyata keçirilir.

Buraxılış sənədlərinin yenidən qeydiyyatdan keçirilməsi, əvəzlənməsi və ya dəyişdirilməsi üçün hər il 1 yanvar tarixinə kadrlar şöbəsindən təhlü-kəsizlik xidmətinə vəzifəsinin, soyadının, adının, atasının adının və sənədin müvafiq nişanla (gecə-gündüz, iş vaxtı –dən, -ə qədər, çanta ilə, hansı zo-
naya və s.) adının göstərildiyi əməkdaşların siyahısı göndərilir.

Vəsiqə və daimi buraxılış vərəqələri firmada işləməyən şəxslərə rəhbərlik tərəfindən onların işlədiyi yerlərin, vəzifələrinin, soyadlarının, adlarının, atalarının adlarının və müvafiq qeydlərin göstərildiyi təsdiqlənmiş siyahı üzrə verilə bilər. Bu sənədlər daimi olaraq buraxılış bürosunda (yaxud səlahiyyətli şəxsdə) saxlanmalı və ziyarətçinin gəlişi zamanı ona verilməlidir. İşin bitməsindən sonra bu şəxslər həmin sənədləri buraxılış bürosuna verirlər.

Göstərilmiş şəxslərə vəsiqələr və daimi buraxılış vərəqələri onların ştatda olduqları idarələrin rəhbərlərinin yazılı xahişləri əsasında verilir.

Üzərində əməkdaşın rəsmi olan və üç aylıq müddətə malik olan müvəqqəti buraxılış vərəqələri müvəqqəti olaraq işləyən və ya ezam edilmiş şəxslərə verilir. Rəsmisiz və bir aya qədər fəaliyyət müddətinə malik olan müvəqqəti buraxılış vərəqələri pasportun (şəxsiyyət vəsiqəsinin) təqdim edildiyi təqdirdə işləyir.

Müvəqqəti buraxılış vərəqələrinin fəaliyyət müddətinin iki aydan çox olmayaraq artırılmasına yol verilir.

Vəsiqə və buraxılış vərəqələri əməkdaşların işə qəbulu zamanı onların ştata daxil edildiyi haqda əmr əsasında verilir.

Birdəfəlik və material buraxılış vərəqələri.

Birdəfəlik buraxılış vərəqəsi onun verilməsindən binaya girmə anına qədər 30 dəqiqə, həmçinin onun üzərində ziyarətçinin firmadan getməsi haqqında qeydin edilməsi anından ziyarətçinin binanı tərk etməsinə qədər 15 dəqiqə müddətində işləyir. Ziyarətçinin olduğu bölmənin rəhbərliyi birdəfəlik buraxılış vərəqəsinin arxasında ziyarətçinin getdiyi vaxt haqqında qeyd etməli və öz soyadını göstərməklə imza qoymalıdır.

Material buraxılış vərəqələri maddi vasitələrinin mühafizə edilməsi üzrə məsuliyyət daşyıan şəxslərə verilir.

Vəsiqə və buraxılış vərəqələrinin uçotu, onların rəsmiləşdirilməsi və ve-rilməsi müvafiq uçot-nəzarət sənədlərində buraxılış bürosu tərəfindən həyata keçirilir.

İş günü bitdikdən sonra buraxılış bürosu əməkdaşları mühafizəçilərdən onlar tərəfindən verilmiş birdəfəlik buraxılış vərəqələrini (onlara birləşdirilimiş talonlarla birlikdə) və material buraxılış vərəqələrini *birdəfəlik və material buraxılış vərəqələrinin üçotu jurnal*ında qeyd edilməklə alırlar.

Buraxılış vərəqələrinin yoxlanılması, tutuşdurulması və öz kötüklərinə yapışdırılması gündəlik olaraq onları elə həmin gün verən buraxılış bürosu əməkdaşları tərəfindən yerinə yetirilir.

İstifadə olunmuş və qopardılmış talonların yapışdırıldığı birdəfəlik və material buraxılış vərəqələrinin kitabçaları, həmçinin onlar üzrə tələbnamələr üç ay ərzində saxlanılır, bundan sonra onlar müvafiq qaydada məhv edilirlər.

İstifadə olunmuş birdəfəlik və material buraxılış vərəqələri lazım olduqca, lakin ildə bir dəfədən tez olmayaraq məhv edilir.

Sənədlərin buraxılış rejimi üzrə uçotu üçün aşağıdakı uçot işləri, kitabları və jurnalları təşkil edilir:

- buraxılış rejimi üzrə əmr və göstərişlərlə bağlı iş;
- bölmə əməkdaşlarının vəsiqələr, daimi və müvəqqəti buraxılış vərəqələri üzrə verdikləri ərizələrlə bağlı iş;
- buraxılış rejimi və material buraxılış vərəqələri üçün imza nümunələri üzrə təlimatlarla bağlı iş;
- buraxılış sənədlərinin məhv edilməsi üzrə aktlarla bağlı iş;
- buraxılış rejimi üzrə köçürülmə ilə bağlı iş;
- birdəfəlik buraxılış vərəqələrinin blankları üzrə məsrəflərin gündəlik uçot kitabı;
- vəsiqələrin, daimi və müvəqqəti buraxılış vərəqələrinin verilməsinin uçot kitabı;

Bundan başqa, buraxılış bürosu ziyarətçilərin birdəfəlik buraxılış vərəqələri üzrə uçotu kitabını da təşkil edir.

Bütün növ buraxılış sənədlərinin tərtibi üçün buraxılış bürosu aşağıdakı
möhür və ştamplara malik olmalıdır:

- birdəfəlik və material buraxılış vərəqələri üçün dairəvi (diametri 25 mm) və ya üçbucaq şəkilli kauçuk möhür;
- vəsiqə və daimi buraxılış vərəqələri üçün dairəvi, relyefli, metal və ya kauçuk möhur (diametr 20 mm);
- rəqəmli nişan ştampları;
- «ÖDƏNİLMİŞDİR», «NÜMUNƏ», «MÜVƏQQƏTİ» ştampları.

Firmanın möhür və ştamplarının uçot jurnalında hər bir ştamp və möhurun ottiskinin tərkibi və təyinatının izahı verilir.

Möhür və ştampların yenisi ilə əvəz edilməsi zamanı köhnələr məhv edilir (aktla rəsmiləşdirilir), jurnalda isə müvafiq qeyd edilir. Yenilər üçün yeni qrafalar yaradılır.

5.3. Stasionar obyektlərin mühafizəsinin təmin edilməsi

Stasionar obyektlərin təhlükəsizliyinin təmin edilməsi özündə əsas etibarı ilə xəbərdarlıq xarakterli mühafizə tədbirlərinin çoxcəhətli reallaşdırılma prosesini əks etdirir. Həqiqətən də, yalnız o mühafizə sistemi effektiv hesab edilə bilər ki, o, ya bədməllərə təhlükəsizlik rejimindəki dəliyi tapmağa sadəcə olaraq imkan vermir, ya da cinayətkar qəsdlərin qarşısını onların ən erkən mərhələsində almaq imkanı yaradır.

Obyektin mühafizə edilməsi sisteminin işlənib hazırlanması və onun fəaliyyətinin təşkil edilməsi əsasında təhlükəsizliyin ardıcıl hüdudlarının yaradılması prinsipi durur. Bu hüdudlar daxilində təhlükələr vaxtında aşkar edilməlidir. Belə hədlər ardıcıl olaraq obyektin yerləşdiyi ərazi ətrafındakı hasardan, əsas, xüsusi vacib otağa qədər, misal üçün qiymətlilər və məxfi informasiyanın saxlandığı anbara qədər ardıcıl yerləşməlidirlər.

Nümunə üçün icazəsiz girişdən mühafizəni nəzərdən keçirək. Bədəməl ofis binası və ziyarətçilərin və əməkdaşların avtomobillərinin saxlanıldığı meydanlar yerləşən obyektin ərazisinə daxil olur. Ərazi üçün mümkün təhlükə – avtomobillərin oğurlanması, onların xarab edilməsi və ya onlarda partlayıcı, yaxud dinləyici qurğuların quraşdırılmasıdır. Ərazinin mühafizəsi onun perimetrinin müxtəlif formalı hasarlanmalarından, xüsusi təchiz edilmiş keçid və giriş yerlərindən, mühafizə siqnaLizasiyasından, mühafizə işıqlandırılmasından və mühafizə televiziya müşahidəsindən ibarət olmalıdır.

Ancaq bədəməl buna rəğmən dayanmaz və binaya, daha sonra isə qiymətlilərin və informasiyanın saxlanıldığı anbara daxil olmağa cəhd etməkdə davam edə bilər. Buradan aydın olur ki, obyektin bütün iştirakçılarının mühafizə

vasitələri bir-birilərini qarşılıqlı olaraq tamamlamalı və bütün icazəsiz daxilolmalardan mühafizə sisteminin effektivliyi bədəməlin bütün təhlükəsizlik hüdudlarını keçmək üçün sərf edəcəyi minimal zamana (bir neçə on dəqiqə) görə qiymətləndirilməlidir. Bu müddət ərzində mühafizə siqnalizasiyası işə düşməli, mühafizə xidmətinin əməkdaşları həyəcanın səbəbini təyin etməli və bədəməlin tutulması üzrə tədbirlər görməlidirlər.

Beləliklə, mühafizə sisteminin effektivliyi təhlükənin ortaya çıxması anından, onun ləğv edilməsinə başlanılmasına qədər olan müddətlə qiymətləndirilir. Mühafizə sistemi nə qədər mürəkkəb və çoxşaxəli olsa, onun dəf edilməsi üçün bir o qədər çox güc tələb olunar və təhlükənin aşkar edilməsi, müəyyənləşdirilməsi, dəf edilməsi və ləğv edilməsi ehtimalı da bir o qədər yüksək olar.

Mühafizə üsulları və vasitələrinin seçilməsinə təsir göstərən amllər sırasına aiddir:

- mühafizə olunan obyektə qarşı mümkün cinayət qəsdləri;
- mühafizə olunan obyektin texniki möhkəmlik dərəcəsi;
- mühafizə-yanğın vasitələrinin mövcud olması və keyfiyyəti;
- obyektin texniki möhkəmliyində yalnız mühafizə və təhlükəsizlik xidmətinə məlum olan kövrək yerlərin mövcud olması;
- qorunan obyektin yerləşdiyi yerin şəraiti, həmçinin onun konstruktiv xüsusiyyətləri;
- qorunan obyektin işinin rejim və xarakteri, onun texnoloji xarakte-ristikaları, obyektdə mövcud olan maddi və maliyyə qiymətliləri;
- obyektin mühafizə rejimi;
- mühafizə xidmətinin kəmiyyət və keyfiyyət xarakteristikaları;

- mühafizəçilərin silahlanma və texniki təchizatlılığı, onlarda avtonəqliyyatın, rabitə, siqnalizasiya vasitələrinin və xüsusi vasitələrin mövcud olması.

Obyektin mühafizə rejimi zamana görə gecə-gündüz (sutkalıq), qismən (sutkanın müəyyən saatlarında) və ya seçmə xarakterli ola bilər. İstifadə edilən güc və vasitələrin miqdarından, obyekt və ya əraziyə nəzarətin sıxlığından asılı olaraq mühafizə rejimi sadə və gücləndirilmiş ola bilər.

Qorunan obyektlərin əhəmiyyətli hissələrində mühafizəçilər sutka ərzində mövcud olurlar. Gündüz vaxtı onlar obyektə gələn ziyarətçilərə nəzarət edir, nəzarət-buraxılış rejimini həyata keçirir, gecə vaxtı isə obyektin qorunması üzrə bütün məsuliyyəti öz üzərlərinə götürərək onun qapalı mühafizəsini təşkil edirlər. Bəzi obyektlər yalnız epizodik olaraq, yəni zaman üzrə seçmə yolu ilə mühafizə olunurlar. Belə obyektlərə sahibinin olmadığı dövr ərzində mühafizə olunan mənzillər, əmtəə-material qiymətlilərinin gətirilməsi dövründə müvəqqəti anbar və ərazilər və b. aiddir.

Bir neçə mühafizə forması mövcuddur, o cümlədən:

- texniki vasitələrin köməyilə, mərkəzləşdirilmiş televiziya pultuna qoşulmuş və avtomatik siqnalizasiya qurğusu olan mühafizə;
- postların qurulması yolu ilə mühafizə (mühafizə şöbəsi və polisin gücü ilə);
- kombinələşdirilmiş mühafizə.

5.3.1. Texniki vasitələrin köməyilə mühafizə

Obyektdəki otaqların mühafizə və nəzarət edilməsi üçün təyinatı və texniki icrasına görə müxtəlif mühafizə vasitələrindən geniş istifadə olunur. Onların köməyilə yanğının meydana çıxmasını, sadəcə olaraq perimetrin pozulmasını (məsələn, əgər külək pəncərəni açsa, yaxud şüşəni sındırsa), otaq daxilində kiminsə və ya nəinsə hərəkət etməsini, nəzarət edilən predmetə (məsələn, otaq daxilində yerləşən seyfə) toxunuşu aşkar etmək olar.

Bir qayda olaraq, kənar şəxslərin daxil olması arzuedilməz olan otaqların mühafizə olunması üçün çoxhüdudlu qorumanı reallaşdıran texniki vasitələr kompleksindən istifadə edilir.

Çoxhüdudlu qorumanın tətbiqi mühafizənin etibarlığını əhəmiyyətli dərəcədə artırır, çünki bu zaman həmin hüdudlardan hər hansı birininin texniki nasazlıq və ya ola bilsin ki, müasir mühafizə siqnalizasiyası sistemləri ilə tanış olan bədəməlin düşünülmüş fəaliyyəti nəticəsində işə düşməməsi halının sığortalanması mümkündür.

Birinci sərhəd vasitəsilə otaqların perimetrlərinin tikinti konstruksiyaları, qapı və pəncərə yerləri, lyuklar, ventilyasiya kanalları, istilik sistemləri, nazik divar arakəsmələri və bayır tərəfdən daxil olması mümkün olan otağın başqa elementləri, o cümlədən polad barmaqlıqlarla təchiz edilmiş yerlər belə qorunurlar.

İkinci sərhəd vasitəsilə xüsusi mühafizə siqnalizasiyası vasitələrinin köməyilə bina daxilindəki otaq mühafizə olunur. Üçüncü sərhəd otaq daxilindəki anbarı, vasitələri və material qiymətliləri və s.-ni mühafizə edir.

5.3.2. Postların qurulması yolu ilə mühafizə

Firma otaqlarının mərkəzləşdirilmiş mühafizə pultuna birləşdirilmiş mühafizəsi hər zaman mümkün olmur. Belə olduqda poçt mühafizəsini təşkil etmək tövsiyə olunur.

Postlar həmçinin artıq mövcud olan mühafizənin möhkəmləndirilməsi üçün də qurula bilər. Postların mövcud olması həm gecə, həm də gündüz vaxtı cinayətkar qəsdlərinin mümkünlüyünü əhəmiyyətli dərəcədə azaldır. Bu növ mühafizə cinayətkarların iş gününün bitməsindən sonra otaqda qalmağa cəhd etməsi halında xüsusilə effektivdir.

5.3.3. Kombinələşdirilmiş mühafizə

Həm texniki vasitələrindən istifadə etməklə, həm də postların qurulması vasitəsilə təşkil edilən mühafizənin güclü və zəif cəhətləri vardır. Birinci növ mühafizə post mühafizəsi ilə müqayisədə bir sıra şübhəsiz üstünlüklərə

malikdir. Bu, həm minimum sayda insanın iştirakı ilə çoxlu sayda otaqlara nəzarət edilməsi, həm də uzun müddət ərzində fasiləsiz işin aparılmasında özünü büruzə verir. Digər tərəfdən o, post mühaifzəsinə tam olaraq yalnız qeyri-iş vaxtlarında istifadə edilə uduzur. Bu iki mühafizə formasının rasional olaraq birləşdirilməsi maksimal etibarlılıqla firmanın otaqlarının, həm iş vaxtı, həm də işdən kənar vaxtlarda qorunmasına imkan verir. Kombinələşdirilmiş mühafizə o zaman xüsusilə effektiv olur ki, onun obyekti çoxmərtəbəlidir və ya çoxsaylı otaqları olan bir binadır.

5.4. Mühafizə rejimi

Effektiv mühafizə rejiminin rolu obyekt daxilindəki bina və otaqların bü-tövlüyünün, material qiymətlilərin və insanların daşınmasının, mühafizəsinin, təmin edilməsindən, obyektin fəaliyyəti haqqındakı informasiyanın sızması üzrə xəbərdar etməkdən, yanğın əleyhinə mühafizənin təmin edilməsindən ibarətdir. Mühafizə rejimi üçün mühafizə vasitələri və güclərinin keyfiyyətli seçilməsi, hazırlanması və yerləşdirilməsi, mühafizə rejimi haqqındakı informasiyanın toplanması və təhlil edilməsi, həmçinin mühafizə xidmətinin obyektdəki fəaliyyətinə nəzarət edilməsi həlledici əhəmiyyət kəsb edir. Mühafizə rejiminin əsas prinsipləri aşağıdakılardır:

- mühafizənin obyektə qarşı hazırlanan hücumun əlamətlərinin əvvəlcədən aşkar edilməsi və onun haqqında xəbərdar etmə və onun aradan qaldırılması (dəf edilməsi) üzrə vaxtında müvafiq tədbirlərin görülməsindən ibarət olan fəallığı və xəbərdaredici xarakteri;
- obyektin mühafizə rejiminin təşkil edilməsinin məqsədəuyğunluğu və

əsaslılığı, mühafizənin gücləndrilməsinin vaxtında həyata keçirilməsi, mühafizə vasitələri və güclərindən rasional istifadə edilməsi;

- obyektin təhlükəsizliyinin təmin edilməsi üçün firmanın öz imkanları ilə hüquq-mühafizə orqanlarının imkanlarının səmərəli birləşdirilməsi;
- mühafizənin vahid plan üzrə həyata keçirilməsi;
- mühafizə olunan obyekt ətrafında yaranan situasiyadan asılı olaraq mühafizənin gizli və ya nümayiş etdirilərək aparılması;
- mühafizəçilərin obyektin təhlükəsizliyinin təmin edilməsinə imkan verən əsas halqanı düzgün müəyyənləşdirmək üçün obyektdə baş verən bütün hadisələr, firmanın kommersiya müqavilələrinin şərtləri və s. haqqında maksimal dərəcədə məlumatlı olması.

5.4.1. Mühafizə rejiminin vəzifələri

Obyektin təhlükəsizliyinin təmin edilməsi üzrə mühafizə bölmələrinin fəaliyyəti təcrübəsində iki qrup məsələ fərqləndirilir:

- analitik və xəbərdarlıq məsələsi;
- prosedur-dəfetmə məsələsi.

Analitik məsələlər cinayət fəaliyyətinin subyektləri və şəxsi mühafizə rejiminin vəziyyəti haqqındakı informasiyanın sistematik toplanması yolu ilə həll edilir. Burada əsas iş informasiyanın toplanmasının fasiləsizliyi və daimiliyi prinsipinə riayət etməkdən ibarətdir.

Xəbərdarlıq məsələlərinin həlli ilk növbədə güclü və etibarlı mühafizə imicinin yaradılması ilə əlaqədardır. Belə imic cinayətkarların obyektə qarşı «uğursuz» qəsdlərini və mühafizə xidmətinin onlara qarşı güclü müqavimət göstərməsini nümayiş etdirən imitasiya tədbirləri seriyası vasitəsilə yaradıla bilər. Bütün bunlar mühafizə rejiminin təəssüratlı nümayiş elementləri (mühafizəçinin təlqinedici görünüşü, müasir mühafizə siqnalizasiyası, obyektdə polisin olması və s.) ilə tamamlana bilər. Mühafizə edilən obyektə

qarşı sui-qəsdi, həmçinin onun maskalanması, onun fəaliyyəti haqqında informasiya kanallarının bağlanılması və rəqiblərin və kriminal elementlərin onun fəaliyyət xarakteri, mülkiyyət forması, mühafizə rejiminin vəziyyəti, obyektdəki əmtəə-material qiymətlilərinin həcmi və s. haqqında yalan məlumatlar vermək yolu ilə qabaqlamaq olar.

Obyektin mühafizə rejiminin ikinci qrup məsələləri hazırlanan qəsdin vaxtında aşkar edilməsi və əvvəlcədən hazırlanmış güclər və vasitələrlə onun qarşısının alınması yolu ilə həll edilir. Bir qayda olaraq, belə tədbirləri (əməliyyatlari) cinayətkarlıq fəaliyyətinin izlərini vaxtında fiksə etmək imkanına malik ola biləcək daxili iş orqanlarının əməkdaşları ilə qarşılıqlı əlaqədə aparmaq daha məqsədəuyğundur. Qəsdin başlanma zamanını əvvəlcədən müəyyən etmək çətin olduğu hallarda cinayətkarları qəsdi başlatmağa qıcıqlandırmaq da olar. Buna kriminal elementlərə qiymətli yüklərin, böyük məbləğ pulların və s. daşınması haqqında yalan məlumat verməklə də nail olmaq olar.

Obyektin mühafizəsinin təşkili zamanı təhlükəsizlik xidməti mühafizəçi-ərin öhdəlikləri siyahısında obyektdə və ya onun yaxınlığıda böhran situasiyasının yaranması zamanı mühafizəçilərin fəaliyyət variantlarını da nəzərdə tutmalıdır. Belə hallarda mühafizəçilərin öhdəliklərinə aid olur:

- cinayətkarın saxlanılması üzrə tədbir görülməsi və saxlanılmış şəxsin daxili işlər orqanlarına ötürülməsi;

- hadisə yerinin, oradakı izlərin və əşyavü-dəlillərin polis əməkdaşları gələnə qədər mühafizəsinin təmin edilməsi;

- cinayət və ya bədbəxt hadisə nəticəsində zərər çəkənlərə tibb işçilərinin gəlməsinə qədər kömək göstərilməsi;

- hadisənin şahidlərinin, həmçinin özü üçün haqq qazandıracaq şahidlər bazasının təyin edilməsi;

- obyekt yaxınlığında ictimai asayişin pozulması faktları haqqında daxili işlər orqanlarına məlumat verilməsi.

Mühafizəçilərin fəaliyyətində əsas diqqəti mühafizə olunan obyektdə işgüzar görüşlərin təşkil edilməsi və biznes üzrə partnyorların qəbul olunmasına vermək lazımdır. Bu halda mühafizə xidməti aşağıdakıları təmin
etməlidir:

1) işgüzar qəbula gəlmiş qonaqların qarşılanması;
2) əsas mühafizə xidməti ilə dəvət olunmuş qonaqların cangüdən-lərinin qarşılıqlı fəaliyyəti;
3) qonaqların geyimlərinin, əşyalarının və onların avtomobillərinin yaxın ərazidə mühafizə edilməsi;
4) işgüzar qəbulda və ya görüşdə qonaqlar arasındakı münaqişələrin qarşısının alınması;
5) qonaqlar üçün hazırlanmış içkilərin, çərəzlərin və başqa yeməklərin vəziyyətinə nəzarət edilməsi;
6) masa arxasında digərlərinə nisbətən daha çox oturan və özlərini qeyri-adi aparan tədbir iştirakçılarının aşkara çıxarılması;
7) aşağıdakı şəxslərin nəzarətdə saxlanılması:
   - işgüzar görüşə və ya qəbula bağlamalar,çantalar, keyslər və s. ilə gələn qonaqları;
   - tədbirə audio və video cihazlar gətirən qonaqları;
   - görüş yerini tez tərk edən qonaqları;
8) qəbul zalında və ya qonşu otaqlarda qonaqlar üçün təhlükəli olan əşyaların aşkara çıxarılması;
9) otaqlarda və telefon vasitəsilə tədbirin təşkilatçılarının və qonaqların danışıqlarının dinlənilməsinə qarşı tədbirlərin aparılması.

Stasionar obyektlərin mühafizəsinin effektivliyinin vacib şərti onların texniki möhkəmləndirilməsi və onlarda təhlükəsizliyin təmin edilməsinin texniki vasitələrinin mövcud olmasıdır.

Stasionar obyektlərin texniki möhkəmlik elementləri aşağıdakılardır:

- obyekt perimetrinin mühəndis-texniki mühafizə vasitələri, buraya aiddir: qadağa olunmuş zona, oraya daxil olma üzrə nəzarət edilməsi vasitə və sistemləri, nəzarət-izləmə zolaqları və başqa sistemlər;
- mühafizə obyektlərinin işıqlandırılması;
- nəzarət-buraxılış məntəqələri;
- videomüşahidə vasitələri;
- rabitə vasitələri.

5.5. Mühafizəçilər

Müdiriyyət mühafizə heyətini nadir hallarda təhlükəsizlik xidmətinin bir hissəsi kimi nəzərdən keçirir. Mühafizəçilər təhlükəsizlik sisteminin o zaman bir hissəsi olurlar ki, rəhbərlik onun funksional elementlərinin vəzifələrini, mürəkkəbliyini və etibarlılıq səviyyəsini yaxşı başa düşür və mühafizə heyətinin bütün təhlükəsizlik kompleksinin işindəki rolunu dəqiq təsəvvür edir.

Mühafizə xidmətinin vəzifə və fəaliyyəti, hər şeydən əvvəl, bir məqsədə tabedir – mühafizə funksiyalarının yerinə yetirilməsi. Mühafizəçilər bu zaman abstrakt düşünə, improvizasiya edə bilməli, təşəbbüskar olmalı, hadisələrə ehtimallı yanaşa bilməlidirlər və s., yəni mühafizəçi özündə bir sıra keyfiyyətləri birləşdirməlidir: intellekt, sağlam fikirlilik, çevik düşünmə, fiziki qüvvə, duyma qabiliyyəti, səbr və s.

Bu keyfiyyətlər onun bütün fəaliyyət formaları zamanı təzahür etməlidir:
- daxili və xarici patrul fəaliyyəti zamanı;
- heyətin keçid və giriş hərəkətləri üzərində nəzarət zamanı;
- müşahidə prosesində;
- təhqiqat aparılması zamanı;

- heyətin və ziyarətçilərin fəaliyyətinin müşahidə edilməsi zamanı;

- məruzələrin, arayışların və başqa sənədlərin hazırlanması zamanı;

- cinayətkarların və qanun pozucularının izlənməsi və saxlanılması zamanı;

- insanların və yüklərin müşayiət edilməsi zamanı və s.

Mühafizəçilərə qadağan olunur:

- hazırlanan və ya həyata keçirilən cinayətlərin onlara məlum olan faktlarını hüquq-mühafizə orqanlarından gizlətmək;

- özünü hüquq-mühafizə orqanlarının əməkdaşı kimi qələmə vermək;

- ayrı-ayrı şəxslərin şəxsi həyatı, siyasi görüşləri və dini inancları ilə əlaqədar məlumatlar toplamaq;

- xidməti otaqlarda müvafiq səlahiyyətli şəxslərdən yazılı icazə almadan video və audio yazılar, foto və kinoçəkilişləri həyata keçirmək;

- vətəndaşların hüquq və əmlaklarına qəsdedici fəaliyyətlərə əl atmaq;

- vətəndaşların həyatını, sağlamlığını, şərəfini, ləyaqətini və əmlakını təhlükə altına qoyan fəaliyyətləri həyata keçirmək;

- öz lisenziyasını başqa şəxslərin istifadə etməsi üçün vermək.

5.6. Maliyyə vəsaitlərinin mühafizəsi

Maliyyə vəsaitlərinin təhlükəsizliyi məqsədilə onlardan istifadənin bütün mərhələlərində (bankdan alma (təhvil verilmə), nəql etmə, kassada müvəqqəti olaraq saxlanılma – vermə (təslim etmə)) vəsaitlərin mühafizəsi şərtlərini təmin

etmək lazımdır. Bu situasiyalardan hər biri xüsusi bilik və bacarıqlar, peşəkarlıq və ehtiyatlılıq tələb edir.

5.6.1. Firmada maliyyə vəsaitlərinin təhlükəsizliyinin təmin edilməsi

RF qanunvericiliyinə görə kassa əməliyyatları üzrə məsuliyyət firmanın rəhbəri üzərinə düşür. Öz fəaliyyətində o, «Müəssisənin və kassa otağının texniki möhkəmləndirilməsi və siqnalizasiya avadanlıqları ilə təchiz edilməsi üzrə vahid tələblər»ə istinad etməlidir.

Burada əsas etibarı ilə göstərilir ki, nağd pul vəsaitlərinin və qiymətlilərin etibarlı mühafizə edilməsi üçün kassa otağı aşağıdakı tələblərə cavab verməlidir.

- başqa xidməti otaqlardan izolə edilməlidir;
- ana divarlara, möhkəm döşəmə və tavana malik olmalıdır;
- pul və qiymətlilərin saxlanılması üçün məcburi qaydada möhkəm şə-kildə tikinti konstruksiyasına bərkidilmiş seyfə (metal şkafa) malik olmalıdır;
- qapılar, pəncərələr, ventilyasiya şaxtaları otağa kənardan nüfuz edilməsini istisna edən etibarlı vasitələrlə təchiz edilməlidir.

Təşkilati planda kassa otağı, bir qayda olaraq, bir neçə, minimum iki mühafizə sərhəddi, həmçinin mühafizə-yanğın siqnalizasiya vasitələrilə təchiz edilir.

5.6.2. Pul və qiymətlilərin nəql edilməsi

Maliyyə vəsaitləri xüsusilə onların daşınması zamanı təhlükəyə məruz qalırlar.

Pul vəsaitləri və qiymətlilərin daşınması xüsusi təchiz edilmiş avtomobillər vasitəsilə həyata keçirilməlidir. Pul və qiymətlilərin daşınması üçün olan avtonəqliyyat aşağıdakı tələblərə cavab verməlidir:

a) qapalı və xüsusi banlara malik olmalıdır (banın, o cümlədən döşəmə və tavanın zirehlə qorunması, pəncərələrdə daxili metal barmaqlıqlar və ya metal jalüzlər, xüsusi aynalar və s.);

b) təkmilləşdirilmiş hərəkət xarakteristikalarına malik olmalıdır;

c) sürücü kabinəsi ilə ban arasında siqnalizasiya, radio əlaqə və qarşılıqlı rabitə olmalıdır;

d) pul daşınması üçün olan ban kifayət qədər işıqlandırılmalı və istilik qurğuları ilə təchiz olunmalıdır;

e) sürücü kabinəsinin və banın qapıları xüsusi daxili kilid qurğularına malik olmalıdır.

Pul və qiymətlilərin daşınması üçün kənar nəqliyyatın icarəyə götürül-məsi qadağandır. İnkassasiya zamanı xüsusi avtomobildə kənar şəxslərin olması və ya getməsi də qadağandır. Zərər çəkənlərə yardım göstərmək zərurəti olduqda inkossatorlar radio əlaqə vasitəsilə növbətçi ilə bağlantı yaratmalı və hərəkət yolu üzərində baş verən hadisə haqqında xəbər verməlidirlər. Bu zaman inkossator avtomobilinin dayanmağa icazəsi yoxdur.

Pul məbləği olan çantaların qəbul edilməsi toplayıcı-inkossator tərəfindən, izolə edilmiş otaqda həyata keçirilməlidir. Çantanın inkossatora verilməsi prosesini nəinki kənar şəxslər, həmçinin pul əməliyyatları ilə əlaqədar olmayan firmanın öz əməkdaşları belə müşahidə etmək imkanına malik olmamalıdırlar.

İnkossator avtomobilinin inkossasiya obyektinə hərəkət yolunda, həmçinin toplayıcı-inkossatorun yolunda aşağıdakılar yolverilməzdir:

- səliqəsiz giriş yolları;
- marşruta yaxın olan kriminogen obyektlər;
- qaranlıq dəhlizlər;
- işıqlandırılmamış həyətlər;
- toplayıcı-inkossatorun inkassasiya obyekti ilə əlaqədar olamyan bitişik təşkilatların içərisindən keçməsi;
- inkossator avtomobilinin saxlanılması üçün rahat dayanacağın olmaması.

İnkassasiyanın təhlükəsizliyinin vacib qaydası firmanın nümayəndə-sinin inkossatoru onun avtomobildən çıx-

dığı zaman qarşılamağa və pul məbləği olan çantaları topladığı zaman onu avtomobilə qədər ötürməyə borclu olmasından ibarətdir. Pul və qiymətlilərlə dolu inkossatorun müşayiət edilməsi zamanı kömək yalnız hücum, yaxınlaşma və s. ehtimalına qarşı nümayəndənin (mühafizəçinin) mövcud olması ilə məhdudlaşır. Pul və qiymətlilərin olduğu çantaları təhvil aldıqdan və ya qəbul etdikdən sonra inkassator onu özü daşımalıdır.

İnkassasiya, inkassasiya edilən obyektlərə baş çəkilməsi və inkassator avtomobilinin marşrutu gizli saxlanmalıdır. Yükün və onu müşayiət edən şəxslərin təhlükəsizliyinin təmin edilməsi üçün marşrut və daşınma vaxtları dövri olaraq dəyişdirilməlidir. Əməliyyatların təşkil edilməsinin o variantı optimaldır ki, avtomobilin sürücüsü nəzərdə tutulan hərəkət marşrutu və pul qəbul edicisi haqqında yalnız yükün qəbul edilməsi və ya avtomobilin hərəkəti zamanı məlumat alsın.

Pul vəsaitlərinin inkassasiyasını, bir qayda olaraq, inkassasiya şöbəsi həyata keçirir.

5.7. İnkassasiya şöbəsi

İnkassasiya şöbəsi təhlükəsizlik xidmətinin struktur bölməsidir. İnkassasiya şöbəsinə təhlükəsizlik xidməti rəisinə və onun müavininə tabe olan şöbə müdiri rəhbərlik edir. Şöbənin tərkibinə bir neçə marşrut qrupu və daxili inkassasiya qrupu daxildir.

Hər bir marşrut qrupunun tərkibinə daxildir: baş inkossator, inkossator və sürücü. Daxili inkassasiya qrupu isə baş inkossatordan və iki inkossatordan təşkil olunmuşdur.

İnkassasiya şöbəsinin şəxsi heyəti bilavasitə şöbə müdiri və onun müavininə tabedir.

Şöbənin vəzifələri aşağıdakılardan ibarətdir:

- bilavasitə bankın pul varidatının inkassasiya edilməsi üzrə müqavilə bağladığı müəssisə və təşkilatlardan pul

məbləğlərinin toplanması, daşınması və banka təhvil verilməsi;

- bankın göstərişi ilə pul və başqa qiymətlilərin daşınması üzrə tapşırıqların yerinə yetirilməsi;

- müştərilərə əvvəlcədən onlar tərəfindən hazırlanmış tələbnamələr üzrə pul məbləğlərinin çatdırılması və onların təyin edilmiş qayda ilə müştərinin kassasına təhvil verilməsi.

İnkassasiya şöbəsinin şəxsi heyəti inkossator vəzifələrini yerinə yetirməyə yararlı olan mühafizəçilər və ya qiymətlilərin daşındığı xüsusi nəqliyyat vasitəsinin sürücüsü ilə tamamlanır.

İnkassasiya işçiləri onlar tərəfindən təyinatı üzrə çatdırılmaq üçün qəbul olunan pul və başqa qiymətlilərin mühafizə olunması üzrə maddi məsuliyyət daşıyırlar. Qiymətlilərin itirilməsi və ya oğurlanması halında vurulmuş zərərin ödənilməsi üzrə maddi məsuliyyət qiymətlilərin çatdırılması üzrə məsul olan birgə olaraq bütün briqada üzvləri üzərinə düşür. Briqada üzvləri ilə kollektiv (briqada) maddi məsuliyyət haqqında müqavilə bağlanılır.

5.7.1. İnkassasiya şöbəsinin rəisi

İnkassasiya şöbəsinin rəisi inkassasiya şöbəsinin işi üzərində rəhbərliyi həyata keçirir və göstərilən şöbənin bütün şəxsi heyətinin birbaşa rəisi hesab olunur.

O bilavasitə təhlükəsizlik xidmətinin rəisinə və onun müavininə tabedir.

İnkassasiya şöbəsinin müdiri aşağıdakılara görə cavabdehdir:

- razılaşmalara uyğun olaraq müntəzəm inkassasiyanın və pul daşımalarının və rəhbərliyin pul və qiymətlilərin daşınması üzrə göstərişlərinin dəqiq yerinə yetirilməsinin təmin edilməsi;

- inkassatorların müəssisə və təşkilatlara girməsi marşrut və qrafiklərinin işlənib hazırlanması, müəssisə və təşkilatların məxfi görüş kartlarının tərtib edilməsi;

- pul varidatının inkassasiya edilməsi və pul və qiymətlilərin daşınması üçün inkassator briqadalarının formalaşdırılması;

- inkasstorların qiymətlilərlə iş qaydalarına riayət etmələri üzrə dövri olaraq yoxlamaların həyata keçirilməsi;

- şöbənin şəxsi heyətinin istifadəsində olan xüsusi vasitələrin, silahların və döyüş sursatların mühafizəsinin təmin edilməsi;

- inkassator heyətinin peşəkar hazırlığının keyfiyyəti.

O borcludur:

- öz fəaliyyətində Rusiya Federasiyasının «Rusiya Federasiyasında xüsusi xəfiyyə və mühafizə fəaliyyəti haqqında» qanununa və başqa qanun və normativ aktlara istinad etməyə, kassa işi, kassa xidməti və inkassasiya işi üzrə qanunvericiliyi, nizamnaməni, normativ sənədləri, silah və xüsusi vasitələrin saxlanılması və istifadə edilməsi qaydalarını, həmçinin təhlükəsizlik xidməti üzrə əsasnamənin tələblərini bilmək;

- inkassasiya işçilərinin pul məbləğlərinin və başqa qiymətlilərin toplanması və daşınması qaydalarını yerinə yetirmələrinə sistematik olaraq nəzarət edilməsi;

- mülkiyyətçinin əmanət edilmiş əmlakının təhlükəsizliyinin təmin edilməsi üzrə təxirəsalınmaz tədbirləri həyata keçirməyə, ona, vətəndaşların təhlükəsizlik xidmətinin şəxsi heyətinin həyat və sağlamlıqlarına qarşı qanunsuz qəsdlərin dəf edilməsini təşkil etməyə, bütün belə qəsdlər haqqında dərhal öz birbaşa rəisinə məlumat verməyə;

- şöbənin şəxsi heyətinin odlu silahdan bütün istifadə halları haqqında dərhal təhlükəsizlik xidməti rəisini xəbərdar etməyə;

- şöbədə lazımi maddi təminatı və qiymətlilərin daşınması və qorunması üçün texniki vasitələrin işini düzgün təşkil etməyə;

- şöbənin şəxsi heyətinin hazırlanması və yenidən hazırlanmasına (ixtisasının artırılmasına) rəhbərlik etməyə;

- Rusiya Federasiyası Daxili İşlər Nazirliyi tərəfindən müəyyən olunmuş qaydada inkossator heyətinin dövri olaraq onların xüsusi vasitə və odlu silahdan istifadə etmələri ilə əlaqədar yoxlanılmasının həyata keçirilməsinə;

- Müəssisənin kadr və maliyyə orqanları ilə şöbə işçiləri üçün əmək haqlarının, dövlət sosial sığortası üzrə müavinətlərin və mühafizə fəaliyyətinin həyata keçirilməsi ilə əlaqədar həlak və ya şikəst olma və ya başqa xəsarət olma ehtimalı üzrə sığortanın hesablanması məsələsi üzrə qarşılıqlı fəaliyyətin həyata keçirilməsinə;

- Lisenziyaların şöbə əməkdaşları və şəxsən özü üçün fəaliyyət müddətinə nəzarət edilməsi, müddətin uzadılması üzrə vaxtında tədbirlər görülməsi;

- Silahların, döyüş sursatlarının və xüsusi vasitələrin uçotunun aparılması və təhlükəsizliyinin təmin edilməsinə;

- Odlu silahların, onun üçün döyüş sursatlarının və xüsusi vasitələrin uçotu, saxlanılması, gəzdirilməsi və daşınması qaydası üzərində nəzarətin təşkil edilməsinə;

- Təhlükəsizlik xidməti rəisinin göstərişi ilə xüsusi vasitlərin, odlu silahların və döyüş sursatlarının hər bir çatşmama, xarab olma və artıq olması halı üzrə təhqiqatın aparılmasına;

- Bankın təhlükəsizlik xidməti rəhbərliyi üçün şöbənin işinin təkmilləşdirilməsi və effektivliyinin artırılması üzrə təklifin işlənib hazırlanması və təqdim edilməsinə;

- Bölmənin normativ sənədlər üzrə nəzərdə tutulan sənədləşməsinin aparılması və təyin edilmiş hesabdarlığın tərtib edilməsinə.

5.7.2. İnkossator

İnkossator – təşkilatdan banka təslim etmək üçün pulun qəbulunu həyata keçirən vəzifəli şəxsdir.

O aşağıdakıları təmin edir:

- ticarət aparan təşkilatların pullarının bank idarəsinə çatdırılması;

- pul vəsaitlərinin kommersiya strukturunun ticarət məntəqəsindən sonradan banka təslim etmək üçün onun ofisinə çatdırılması;

- pulların sonradan əməkdaşların əmək haqlarının verilməsi üçün bankdan firma ofisinə çatdırılması;

- pul vəsaitlərinin bankdan alınması ilə bank krediti götürüldüyü əmtəənin istehlak yerinə daşınması və valyuta-maliyyə dövriyyəsinin başqa fəaliyyətləri.

Öz funksional öhdəliklərini yerinə yetirərkən inkossatora aşağıdakılar qadağan olunur:

- inkassasiya və qiymətlilərin daşınması ilə əlaqədar olmayan fəaliyyətləri həyata keçirmək;

- avtomaşının dayanması zamanı kənar şəxslərlə söhbət etmək və ya avtomobildən uzaqlaşmaq;

- radiostansiya vasitəsilə açıq ötürülə bilən məlumatlardan fərqli məlumatların ötürülməsi;

- xidmət göstərilən təşkilatlarda əmtəə və xidmətlər əldə etmək və həmçinin başqa xidmətlərdən istifadə etmək;

- əmanət edilmiş qiymətliləri nəzarətsiz buraxmaq;

- kənar şəxslərin xüsusi avtomobildə olması və getməsinə yol vermək;

- inkassasiya və qiymətlilərin daşınması qaydaları ilə uyğun gəlməyən
göstərişlərin yerinə yetirilməsi.

Pul və qiymətliləri daşıyan mühafizəçilərin silah tətbiq edə biləcəkləri situasiya yarandıqda onlar «Xüsusi xəfiyyə və mühafizə fəaliyyəti haqqındakı qanunun» 16 və 18-ci maddələrində qeyd edilmiş qayda və tələblərindən istifadə etməlidirlər. Bununla belə, peşəkar inkossatorlar tərəfindən odlu silahdan istifadə edilməsini reqlamentləşdirən qaydaların nəzərinizə çatdırılması da maraqsız olmazdı.

Tabel silahı inkossatorlar tərəfindən aşağıdakı məqsədlər üzrə istifadə edilə bilər:

- inkassasiya edilən və ya daşınan pul vəsaitləri və qiymətlilərin qorunması üçün;
- inkossatorun həyatı təhlükə altında olduqda cinayətkarların hücumunun dəf edilməsi üçün;
- inkassasiya işçilərinə və ya onlar tərəfindən qorunan qiymətlilər və obyektlərə hücum etmiş cinayətkarların saxlanılması üçün;

Silahın tətbiqindən sonra:

- bu fakt haqqında inkassasiya üzrə növbətçiyə və daxili işlər orqanlarının ərazi növbətçisinə məlumat verilir;
- hadisə yerinə bank işçilərinin və polisin gəlməsinə qədər inkossatorlar orada qalır və qiymətlilərin təhlükəsizliyini təmin edirlər.

İnkassasiya xidməti əməkdaşlarına aşağıdakı hallarda odlu silahdan istifadə etmək qadağan olunur:

- atəş zamanı kənar şəxslərin xəsarət ala biləcəyi çoxadamlı küçələrdə, meydanlarda və başqa ictimai yerlərdə;
- qadınlar və yetkinlik yaşına çatmayanlara qarşı, onlar tərəfindən silahlı hücumun təşkil edilməsi halı istisna olmaqla;
- yanlarında uşaqları olan vətəndaşlara qarşı.

5.8. Heyətin təhlükəsizliyinin təmin edilməsi

Heyətin, o cümlədən firmanın yuxarı vəzifəli şəxslərinin şəxsi təhlükə-
sizliyi aşağıdakılardan ibarətdir:

- mühafizəçi-cangüdənlərdən ibarət mühafizə xidməti;
- şəxsin fərdi təhlükəsizliyindən, o cümlədən cinayət fəaliyyətlərinin dəf edilməsinə fiziki hazırlıq, böhran situasiyalarına reaksiya verilməsinə üzrə psixoloji hazırlıq;

- şəxsi məqsədlər üçün istifadə edilməyə icazə verilən şəxsi təhlükəsizlik vasitələrindən istifadə edilməsi.

Şəxsi təhlükəsizliyi böhran situasiyalarında özünü idarə edə bilmək qabiliyyəti və yüksək mənəvi keyfiyyətlə yanaşı istənilən şəraitdə tez və qəti şəkildə hərəkət edə bilən şəxsi mühafizəçilər təmin edə bilər. Onlar fiziki cəhətdən yaxşı inkişaf etməli, mühafizə edilən şəxs və onun ailə üzvləri ilə psixoloji cəhətdən uzlaşmalı və bu işə peşəkarcasına hazırlanmalıdır.

Bəs bu və ya digər iş üzrə şahid kimi çıxış edən şəxsiyyət necə müdafiə olunur? Rus qəzetlərindən birində bu suala aşağıdakı kimi cavab verilmişdir.

«Şahid müdafiə olunacaqdır!»

Qərbin mafiya haqqında filmlərində çox vaxt polis agentlərini şahidləri məhkəmənin sonuna qədər gecə və gündüz necə qoruduqları göstərilir. Bizdə şahidlərin bu cür qorunması təcrübəsi mövcuddurmu?

«O. MORQULİS

CAVAB*: Əlbəttə ki, mövcuddur. Bir müddət öncə «mütəşşəkil cinayətkar qrupları tərəfindən təşkil edilmiş cinayətlərin açılmasına yardım edən vətəndaşların sosial müdafiəsi və maddi stimullaşdırılması tədbirləri haqqında» əsasnamə təsdiq olunmuşdur (№ 791-RP).*

Şahidlərin, zərərçəkənlərin, onların qohumlarının və yaxınlarının həyat və sağlamlıqlarının onların istəklərinin və konkret situasiyaların nəzərə alınması ilə müdafiəsi üçün aşağıdakı təhlükəsizlik tədbirləri tətbiq edilə bilər:

- şəxsi mühafizə, yaşayış yerinin və əmlakın mühafizəsi;

- qanunvericiliklə təyin olunmuş qaydada silahların, xüsusi vasitələrin və fərdi mühafizə vasitələrinin verilməsi;

- müvəqqəti (bir aydan bir ilə qədər) təhlükəsiz yerdə yerləşdirmə;

- informasiya sistemlərində qorunan şəxslər haqqındakı məlumatların məxfiliyinin təmin edilməsi;

- başqa işə (xidmətə) keçirilmə, iş və ya təhsil yerinin dəyişdirilməsi;

- başqa yaşayış yerinin təqdim edilməsi;

- sənədlərin təyin edilmiş qaydada əvəz edilməsi, xarici görünüşün dəyişdirilməsi.

Təhlükəsizliyin və mühafizənin təmin edilməsi Moskva ş. DDİİ xüsusi bölməsi üzərinə düşür».

Sosial müdafiənin tədbirlərinə vətəndaşların həyatına, sağlamlığına və əmlakına vurulmuş zərərin, həmçinin müdafiə tədbirlərinin tətbiqi üzündən onların itirilməsi (əmək haqqında, iş stajında və s.-də itkilər) halında onların maddi kompensasiyası və həlak olma zamanı onların qohumlarına maddi yardım göstərilməsi daxildir.

Şəxsə qarşı təhlükələrin ən geniş yayılmış forması bu və ya başqa tələblərlə anonim zənglərdir.

Terroristlərin motivləri, sadə təhdid və zorakılıqdan tutmuş, öldürməklə hədələməyə qədər müxtəlif ola bilər. Belə hərəkətlər təkcə bir şəxsi yox, onun ailəsini və firmanı qorxu altında saxlayır. Təbii ki, hər bir belə zəng ter-rora qarşı əks təsir göstərilməsi cəhətdən nəzərə alınmalıdır: bu ya maqni-tafon yazısı, ya da telefonla təhdid edən şəxsin xarakterik xüsusiyyətlərinin formalizə edilmiş kartının doldurulması yolu ilə həyata keçirilir.

Belə materialların mövcud olması təhlükəsizlik xidmətinə operativ-axtarış və müdafiə tədbirlərini aparmağa imkan verir.

Telefonla hədə-qorxu gələn şəxsin xarakterik xüsusiyyətləri xəritəsi

Cins	Qiy	Yaşı	Qiy	Səsi	Qiy	Danışığı	Qiy
Kişi		Böyük		Gur (zil)		Sürətli	
Qadın		Yeniyetmə		Kobud		Yavaş	
Ünsiyyət forması	Qiy	Uşaq		Yumşaq		Aydın	
Sadə		Xüsusiyyətləri		Kəskin (sərt)		Anlaşılmaz	
Kobud				Burnunda danışan		Pəltək	
Mülayim				Xırıltılı (batıq)		Xüsusiyyətləri	
Nəzakətli				Xüsusiyyətləri			
Xüsusiyyətləri							
Tələffüz	Qiy	Dili	Qiy	Danışıq tərzi	Qiy	Fon	Qiy
Aydın		Adi		Sakit		Yoxdur	
Yaxşı		Alicənab		İsteriyalı		Danışıq	

Anlaşılma z		Ədəbsiz		Dolaşıq		Musiqi	
Pis		Naşı		Əsəbi		Səs-küy	
Xüsusiyyətləri		Xüsusiyyətləri		Xüsusiyyətləri		Xüsusiyyətləri	
Söhbətin tərkibi				Əlavə məlumatlar			

Tarix_________Vaxt__________tərtibatçının S.A.A.

Görülən tədbirlər:

FƏSİL VI

KADRLAR ŞÖBƏSİ

Çoxdan məlum olan «kadrlar hər şeyi həll edirlər» aforizmi bu gün də öz əhəmiyyətini itirməmişdir, ona görə yox ki, yaxşı mütəxəssislər olmadan sağ qalmaq olmaz, həm də ona görə ki, hazırki dövrdə əməkdaşların etibarlılığı çox da yüksək səviyyədə deyildr. Statistika göstərir ki, firma məsrəflərin 80%-ni öz əməkdaşlarının bu və ya digər cinayətkar fəaliyyətdə birbaşa iştirakına görə çəkir.

Mütəxəssislər heyətin etibarlığını bir neçə kriteriyasına görə fərqləndirirlər və ideal halda kommersiya müəssisəsinin əməkdaşı onlardan hər birinə uyğun gəlməlidir. Bu kriteriyalara aiddir:

- peşəkar etibarlılıq;
- psixoloji etibarlılıq;
- mənəvi etibarlılıq.

Firmanın təhlükəsizliyinə qarşı öz şəxsi heyəti tərəfindən təhlükələrin konkret hallarının təhlili göstərir ki, çox vaxt onlar aşağıdakı səbəblər üzündən ortaya çıxır:

- aşağı ixtisaslılıq;
- işdən mənəvi cəhətdən məmnun olmama;
- zərərli vərdişlər və b.

Ümumiyyətlə, əməyin motivasiyası və firmaya sədaqət hər zaman bir-birilə dolaşmış çoxsaylı motivlərlə şərtlənir. Biriləri

üçün yüksək məvacib, digəri üçün karyera, üçüncüləri üçün sosial müdafiə, dördüncülər üçün prestij və ya yaradıcı işlə məşğul olmaq imkanı vacibdir. İncik düşmüş əməkdaş – tez və ya gec işə düşəcək gec açılan bombadır.

Firmanı öz şəxsi əməkdaşlarından qorumağa imkan verən universal resept, yüz faizlik təhlükəsizliyin təmin edilməsi vasitələrinin olmadığı kimi, hələ ki, yoxdur. Ancaq bu təhlükəsizliyin maksimal dərəcədə aşağı salmaq, onu nəzarətdə saxlamaq və arzuolunmaz nəticələrdən qaçmaq imkanı vardır. Bu – dərk edilmiş, mütəşəkkil, ardıcıl və məqsəd yönümlü kadr siyasətidir. O, firmanın normal fəaliyyəti üçün biznes-planın yaratdığı qədər vacib şərait yaradır. Bu siyasət üç əsas prinsipə əsaslanır:

- heyətin müasir metodların köməyilə ağıllı şəkildə seçilməsi;
- düşünülmüş və savadlı şəkildə qurulmuş mükafatlandırma və vəzifə artımı sistemi;
- firmada heyətin birgə işi üçün xoş qarşılıqlı münasibətləri dəstəkləyən təşkilati mədəniyyət.

Bütün bunlar təhlükəsizliyin başlıca şərtlərindən biri olan kadr siyasətinin mahiyyətini təşkil edir.

6.1. Məxfi informasiya ilə işləməyə buraxılmış əməkdaşlarla işin xüsusiyyətləri

Kommersiya müəssisəsinin kadr xidməti vətəndaşın, onu müvafiq vəzifəyə təyin edərkən özü haqqında verdiyi məlumatların həqiqiliyinin yoxlanılmasını təşkil edir.

Yoxlamanın aparılması üçün əsas kimi aşağıdakılar çıxış edə bilər:

- hüquq-mühafizə orqanlarından, dövlət vergi xidməti orqanlarından, məhkəmə orqanlarından, şəxsin əvvəlki işlədiyi müəssisə və təşkilatlardan əldə edilmiş informasiya;
- hüquq-mühafizə orqanlarından əldə edilmiş məlumatların etibarsızlığı və natamamlığı.

Namizəd haqqındakı məlumatların yoxlanılması bir ay müddətində aparılır. Bu müddət namizəd üçün sınaq müddətinin təyin edilməsi şərti ilə uzadıla bilər.

Yoxlama məqsədilə hüquq-mühafizə və idarəetmə orqanlarına, müəssisə və təsisatlara tələbin təmin edilməsi müddətinin göstərilməsi ilə müvafiq tələbnamələr göndərilə bilər.

Yoxlanış sənədləri məxfi informasiyaya aiddir və namizədin şəxsi işinə əlavə edilir.

Yoxlanılan şəxsin yoxlanış sənədləri ilə tanış olmağa və yazılı izahat verməyə hüququ vardır. Göstərilən izahatlar yoxlanış sənədlərinə əlavə edilir.

Yoxlamanın gedişi zamanı məlum olsa ki, yoxlanılan şəxs özü haqqında natamam və ya düzgün olmayan məlumatlar, yaxud qəsdən yalan məlumatlar vermişdir, müdiriyyət həmin şəxsi işə götürməkdən imtina etmək hüququna malikdir.

Yeni əməkdaşların işə götürülməsi zamanı müəssisələrin, təşkilatların və firmaların əksəriyyəti müəyyən risklə qarşılaşır. Müsahibələrin və yoxlamaların müxtəlif formalarına baxmayaraq, firmanın əməkdaşları heç də həmişə öz təşkilatlarına münasibətdə sadiq olmurlar. Statistika göstərir ki, istənilən firmanın heyəti istənilən şəraitdə dəyişməz qalan 25% düzgün insanlardan ibarətdir, daha 25%-i firmanın maraqları hesabına varlanmaq üçün əlverişli məqam gözləyən insanlardır. Yerdə qalan 50% insanlar isə, bu və ya digər şəraitdən asılı olaraq, həm düzgün, həm də firma maraqları hesabına varlanmaq istəyən insanlar ola bilər.

Dünya təcrübəsinin göstərdiyi kimi, kadr təhlükəsizliyinin təmin edilməsi məsələsi poliqrafda (yalan detektorunda) psixofizioloji testləşdirmənin köməyilə həll edilə bilər. Bu metod ənənəvi müsahibə və yoxlamalarla münasibətdə bir sıra üstünlüklərə malikdir.

Xarici mütəxəssislərin qiymətləndirməsinə görə, poliqrafdan istifadə etməklə özəl firmalarda məsuliyyətli işlərə əməkdaşların götürülməsi zamanı aydın olmuşdur ki,

namizədlərin üçdə-biri öz keçmişləri haqqında hər hansı məlumatları və ya şəxsi mənfi cəhətlərini gizlədirlər. Psixofizioloji testləşdirmə metodunun köməyilə əldə edilmiş məlumatlar başqa metodlardan istifadə etməklə, hətta onlardan kompleks istifadə edilsə belə, əldə edilə bilməz.

Psixofizioloji testləşdirmə metodu alınan nəticələrin yüksək etibarlılığını və həqiqiliyini təmin edir. Qeyd etmək kifayətdir ki, təcrübəli mütəxəssis tərəfindən əldə edilən məlumatların həqiqiliyi 90%-i keçir.

6.2. Məxfi informasiya ilə işləməyə buraxılmış şəxslərin şəxsi işlərinin aparılması qaydası

Məxfi informasiya ilə işləməyə icazə verilmiş əməkdaşlarla iş üzrə müfəttiş qismində kadr xidməti həmin əməkdaşların şəxsi işini aparır. Bu işlər təhlükəsizlik rejiminə riayət edilməsilə məxfi informasiya kateqoriyasına aiddir.

Şəxsi işə məxfi informasiya rejimi ilə əlaqədar vəzifədə işləməyə razılıq haqqında ərizə, müəssisə tərəfindən məxfi informasiyalara aid edilən məlumatları yaymamaq haqqında könüllü razılıq (iltizamnamə), kadrların uçotu üzrə şəxsi vərəqə də əlavə edilir.

Kadr xidməti məxfilik rejiminin saxlanılması üzrə tələb və vəziyyətlərin bütün pozulma şəraitləri və halları haqqındakı məlumatları, əməkdaşın verilmiş faktla bağlı izahatlarını və rəhbərlik tərəfindən qəbul olunmuş inzibati tədbirlər haqqındakı informasiyanı dosyeyə[3] daxil edir.

RUSİYA FEDERASİYASININ ƏMƏK KODEKSİ (MƏCƏLLƏSİ)

(çıxarış)

---

[3] dosye – bir iş və ya məsələ ilə bağlı bütün sənəd və materiallar

FƏSİL XIV. İŞÇİNİN ŞƏXSİ MƏLUMATLARININ QORUNMASI

Maddə 85. İşçinin şəxsi məlumatları haqqında.

İşçinin şəxsi məlumatlarının işlənməsi

İşçi haqqında şəxsi məlumatlar – əmək münasibətləri və konkret işçi ilə əlaqədar olan iş verən üçün zəruri olan informasiya.

İşçi haqqında şəxsi məlumatların işlənməsi – işçi haqqındakı şəxsi məlumatların əldə edilməsi, saxlanılması, kombinələşdirilməsi, ötürülməsi və istənilən başqa formada istehsal edilməsidir.

Maddə 86. İşçi haqqında şəxsi məlumatların işlənməsi və onların müdafiəsi üzrə zəmanətin ümumi tələbləri.

İnsan və vətəndaşların hüquq və azadlıqlarını təmin etmək məqsədilə iş verən və onun nümayəndələri işçilər haqqındakı şəxsi məlumatların işlənməsi zamanı aşağıdakı ümumi tələblərə riayət etməlidirlər:

1) işçilər haqqınakı şəxsi məlumatların işlənməsi müstəsna olaraq qanunlara və başqa normativ aktlara riayət edilməsi, işçilərin işə düzəlməsinə köməklik göstərilməsi, işçilərin öyrədilməsi və vəzifəsinin artırılması, şəxsi təhlükəsizliyinin təmin edilməsi, işlərin yerinə yetirilməsinin keyfiyyət və kəmiyyəti üzərində nəzarət edilməsi və əmlakın təhlükəsizliyinin təmin edilməsi məqsədilə həyata keçirilə bilər;

2) işçi haqqında işlənilən şəxsi məlumatların həcm və tərkibinin müəyyən edilməsi zamanı iş verən Rusiya Federasiyasının Konstitutsiyasına, mövcud Kodeksə və başqa federal qanunlara istinad etməlidir;

3) işçi haqqındakı şəxsi məlumatları onun özündən almaq lazımdır. Əgər işçi haqqında şəxsi məlumatları yalnız üçüncü şəxs tərəfindən almaq mümkündürsə, onda işçi bu haqda əvvəlcədən xəbərdar edilməli və ondan yazılı razılıq alınmalıdır. İş verən işçiyə şəxsi məlumatların əldə edilməsi məqsədləri, nəzərdə tutulan mənbələri və üsulları haqqında,

həmçinin əldə edilməli olan şəxsi məlumatların xarakteri və işçinin həmin məlumatlara yazılı şəkildə razılıq verməməsinin nəticələri haqqında məlumat verməlidir;

4) iş verən işçinin siyasi, dini və başqa görüşləri və şəxsi həyatı haqqındakı məlumatları əldə etmək və işləmək hüququna malik deyildir. İşçinin şəxsi həyatı haqqında birbaşa əmək məsələləri ilə əlaqədar olan məlumatların əldə edilməsi zərurəti yarandıqda Rusiya Federasiyasının 24-cü maddəsinə görə iş verən həmin məlumatların əldə edilməsi və işlənməsi üçün işçinin yazılı razılığını almalıdır;

5) iş verən işçinin ictimai birliklərdəki üzvlükləri və ya onun həmkarlardakı fəaliyyəti haqqındakı şəxsi məlumatları, federal qanunla nəzərdə tutulmuş
hallar istisna olmala, əldə etməyə və işləməyə hüququ yoxdur;

6) iş verən işçinin maraqları ilə əlaqədar qərar qəbul edərkən haqqındakı şəxsi məlumatların müstəsna olaraq avtomatlaşdırılmış işlənməsi və ya elektron yolla alınmış məlumatlara əsaslana bilməz;

7) işçi haqqındakı şəxsi məlumatların onların qanunsuz istifadə edilməsi və ya itirilmədən qorunması iş verən tərəfindən onun vasitələrindən federal qanunlarla təyin edilmiş qaydada istifadə edilməsi vasitəsilə təmin edilməlidir;

8) işçilər və onların nümayəndələri işçilər haqqındakı şəxsi məlumatların işlənməsi qaydasını təyin edən sənədlərlə, həmçinin onların bu sahədəki hüquq və öhdəlikləri üzrə iltizamnamə ilə tanış edilməlidirlər;

9) işçilər sirlərin saxlanılması və qorunması üzrə öz hüquqlarından imtina etməməlidirlər;

10) iş verənlər, işçilər və onların nümayəndələri işçilər haqqında şəxsi məlumatların qorunması tədbirlərini müştərək olaraq işləyib hazırlamalıdırlar.

Maddə 87. İşçilər haqqında şəxsi məlumatların saxlanılması və istifadə edilməsi

Təşkilatda işçilər haqqındakı şəxsi məlumatların saxlanılması və istifadə edilməsi qaydası iş verən tərəfindən mövcud Kodeksin tələblərinin nəzərə alınması ilə təyin edilir.

Maddə 88. İşçi haqqında şəxsi məlumatların ötürülməsi

İşçi haqqında şəxsi məlumatların ötürülməsi zamanı iş verən aşağıdakı tələblərə riayət etməlidir:

İşçi haqqında şəxsi məlumatların işçinin yazılı razılığı olmadan üçüncü tərəfə verilməməsi, bu işçinin həyat və sağlamlığına qarşı təhlükələrin qarşısının alınması məqsədilə zəruri olduğu hallar, həmçinin federal qanunla təyin edilmiş hallar istisna olmaqla;

İşçi haqqında şəxsi məlumatların kommersiya məqsədlərilə onun yazılı razılığı olmadan başqasına verilməməsi;

İşçi haqqında şəxsi məlumatları əldə edən şəxsləri bu məlumatlardan yalnız onların verildikləri məqsəd üzrə istifadə oluna bilməsi haqqında xəbərdar etməli və həmin şəxslərdən bu qaydalara riayət etmələrinin təsdiqlənməsini tələb etməlidirlər. İşçi haqqında şəxsi məlumatları əldə edən şəxslər məxfilik rejiminə riayət etməlidirlər. Bu hal işçilər haqqında şəxsi məlumatların federal qanunla nəzərdə tutulmuş qaydada mübadilə edilməsinə aid deyildir;

İşçi haqqında şəxsi məlumatların ötürülməsini yerli normativ akta müvafiq olaraq işçinin iltizam altında tanış edilməli olduğu bir təşkilat daxilində həyata keçirilməlidir;

İşçi haqqında şəxsi məlumatlarından yalnız səlahiyyətli şəxslərin istifadə etməsinə icazə vermək, bu zaman göstərilmiş şəxslər yalnız konkret funksiyaların yerinə yetirilməsi üçün zəruri olan şəxsi məlumatları əldə etməyə səlahiyyətlidirlər;

İşçinin sağlamlığı haqqında məlumatları tələb etməmək, işçinin əmək funksiyalarını yerinə yetirmək imkanlarına malik olma halına aid olan məsələlər istisna olmaqla;

İşçi haqqında şəxsi məlumatların işçilərin nümayəndəlrini mövcud Kodekslə müəyyən edilmiş qaydada ötürülməsi və bu

informasiyanı yalnız işçi haqqında onların nümayəndələr tərəfindən göstərilmiş funksiyalarının yerinə yetirilməsi üçün zəruri ola şəxsi məlumatlarla məhdudlaşdırmaq.

Maddə 89. İşçilərin iş verənin sərəncamında olan şəxsi məlumatların qorunmasının təmin edilməsi məqsədilə hüquqları.

İş verənin sərəncamında olan şəxsi məlumatların qorunması məqsədilə işçilər aşağıdakı hüquqlara malikdirlər:

– onların şəxsi məlumatları və həmin məlumatların işlənməsi haqqında tam informasiya almaq;

– öz şəxsi məlumatlarına azad, pulsuz giriş, o cümlədən özünə işçi haqqında şəxsi məlumatı daxil edən istənilən yazının surətini almaq hüququ, federal qanunla nəzərdə tutulmuş hallar istisna olmaqla;

– öz şəxsi məlumatlarının qoruması üçün öz nümayəndələrini müəyyən etmək;

– işçilərlə əlaqədar tibbi məlumatlara tibbi məlumatların toplanması üzrə mütəxəssisin köməyilə giriş əldə etmək;

– yanlış və ya natamam məlumatların, həmçinin mövcud Kodeksin tələblərinin pozulması ilə işlənmiş məlumatların ləğv edilməsi və ya düzəldilməsi üzrə tələb irəli sürmək. İş verənin işçi haqqında şəxsi məlumatların ləğv edilməsi və ya düzəldilməsindən imtina etməsi zamanı işçi iş verənə yazılı formada narazılığının müvafiq əsaslandırılması ilə ərizə vermək hüququna malikdir. İşçi qiymətləndirmə xarakterli şəxsi məlumatları öz nöqteyi-nəzərini ifadə edən ərizə ilə tamamlamaq hüququna da malikdir.

İş verən tərəfindən əvvəllər işçinin şəxsi məlumatlar haqqında yanlış və ya natamam məlumatlar verilmiş bütün şəxsləri həmin məlumatlarda aparılmış bütün ləğvetmə, düzəlişlər və əlavələr haqqında məlumat-landırılmasını tələb etmək;

İşçinin şəxsi məlumatlarının qorunması zamanı iş verənin istənilən qanunsuz fəaliyyəti və ya fəaliyyətsizliyi haqqında məhkəməyə müraciət etmək.

Maddə 90. İşçi haqqında şəxsi məlumatların işlənməsi və qorunmasını tənzimləyən normaların pozulması üzrə məsuliyyət.

İşçi haqqındakı şəxsi məlumatların əldə edilməsi, işlənməsi və qorunmasını tənzimləyən normaların pozulmasında təqsirli şəxslər federal qanunlara müvafiq olaraq inzibati, vətəndaş-hüquqi və ya cinayət məsuliyyəti daşıyırlar.

FƏSİL VII

XÜSUSİ ŞÖBƏ. KOMMERSİYA SİRRİNİN TƏHLÜKƏSİZLİYİNİN TƏMİN EDİLMƏSİ

Konfidensial informasiya – Rusiya Federasiyasının qanunvericiliyinə əsasən daxil olunması məhdudlaşdırılan sə-

nədləşdirilmiş informasiyadır. Müdafiənin təmin edilməsi dərəcəsinə görə informasiya aşağıdakı parametrə görə klassifikasiya edilir: açıq informasiya və yaxud ümumi istifadə üçün informasiya və məhdud istifadə üçün informasiya (qorunan informasiya) öz növbəsində qorunan informasiya konfidensial informasiyaya və dövlət sirrinə aid edilən informasiyaya bölünür («Dövlət sirri haqqında» RF Qanunu. Konfidensial xarakterli məlumatlar 188 nömrəli 6 mart 1997-ci il RF Prezidentinin qərarı ilə təsdiqlənib və konfidensial xarakterli məlumatların siyahısı şəklindədir. Siyahının məzmunu struktur olaraq cədvəl 12-də göstərilib.

Hər müəssisədə, hər firmada konfidensial informasiya aşağıdakılardır:

1. Personal insanlar
2. Sənədlər
3. Nəşrlər
4. İnformasiyanın texniki daşıyıcıları
5. İstehsal və əmək fəaliyyətini təşkil etmənin texniki vasitələri
6. Məhsul
7. Sənaye və istehsalat tullantıları

Təhlükəsizlik xidməti dəqiq bilməlidir ki, kimdə (hansı mənbədə) və harada (hansı bölmədə və nə cür şəkildə) konfidensial informasiya var, kim qorunan məlumatları ələ keçirməyə kömək edir.

Ümumi fikrə görə konfidensial informasiyanı hüquqdan kənar əldə keçirməyə aşağıdakılar imkan yaradır:

- konfidensial informasiyanın ona sahib olan tərəfdən açılması (mənbə tərəfdən);
- texniki kanallarla konfidensial informasiyanın sızması;
- konfidensial informasiyaya pisniyyətli adamlar və digər elementlər tərəfindən sanksiyasız müdaxilə.

Cədvəl 12

Konfidensial informasiya (Rusiya Federasiyasının qanunvericiliyinə uyğun girişin məhdudlaşdırılan sənədləşdirilmiş informasiya)

Şəxsi	Vətəndaşın şəxsiyyətini müəyyənləşdirməyə imkan verən personal məlumatlar. Müəyyən edilmiş qaydada kütləvi informasiya vasitələrində yayıla bilən məlumatlar istisna olmaqla onun şəxsi həyatının faktları, hadisələri və vəziyyətlər haqqında məlumatlar
Məhkəmə-istintaq	İstintaq və məhkəmə araşdırması sirri olan məlumatlar
Xidmət	Dövlət hakimiyyəti orqanları ilə girişin məhdudlaşdırılmış xidməti məlumatlar
Peşəkar	Qanunla müdaxiləsi məhdudlaşdırılmış peşəkar fəaliyyətlə əlaqədar məlumatlar (həkim, notarial, vəkil sirri, məktublaşma sirri, telefon danışıqları, poçt göndərmələrinin, teleqraf və başqa məlumatların sirri)
Kommersiya	İstifadəsi qanunla məhdudlaşdırılan kommersiya fəaliyyəti ilə əlaqədar məlumatlar (Kommersiya sirri)
İstehsalat	Sənaye nümunəli faydalı modelin ixtirasının məzmunu haqqında rəsmi nəşrdəki informasiyaya qədər olan məlumat

7.1. Kommersiya sirri

İnformasiya xidməti, yaxud kommersiya sirri o vaxt olur ki, üçüncü şəxslərə naməlumluğu səbəbindən o həqiqi, yaxud potensial kommersiya dəyərinə malik olur, qanuni yolla onu əldə etmək mümkün deyil və informasiya sahibi onun konfidensiallığının qorunması üçün ölçü götürür (RFQM maddə 139).

Kommersiya informasiyasının vacib mənbələrindən biri insanlar, sə-nədlər və nəşrlərdir. İnsanlarla və sənədlərlə işin necə təşkil olunduğundan firmanın təhlükəsizliyi asılıdır.

Hüquqdankənar, yaxud ehtiyatsız hərəkətlərin, həmçinin kommersiya sirri ilə qeyri-peşəkar hərəkət, yaxud onun açıqlanmasının doğurduğu iqtisadi, maliyyə və maddi ziyanın firmaya vurulmasının qarşısını almaq məqsədlərinə aşağıdakı təkliflər xidmət edir.

Kommersiya sirrini təmin etmək üzrə təkliflər ümumi tövsiyə xarakteri daşıyır, normativ sənəd deyil, kommersiya xarakterli məlumat olan sənədlərlə işə yönəldilib və ən əsası, kommersiya sirlərinin mühafizəsinin təşkilati ölçülərini nəzərdə tutur.

Kommersiya sirri dedikdə dövlət sirri olmayan istehsal-texniki, elmi-tədqiqat, təcrübə-konstruktor və firmanın fəaliyyəti ilə bağlı məlumatlar, həmçinin onun texnoloji informasiyası, idarəsi, maliyyəsi və s. bağlı məlumatlar başa düşülür ki, bunların da açıqlanması, sızması və onlara sanksiya verilmiş müdaxilə firmanın maraqlarına ziyan vura bilər.

Kommersiya sirri olan məlumatlara firmanın direktorunun əmri ilə işə salınan və təsdiqlənən kommersiya sirri olan konkret məlumatların siyahısı ilə nəzərdə tutulmuş sirr olmayan məlumatlar aiddir.

Kommersiya sirri onun mülkiyyətidir. Əgər kommersiya sirri razılıq əsasında digər müəssisələrlə birgə fəaliyyətin nəticəsidirsə, onda bu sirr hər iki tərəfin mülkiyyəti ola bilər. Bu hal razılıqda öz əksini tapmalıdır.

Qeyd etmək lazımdır ki, kommersiya sirri olan sənədə münasibliyin məhdudiyyət qrifinin nişanına vahid müəyyənlik yoxdur. Belə qrif «kommersiya sirri», «müəssisənin sirri» və başqa sözlər də ola bilər. Bu cür məhdudiyyət qrifi məxfiliyin qrifi deyil, o yalnız göstərir ki, verilən informasiyaya mülkiyyət hüququ qanunvericiliklə mühafizə olunur.

Cədvəl 13

Kommersiya sirri

Müəyyənlik	Məzmun
Subyekt	Müəssisələr, təşkilatlar, kollektivlər, vətəndaşlar
Obyekt	Bu anlayış intellektual və sənaye mülkiyyətinin geniş spektrinə tətbiq oluna bilər
Xarakteristikalar	1. Fəal resurs 2. Konfidensial informasiya 3. Mülkiyyətin xüsusi forması 4. Bazar yeniliyi əmtəəsi
Qiymətlilik	Real (potensial) olaraq rəqabət mübarizəsində üstünlüklər yaradır
Tələblər	1. Potensial xeyirlidir 2. Ümumən məlum deyil
Təsir müddəti	Əmtəənin həyan tsikli ilə müəyyən edilir
Müdafiə	1. Hüquq 2. Təşkilati 3. Mühəndir-texniki

Kommersiya sirri-dövlət məxfiliyi olmayan istehsalla, texnologiya ilə, idarəetmə ilə, maliyyə ilə və digər fəaliyyətlə bağlı, açıqlanması, sızması və ona sanksiya olunmamış müdaxilə sahiblərinə ziyan vura bilən məlumatlardır. Kommersiya sirrinə aid deyil:

1. Dövlət tərəfindən mühafizə olunan məlumatlar
2. Qanuni əsaslarla ictimai məlumatlar
3. Ümumən münasib məlumatlar, patentlər, əmtəə nişanları
4. Fəaliyyətin neqativ tərəfi haqqında məlumatlar
5. Təsərrüfat fəaliyyətinin təsis sənədləri və məlumatları

7.2. Kommersiya sirri sayılan informasiyanın və onun «həyat» müddətinin müəyyən edilməsi qaydası

«Kommersiya sirri» (KS) qrifinin qoyulması vacibliyinin müəyyən edilməsi yuxarıda adı çəkilən siyahı əsasında həyata keçirilir.

Sənədlər üzərində- icraçı ilə və sənədə qol çəkən şəxslə, nəşrin üzərində – müəlliflə (tərtib edənlə) və nəşri çapa təsdiqləyən rəhbərlə.

Sənəddə olan kommersiya sirrinin təsir müddəti hər bir konkret halda sənədə qol çəkən şəxslə, yaxud icraçı ilə konkret tarix şəklində, yaxud «əmək müqaviləsi bağlanana qədər», yaxud «müddətsiz» şəklində müəyyən edilir.

Kommersiya sirri olan məlumatlardan ibarət sənədlərdə, işlərdə və nəşrlərdə «kommersiya sirri» qrifi (KS) qoyulur. Sənədlərdə və nəşrlərdə, bundan əlavə nüsxələrin nömrələri də qoyulur.

«Kommersiya sirri» qrifi və nüsxənin nömrəsi sənədin birinci səhifəsinin sağ yuxarı küncündə, nəşrin üst qabığında və titul vərəqində və bu materiallara olan müşayiətedici məktubun birinci səhifəsində qoyulur.

Kommersiya sirri olan sənədin hər nüsxəsinin son vərəqinin arxa tərəfində nişan çap olunur ki, burada da: çap olunmuş nüsxələrin miqdarı, icraçının nömrəsi, soyadı, telefonu, sənəddə olan sirrin təsir etmə müddəti (konkret vaxt, yaxud «əmək razılığının bağlanmasına qədər», yaxud «müddətsiz») makinaçının soyadı göstərilir.

«Kommersiya sirri» qrifinin götürülməsi sualı haqqında qərar tərkibinə təhlükəsizlik xidməti və müvafiq struktur bölmələrin nümayəndələri daxil olan müəyyən edilmiş qaydada yaradılan xüsusi komissiyanın üzərinə qoyulur.

Komissiyanın qərarı sərbəst formada yazılan aktla sənədləşdirilir və müdirlə və yaxud istiqamət üzrə onun müavini ilə təsdiqlənir. Aktda «KT» qrifi üzərindən götürülən işlər sadalanır. Aktın bir nüsxəsi işlərlə bir yerdə arxivə, daimi saxlanılma üçün isə – dövlət arxivinə götürülür. İşlərin üst vərəqindəki «KT» qrifi möhürlə, yaxud onun götürülməsi üçün əsas olmuş aktın tarixinin və nömrəsinin əl yazısı ilə göstərilməsi ilə qüvvədən salınır.

Analoji qeydlər işlərin təsvirinə və nomenklaturalarına daxil edilir.

5 dekabr 1991-ci il №35 Rusiya Federasiyasının hökumətinin qərarı.

(3 dekabr 2002-ci il №731 tarixli RF hökumətinin qərarının daxil etdiyi dəyişiklikləri nəzərə alaraq).

Kommersiya sirri ola bilməyən məlumatların siyahısı haqqında.

Dövlət Vergi xidmətinin, hüquq-mühafizə və nəzarət orqanlarının fəaliyyətini təmin etmək məqsədi ilə, həmçinin özəlləşdirmə prosesində sui-istifadələrin qabağını almaq məqsədi ilə RSFSR hökuməti qərara alır.

1. Müəssisənin və sahibkarın kommersiya sirri aşağıdakıların ola bilmədiyi müəyyən edilsin:

- təsis sənədləri (müəssisənin yaradılması qərarı yaxud təsisçilərin müqaviləsi) və nizamnamə;
- sahibkarlıq fəaliyyəti ilə məşğul olmağa hüquq verən sənədlər (hüquqi şəxslərin Vahid dövlət reyestrinə hüquqi şəxslər haqqında qeydlərin daxil edilməsi faktını təsdiqləyən sənədlər, individual sahibkarların dövlət qeydiyyatı haqqında şəhadətnamələr, lisenziyalar, patentlər);
- hesabatın müəyyən edilmiş formaları üzrə maliyyə-hesabat fəaliyyəti haqqında məlumatlar və RSFSR dövlət büdcə sisteminə vergilərin və digər mütləq ödəmələrin hesablanması və ödənilməsinin düzgünlüyünün yoxlanılması üçün vacib olan digər məlumatlar;
- tədiyə qabiliyyəti haqqında sənədlər;
- işləyənlərin sayı, tərkibi, onların əmək haqları və əmək şəraitləri, həmçinin boş iş yerlərinin olması haqqında məlumatlar;
- vergilərin ödənilməsi və mütləq tədiyyələr haqqında sənədlər;
- ətraf mühitin çirklənməsi, monopoliyaya qarşı qanunvericiliyin pozulması, təhlükəsiz əmək şəraitinə əməl olunmaması, əhalinin sağlamlığına ziyan vuran məhsulun satışı, həmçinin RSFSR qanunvericiliyinin başqa pozuntuları və bu zaman vurulan zərər haqqında məlumatlar;

- Müəssisənin vəzifəli şəxslərinin kooperativlərdə, kiçik müəssisələrdə, aksioner cəmiyyətlərində, birliklərdə və sahibkarlıq fəaliyyəti ilə məşğul olan digər təşkilatlarda iştirakı haqqında məlumatlar.

2. Dövlət və bələdiyyə müəssisələrinə onların özəlləşdirilməsinə qədər və sonra kommersiya sirrinə aşağıdakı verilənləri aid etməyi qadağan etmək;

- müəssisənin mülkiyyətinin ölçüləri və onun pul vəsaitləri haqqında;
- digər müəssisələrin gəlir aktivlərinə (qiymətli kağızlara), faiz istiqrazlarına və borclarına, birgə müəssisələrin nizamnamə fondlarına vəsaitlərin qoyuluşu haqqında;
- RSFSR qanunvericiliyindən və bağladığı müqaviləələrdən irəli gələn müəssisənin kredit, ticarət və başqa öhdəçilikləri haqqında;
- Kooperativlərlə, başqa qeyri-dövlət müssisələri ilə, yaradıcılıq və müvəqqəti əmək kollektivləri ilə, həmçinin ayrı-ayrı vətəndaşlarla müqavilələr haqqında.

3. Sahibkarlıq fəaliyyəti ilə məşğul olan müəssisələr və şəxslər, dövlət və bələdiyyə müəssisələri rəhbərləri RSFSR qanunvericiliyinə əsasən hakimiyyət orqanlarının, idarəetmə, nəzarət və hüquq-mühafizə orqanlarının buna hüququ olan digər hüquqi şəxslərin, həmçinin müəssisənin əmək kollektivinin tələbi ilə bu qərarın bir və iki bəndlərində sadalanan məlumatları təqdim etməyə borcludurlar.

4. Bu qərarın təsiri beynəlxalq müqavilələrə uyğun kommersiya sirrinə aid edilən məlumatlara, həmçinin qüvvədə olan qanunvericiliyə görə dövlət sirri sayılan müəssisələrin fəaliyyəti haqqında məlumatlara yayılmır.

B.Yeltsin

7.3. Məxfi informasiyaya qanunsuz yiyələnmə üsulları

Firmanın kommersiya sirri olan məlumatlar pisniyyətli insanlar tərəfindən sirrin açılması, sızması yaxud sərancamsız daxilolma nəticəsində əldə edilə bilər.

Bu hərəkətlərin hər biri müəyyən xüsusiyyətə malikdir.

7.3.1. Sirrin açılması

Kommersiya sirrinin açılması deyəndə vəzifəli yaxud digər şəxslər tərəfindən mühafizə olunan məlumatların xidməti zəruriyyətdən irəli gəlməyən, vaxtından tez açıqlanması, həmçinin bu cür məlumatların açıq texniki kanallarla ötürülməsi, yaxud icazə verilməmiş EHM emalı kimi hüquqa zidd, qərəzli yaxud ehtiyatsız hərəkətlər nəzərdə tutulur.

Yuxarıda göstərilən məlumatların açıq nəşri dedikdə, materialların açıq mətbuatda çapdan çıxması, radio və televiziya ilə verilməsi, beynəlxalq və daxili qurultaylarda, konfransiyalarda, müşavirələrdə, simpoziumlarda, dissertasiyaların ictimai müdafiəsində və digər ictimai çıxışlarda səsləndirilməsi, azad paylanma, materialların xaricə çıxarılması yaxud xarici firmalara, təşkilatlara yaxud birbaşa xidməti borcdankənar şəxslərə ötürülməsi başa düşülür.

Bu məlumatların açıq nəşrinin vacibliyi və imkanı, həmçinin onların nəşrinin həcmləri, formaları və vaxtı direktor yaxud onun müavinləri ilə daimi fəaliyyət göstərən ekspertlər komissiyasının rəyinə görə müəyyən edilir.

Kommersiya informasiyasının açıq nəşrini məhdudlaşdırmaq üzrə ölçülər aşkarlıq prinsipinin ziyanına və ictimaiyyətdən təsərrüfatsızlıq, israfçılıq, vicdansız rəqabət və digər neqativ hallar faktlarını gizlətmək üçün istifadə oluna bilməz.

Müqavilə yaxud inanma əsasında əldə edilmiş, yaxud da birgə istehsal fəaliyyətinin nəticəsi olan məlumatların açıq nəşri üçün istifadə edilməsinə
əməkdaşların birgə razılığı olduqda icazə verilir.

Birbaşa xidməti əlaqə ilə bağlı olmayan özgə təşkilatlara informasi-yanın ötürülməsi bir qayda olmaqla informasiyanın təqdim edilməsinə maddi xərclərin ödənilməsi və müqavilə öhdəçiliklərini pozmağa görə kompensasiya daxil olmaqla

istifadəçilərin öhdəlikləri və cavabdehliyini nəzərə alan müqavilə münasibətləri ilə tənzimlənir.

Kommersiya informasiyasının xidməti, təftiş fiskal və istintaq orqanlarının nümayəndələrinə, Dövlət Dumasının desputlarına, mətbuat orqanlarına, radio və digərlərinə təqdim edilməsi müvafiq qaydalarla tənzimlənir.

«Kommersiya sirri» qrifi ilə tiraj edilmiş sənədlər və nəşrlər məhdud yayım üçün məlumatlardan ibarət olan materiallar kimi nəzərdən keçirilir.

«KS» qrifli materiallarla iş zamanı məxfiliyin kommersiya sirrinin saxlanılması üzrə lazımi ölçülərin vaxtında işlənib həyata keçirilməsinin təmin edilməsi məsuliyyəti direktorun, onun istiqamətlər üzrə müavinlərinin və struktur bölmələrin rəhbərlərinin üzərinə düşür. Kommersiya sirrinin mühafizəsinin təşkili və həyata keçirilməsinə, ona riayət olunmasına daimi nəzarətin aparılması təhlükəsizlik xidmətinə həvalə edilir.

Təhlükəsizlik xidməti kommersiya sirrinin saxlanılması üzrə ölçülən şəxslərin dairəsini maksimal məhdudlaşdırmaq, belə məlumatları saxlayan sənədlərin fiziki qorunması, «KS» qrifli informasiyanın mühafizə olunan EHM emalı, konkret informasiyanın məxfiliyi üzrə tələblərin daxili və xarici ticarət partniyorları ilə müqavilələrin daxil edilməsi yolu ilə götürülür.

Kommersiya sirrinin mühafizəsi nəzərdə tutur:

- kommersiya sirri olan informasiyanın və onun təsir müddətlərinin müəyyənləşdirilməsi qaydasını;
- kommersiya sirrini təşkil edən məlumatlarda əməkdaşların, ezamiyyət olunmuş və adi şəxslərin daxilolma sistemini;
- «KS» qrifli sənədlərlə işləmək qaydasını;
- «KS» qrifli sənədlərin, işlərin və nəşrlərin qorunmasının təminini;
- kommersiya sirri olan məlumatlarla buraxılmış şəxslərin vəzifələrini;
- kommersiya sirrini təşkil edən məlumatlarla iş zamanı məxfiliyin təmininə nəzarətin təşkili və aparılması prinsipləri;

- kommersiya sirri olan sənədlərin itirilməsi məlumatların aşkarlanmasına görə məsuliyyət.

«Kommersiya sirri» qrifli sənədlərin, işlərin və nəşrlərin uçotunun, artırılmasının saxlanılmasının həyata keçirilməsinə nəzarət təhlükəsizlik xidmətinin səlahiyyətli üzvlərinə həvalə edilir.

«Kommersiya sirri» qrifli sənədlərdə və nəşrlərdə məlumatların aşkarlanmamasına nəzarət təhlükəsizlik xidməti şöbələri ilə həyata keçirilir.

7.3.2. Sızılma

Ümumi planda konfidensial informasiyanın sızılmasına qorunan məlumatların təşkilat hüdudlarından, yaxud bu məlumatların etibar edilən şəxslər dairəsindən nəzarətsiz çıxışı kimi baxmaq olar.

Konfidensial informasiyanın sızılması texniki kanallarla müəyyən şəraitdə həyata keçirilir.

Kommersiya sirlərinin sızılmasına səbəb olan faktor və şəraitlərə aiddir:

- əməkdaşların kommersiya sirlərinin qorunması qaydalarını yaxşı bilməməsi və onlara dəqiqliklə riayət etməyin vacibliyini axıra qədər dərk etməmələri;
- attestasiyadan keçməmiş konfidensial informasiyanın emalının texniki vasitələrin istifadəsi;
- qaydaların, təşkilati və mühəndis-texniki ölçülərin informasiyanın qorunması qaydalarına əməl olunmasına zəif nəzarəti.

Nitq informasiyasının mümkün sızılma kanalları.

İnformasiya siqnallarının yaranmasının fiziki təbiətindən, akustik dalğaların yayılma mühitindən və onların tutulma üsullarından asılı olaraq, akustik (danışıq) informasiyasının sızılma kanallarının hava, vibrasiya, optik-elektrik və parametrik kanallarına bölmək olar.

1. İnformasiyanın sızılmasının hava texniki kanalları.

Bu kanallarda akustik siqnalların yayılma mühiti havadır və onları tutmaq üçün miniatür yüksək həssaslı mikrofonlar və xüsusi istiqamətlənmiş mikrofonlardan istifadə edilir. Miniatür mikrofonlar portativ səsyazma qurğuları yaxud miniatür ötürücülərlə birləşdirilir. Miniatür mikrofonları və ötürücüləri konstruktiv birləşdirən muxtar qurğuları akustik qoymalar adlandırırlar.

Qoyma qurğusu ilə tutulmuş nitq informasiyası radiokanalla antik kanalla, dəyişkən cərəyan şəbəkəsi ilə, köməkçi texniki vasitələrin və sistemlərin birləşdirici xətləri ilə, kənar ötürücülərlə (sutəchizatı və kanalizasiya boruları, metalkonstruksiyalar ilə və s.) özü də ki, borularla və metal-konstruksiyalarla informasiyanın ötürülməsi üçün təkcə elektromaqnit yox, həm də mexaniki ultrasəs rəqsləri istifadə oluna bilər.

Qoyma qurğuları ilə ötürülən informasiyanın qəbulu bir qayda olaraq münasib dalğa diapozonunda işləyən xüsusi qəbuledici qurğularla həyata keçirilir. Lakin elə qoyma qurğularına da rast gəlmək olar ki, informasiyanın qəbulunu adi telefon aparatından həyata keçirmək olur. Belə belə qurğular ya bilavasitə nəzarət olunan otaqda yerləşən və «nəzarətçi telefon» adlanan telefon aparatının korpusunda quraşdırılır, yaxud da telefon xəttinə, adətən telefon rozetkasına qoşulur. Müşayiətedici qurğunu konstruktiv olaraq miniatür mikrofon və xüsusi kommunikasiya blokunu birləşdirir və adətən «telefon qulağı» adlandırılır. İnformasiya akustik qoymaların istifadəsi nəzarət olunan obyektə (otağa) daxil olmanı tələb edir. Bu mümkün olmadığı hallarda danışıq informasiyasını tutmaq üçün istiqamətlənmiş mikrofonlardan istifadə olunur.

2. Vibrasiyalı texniki kanallar

İnformasiya sızılmasının vibrasiyalı texniki kanallardan akustik siqnalların yayılma mühiti binaların, tikintilərin, kanalizasiyanın və digər bərk əşyaların konstruksiyalarıdır. Bu halda akustik rəqslərin tutulması üçün kontakt mikrofonları (stetoskoplar) istifadə edirlər.

Vibrasiya kanalı ilə həmçinin qoyma qurğularından istifadə etməklə informasiyanı tutmaq mümkündür. Əsasən informasiyanı ötürmək üçün radiokanal istifadə olunur, ona görə də bu cür qurğuları tez-tez radiosistemlər adlandırırlar. Qoyma qurğularından informasiyanı antik kanalla, həmçinin ultrasəs kanalı (binanın metal konstruksiyaları ilə) ilə ötürməklə də istifadə etmək mümkündür.

3. İnformasiya sızılmasının elektroakustik kanalları

İnformasiya sızılmasının elektroakustik kanalları akustik siqnalların elektrik siqnallarına elektroakustik çevrilmələr hesabına yaranır və mikrofon effektinə malik olan texniki sistemləri vasitəsilə, həmçinin yüksəkdalğalı məcburetmə yolu ilə akustik rəqslərin tutulmasından ibarət olur.

Texniki rabitə sistemlərinin bəzi elementləri, o cümlədən transformatorlar, induktivlik katuşkaları, təkrar elektrosaatların elektromaqnitləri, telefon aparatlarının zənglərinin, gündüz lampalarının drosselləri və s. akustik rəqslərin mənbəyinin yaratdığı akustik sahənin təsiri altında öz parametrlərini dəyişmək xüsusiyyətlərinə (həcm, induktivlik, müqavimət) malikdir.

Parametrlərin dəyişməsi ya bu elementlərin üzərində təsiredici informasiya siqnalları qanununa görə dəyişilən EDS əmələ gəlməsinə (akustik sahənin) ya da informasiya siqnalı kimi bu elementlərlə axan cərəyanın modulyasiyalarına gətirib çıxarır. TRS göstərilən elementlərdən başqa bilavasitə elektroakustik çeviricilərini daxil edə bilər: yanğın siqnalizasiyasının bəzi öütürücülərini, retranslyasiya şəbəkəsinin bərkdanışanlarını və s. özü də mikrofon effektinə malik TRS-dən akustik sahəyə ən böyük həssaslıq abunə bərkdanışanlarındadır.

İnformasiyanın sızılma kanallarındakı akustik rəqsin tutulması TRS birləşdirici xətlərinə xüsusi yüksək həssaslıq gücləndiricilərinin bilavasitə qoşulması yolu ilə həyata keçirilir.

Məsələn, elektromexaniki çağırış zəngləri olan telefon aparatlarının birləşdirici xətlərinə belə bilavasitə qoşmaqla, bu

aparatların yerləşdiyi otaqlarda gedən söhbətlərə qulaq asmaq olar.

Yüksəktezlikli (YT) məcburedilmə yolu ilə informasiyanın texniki sızılma
kanalına YT- siqnalının informasiya siqnalına modulyasiyasının baş verdiyi TRS parametrik, yaxud qeyri-xətti elementləri ilə funksional əlaqələri olan xətlərə yüksək tezlikli cərəyanların sanksiya edilməmiş kontakt daxiledilmə yolu ilə nail olmaq olar. TRS bu elementlərindəki informasiya siqnalı axırıncıların «mikrofon effekti» sayəsində yaranır.

YT- siqnal üçün qeyri-xətti, yaxud parametrik elementlər bir qayda olaraq razılaşdırılmamış yüklənmə olduğundan, modelləşdirilmiş YT-siqnalı ondan əks olunacaq və xətlə əks-istiqamətdə yayılacaq, ya da şüalanacaqdır. Əks olunmuş yaxud şüalandırılmış YT-siqnalların qəbulu üçün yüksəkhəssaslı xüsusi qəbuledicilər istifadə olunur. Zondlaşdıran və təkrar əks edilən siqnalların təsirini aradan götürmək üçün impuls siqnalları istifadə oluna bilər.

4. Optik-elektron texniki sızılma kanalı.

Bu kanal lazer şüası ilə akustik sahədə vibrasiya edən nazik əksedci səthlərin (şüşələrin, şəkillərin, güzgülərin) şüalandırılması zamanı yaranır. Əksolunmuş lazer şüalanması amplituda və fazaya görə modelləşdirilir (səthlərin vibrasiyası qanuna görə) və lazer şüalandırılması qəbuledicisi ilə qəbul edilərək, demodulyasiyadan sonra nitq informasiyasına çevrilir. Özü də lazer və qəbuledici bir yerdə yaxud da müxtəlif yerlərdə quraşdırıla bilər.

Yuxarıda qeyd olunan informasiyanın ötürülməsinin texniki vasitələri və texniki rabitə sistemlərinin xüsusiyyətlərindən, həmçinin texniki kəşfiyyatın imkanlarından irəli gələnləri nəzərə alaraq belə qərara gəlmək olar ki, sanksiya olunmamış müdaxilə imkanı potensial olaraq mövcuddur.

7.3.3. Sanksiya olunmamış müdaxilə

Konfidensial informasiyaya Sanksiya olunmamış istifadə cəhdi – bu əvvəlcədən fikirləşmiş bədəməl şəxslərin mühafizə

olunan məlumatların ələ keçirilməsi məqsədilə hüququna zidd hərəkətləridir. Sanksiya olunmamış istifadə həm leqal, həm də qeyri-leqal yolla müdaxilə kanalları vasitəsilə həyata keçirilir.

Sanksiya olunmamış istifadənin ən çox yayılan üsullarına aiddir:

- təşəbbüskar əməkdaşlıq, əməkdaşlığa cəlb edilmə, hiylə ilə öyrənmə, qulaq vermə, müşahidə, məhvedilmə, şəkilçəkmə (əməkdaşlara yönəldilib);
- müşahidə, oğurluq, surətçıxarma, saxtalaşdırma, məhvedilmə, ələ keçirmə, qeyri-aşkar tanışlıq, şəkilçəkmə, yığılma və emal (sənədlərə yönəldilir);
- saxtalaşdırma, qeyri-aşkar tanışlıq, yığım və analitik emal (nəşriyyatda çıxan məlumatlara yönəldilir);
- oğurluq, surətçıxarma, saxtalaşdırma, məhv edilmə, yığma və analitik emal (texniki vasitələrə yönəldilir);
- qulaqvermə, məhvedilmə, qanunsuz qoşulma, tutma (OPD texniki vasitələrinə yönəldilir);
- qulaqvermə, müşahidə, oğurluq, surətçıxarma, saxtalaşdırma, məhvedilmə, qanunsuz qoşulma, tutma, qeyri-aşkar tanışlıq (ASOD texniki vasitələrinə yönəldilir);
- müşahidə, oğurluq, surətçıxarma, saxtalaşdırılma, məhvedilmə, qeyri-aşkar tanışlıq, şəkilçəkmə (məhsula yönəldilir);
- oğurluq, yığma və analitik emal (tullantılara yönəldilir).

7.4. Konfidensial informasiyaya mütəxəssislərin buraxılma qaydası

Mütəxəssislərin konfidensial xarakterli məlumatlara yiyələnmələri könüllü qaydada bunun üçün təyin olunmuş təhlükəsizlik xidməti mütəxəssisləri tərəfindən həyata keçirilir.

1. Yiyələnmə nəzərdə tutur.

- müəssisənin kommersiya sirri olan ona etibar edilmiş məlumatların mütəxəssisin açıqlanması haqda öhdəlik götürməsi;

- mütəxəssisin konfirensial informasiya ilə iş zamanı onun hüquqlarının bir hissəsinin məhdudlaşdırılmasına razılığı;
- mütəxəssisin onunla yoxlama və nəzarət tədbirlərinin keçirilməsinə razılığı kommersiya sirrinin mühafizəsi üzrə, konfidensial sənədlərin mövcudluğu və onların saxlanma qaydaları üzrə əsas müddəaların və tələblərin yerinə yetirilməsi;
- mütəxəssisin Rusiya qanunvericiliyinin və müəssisənin kommersiya sirri haqqındakı normaları və onların və onun aşkarlanmasına görə məsuliyyət normaları ilə tanış edilməsi;
- kommersiya sirrinin mühafizəsi üzrə mütəxəssisə təlimatın verilməsi;
- konfidensial xarakterli məlumatlara yiyələnmək haqda qərarın qəbul edilməsi;
- konfidensial xaratkerli məlumatlarla iş zamanı mütəxəssisin işinə nəzarət.

2. Mütəxəssisin kommersiya sirlərinə yaxın buraxılma tələb edir:

- kommersiya sirləri ilə iş üzrə instruksiyaların tələblərinə ciddi əməl etmək;
- informasiya təhlükəsizliyi reciminin pozulmasına görə məsuliyyət.

7.4.1. Kommersiya sirrini təşkil edən məlumatlardan əməkdaşların, ezamiyyətdə olanların və fərdi şəxslərin istifadə edilməsinə icazə verilməsi sistemi

Kommersiya sirri olan məlumatlara əməkdaşların yaxın buraxılması direktor, onun istiqamətləri üzrə müavinləri və struktur bölmələrin rəhbərləri tərəfindən həyata keiçrilir.

Bölmələrin və təhlükəsizlik xidmətinin rəhbərləri «KS» qrifi məlumatlara yaxın buraxılan şəxslərin seçilməsinə cavabdehdirlər. Onlar bu məlumatların yalnız öz xidməti borclarını yerinə yetirmək üçün vacib olan şəxslərin bu məlumatlara yaxın buraxmaq üzərində sistematik nəzarəti təmin etməyə borcludurlar.

Kommersiya sirri olan məlumatlara lazımi mənəvi və işgüzar xüsusiyyətlərinə malik olan, kommersiya sirrini qo-

rumağı bacaran şəxslər və yalnız təhlükəsizlik xidmətində kommersiya sirrinin saxlanması üzrə individual yazılı öhdəçiliyi yazdıqdan sonra yaxın buraxılır.

«KS» işlərə onlara bilavasitə münasibəti olan əməkdaşların yaxın buraxılması struktur bölmənin rəhbərinin qolu olan və qovluğun içəri tərəfindən olan siyahıya uyğun, sənədlərə isə – bölmə rəhbərlərinin qətnamələrində olan göstərişlərə uyğun həyata keçirilir.

Ezamiyyət olunmuş və fərdi şəxslər «KS»qrifli sənədlərlə və nəşrlərlə tanışlıq və iş üçün onların işlədikləri təşkilatların yazılı sorğusu olduqda və bu sorğuda mövzu və yerinə yetiriləcək tapşırığın həcmi həmçinin tapşırığın yerinə yetirilməsinə sərəncam göstərildikdə bu sənədlərin məxsus olduğu firma və bölmələrin rəhbərlərinin yazılı icazəsi ilə buraxılır.

«KS» qrifi olan məlumatları olan sənədlərdən və nəşrlərdən seçilmiş yazıları elə bu cür qrifi olan dəftərlərdə qeyd edilir və nümayəndənin işi sona çatdıqdan sonra təşkilatın ünvanına göndərilir.

«KS» qrifi olan işlər və nəşrlər ifaçılara verilir və onlardan ələ verilən işlərin və nəşrlərin uçot vərəqində (forma 4) iltizamlarını aldıqdan sonra qəbul edilir.

7.4.2. «KS» qrifli sənədlərlə işləmə qaydası

Kommersiya sirlərini təşkil edən məlumatlardan ibarət sənədlər təhlükəsizlik xidmətinin dəftərxanasında, yaxud da ümumi şöbədə təhlükəsizlik xidmətinin səlahiyyətli işçisi ilə mütləq qeydiyyata düşməlidir. Onlar sənədlə nəzərdə tutulmuş rekvizitləri və «KS» qrifi (yaxud da bütövlükdə – «Kommersiya sirri») olmalıdır. Əcnəbilərdən alınmış sənədlərdə «KS» qrifini qrafit qələmlə nişan qoyurlar. Əcnəbilərə ötürülən sənədlərdə «KS»qrifi qoyulmur. Əcnəbilərdən alınan sənədlərdə «KS» qrifi qrafit qələmlə nişanlanır.

Sənədin mətnində və onun rekvizitlərində əlavə olaraq informasiyaya olan hüquqlar, ondan istifadə qaydası, nəşr olunmaya olan məhdudiyyətlərin müddəti ola bilər və s.

Mətndə və rekvizitlərdə «KS» qrifinin və xəbərdarlıqların olmaması azad yayılma nəzərdə tutur və belə ehtimal olunur ki, informasiyanın müəllifi və onun yayımına icazə verən (sənədi imzalayan, təsdiq edən) səlahiyyətli şəxs azad yayımın bütün nəticələrini nəzərə alıblar.

«KS» qrifi ilə, yaxud da başqa qriflə daxil olan bütün müxabirlərə bu materiallarla işləmək tapşırığı olan dəftərxana əməkdaşları tərəfindən qəbul olunur və açılır. Bu zaman sənədlərin və nəşrlərin vərəqlərinin və nüsxələrinin sayı, həmçinin də müşayiət məktubunda göstərilən əlavələrin olması yoxlanılır.

Zərflərdə «KS» sənədləri, yaxud da onlara olan əlavələr olmazsa, iki nüsxədə akt tərtib olunur və onlardan biri göndərənə ünvanlanır.

Bütün daxil olan xaric olan və daxili sənədlər, həmçinin «KS» qrifli nəşrlər qeydiyyatdan keçməlidir. Bu cür sənədlər vərəqlərin sayına görə, nəşrlər isə (kitablar, jurnallar və s.) – hər nüsxə üzrə nəzərə alınır.

«KS» qrifli sənədlərin və nəşrlərin uçotu jurnallarda (forma 1) yaxud kartlarda (forma 2) qeyri-sirr olmayan sənədlərin uçotundan ayrılıqda aparılır.

Jurnalların səhifələri nömrələnir, tikilir və möhürlənir. İşlərə tikilməyən nəşrlər inventor uçot jurnalında (forma 5) nəzərə alınır.

«KS» qrifli sənədlərin və nəşrlərin hərəkəti jurnallarda yaxud kartlarda vaxtında əks edilməlidir.

Hər qeydiyyata düşmüş sənəddə, həmçinin «KS» qrifli nəşrlərə müşayiət vərəqində ştamp qoyulur və bu ştampda sənədin adı, qeydiyyat nömrəsi və onun daxilolma tarixi qoyulur. Yayım üçün alınmış «KS» qrifli nəşrin tirajı bir daxilolma nömrəsi altında nəşrlərin uçotu və paylanması jurnalında (forma 3) qeydiyyata alınır. Sənədin əlavə çoxaldılmış nüsxələri bu sənədin nömrəsi altında qeydə alınır, bu haqda çoxaldılmış sənəddə və uçot formalarında qeyd edilir, əlavə çoxaldılmış

nüsxələrin nömrələnməsi bundan əvvəl qeydiyyata alınmış nüsxələrin nömrəsindən başlayaraq aparılır.

«KS» qrifli materialların çapı texniki sənədlərin tərtibi bürosunda, yaxud struktur bölmələrində onların rəhbərlərinin cavabdehliyi əsasında həyata keçirilir.

«KS» qrifli çap olunmuş və imzalanmış sənədlər onların qaralamaları və variantları ilə birlikdə uçot aparan dəftərxana əməkdaşlarına qeydiyyat etmək üçün ötürülür. Qaralamalar və variantlar bu əməkdaşla məhv edilir və bu haqda çıxış sənədinin surətində: «Qaralama (və variantlar) məhv edilib» sözü tarif və imza ilə birlikdə yazılır.

«KS» qrifli sənədlərin və nəşrlərin nəşriyyatlarda və çoxaltma aparat-larında çoxaldılması təhlükəsizlik xidmətinin icazəsi ilə və bölmə rəhbərinin imzaladığı və istiqamət üzrə rektor müavinin təsdiq etdiyi sifarişlər üzrə dəftərxananın nəzarəti altında həyata keçirilir. Çoxaldılmış sənədlərin və nəşrlərin uçotu xüsusi jurnalda hər nüsxə üzrə həyata keçirilir.

«KS» qrifli sənədlərin və nəşrlərin paylanması struktur bölmə rəhbərinin imzaladığı göndərilən nüsxələrin uçot nömrəsi göstərilən siyahılar əsasında həyata keiçrilir.

«KS» qrifli sənədlər yerinə yetirildikdən sonra ayrı-ayrı işlərə qruplaşdırılır. Onların qruplaşdırma qaydası qeyri-məxfi istehsal işinin nomenklaturaları ilə nəzərdə tutulur. İş nomenklaturasına mütləq qaydada bütün arayış kartotekaları və «KS» qrifli sənədlər və nəşrlər daxil edilir.

Açıq radiorabitədən istifadə etdikdə «KS» qrifi olan məlumatlara ötürməyə qadağa qoyulur. Belə məlumatlar yalnız qapalı texniki rabitə kanalı ilə yaxud da açıq teletayn rabitəsi yolu ilə sənədlərdə və teleqramlarda müvafiq ştampın qoyulması ilə ötürülə bilər

Xətti rabitədən istifadə edərkən ünvançının və göndəricinin vəzifəsini göstərmək qadağandır, yalnız göndəricilərin və alıcıların teleqraf ünvanlarını və soyadlarını göstərməyə icazə verilir.

Əməkdaşların «KS» qrifli səndlərin və nəşrlərin surətlərini çıxarmağa (əlyazmasını, maşın yazısını, mikro və fotosurətlərini, elektroqrafik və s. surətlərini), həmçinin onlardan çıxarışlar etməyə bölmə rəhbərlərinin icazəsi olduqdan sonra ixtiyarı var.

«KS» qrifli sənədlərdən və nəşrlərdən kənardan olan təşkilatlar üçün surətlərin çıxarılması bu sənəd və nəşrləri hazırlamış bölmə rəhbərlərinin icazəsinin yazılı tələbnaməsi əsasında edilir.

Analoji qeydlər siyahılara və işlərin nomenklaturasına daxil edilir.

«KS» qifli informasiyanın EHM emalı zamanı iş qaydası qeyri-məxfi informasiyanın emalı zamanı PEHM iş qaydası haqqında təlimatın tələblərinə uyğun olaraq müəyyən edilir.

7.4.3.Sənədlərin, işlərin və nəşrlərin saxlanmasının təmin edilməsi

«KS» qrifli sənədlər, işlər və nəşrlər xidməti binalarda və kitabxanalar-da etibarlı bağlanan və möhürlənən şkaflarda (anbarlarda) saxlanılmalıdır. Bu zaman onların fiziki saxlanmasını təmin edən şərait yaradılmalıdır.

İş üçün verilmiş «KS» qrifli işlər dəftərxanaya, yaxud təhlükəsizlik xidmətinin səlahiyyətli şəxsinə həmin gün qaytarılmalıdır.

«KS» qrifli ayrı-ayrı işlər dəftərxananın rəisinin yaxud da təhlükəsizlik xidmətinin səlahiyyətli şəxsinin icazəsi ilə icraçıda tapşırığı yerinə yetirmək üçün lazım olan müddət ərzində onların qorunması və çoxalması qaydalarına tam riayət olunması şərti ilə saxlana bilər.

«KS» qrifli sənədlərin, işlərin və nəşrlərin bu sənədlərə yaxın buraxılmış başqa əməkdaşlara ötürülməsi yalnız dəftərxana yaxud təhlükəsizlik xidmətlərinin səlahiyyətli şəxsi vasitəsilə həyata keçirilir.

«KS» qrifli sənədlərin dəftərxananın yaxud təhlükəsizlik xidmətinin səlahiyyətli şəxsinin sanksiyası olmadan bir işdən o birisinə yerdəyişməsi, yaxud çıxarılması qadağan edilir. Aparılmış

bütün çıxarılmalar, yaxud yerdəyişmələr haqqında uçot sənədlərinin daxili siyahıları daxil edilməklə qeydlər edilir.

«KS» qrifli sənədləri, işləri və nəşrləri onlarla evdə, mehmanxanalarda və s. işləmək üçün xidməti binalardan kənara çıxarmaq qadağandır.

Vacib olan hallarda bölmələrin rəhbərləri icraçılara yaxud dəftərxananın əməkdaşlarına bu şəhərin hüdudlarında yerləşən təşkilatlarda onların razılaşdırılması, imzalanması və s. üçün «KS» qrifli sənədlərin binadan çıxarılmasına icazə verə bilərlər.

Başqa şəhərlərdə ezamiyyət olunan şəxslərə yolda «KS» qrifli sənədlərlə, işlərlə və nəşrlərlə olmaq qadağandır. Bu materiallar qabaqcadan əməkdaşın ezam olunduğu təşkilatın ünvanına bir qayda olaraq sifarişli yaxud qiymətli poçt göndərmələri, həmçinin də kuryerlə göndərilməlidir.

«KS» qrifli sənədlərin, işlərin və nəşrlərin uçot və saxlanmasına cavabdeh əməkdaşlar əvəz edilərkən, bu sənədlərin sərbəst formada qəbul-ötürmə aktı tərtib olunur və istiqamətlər üzrə direktor müavini yaxud da struktur bölmələrin rəhbərləri ilə təsdiqlənir.

7.4.4. Kommersiya sirri sayılan məlumatlarla işlərkən obyekt daxili rejimin tələblərinin yerinə yetirilməsinə nəzarət

Kommersiya sirri ilə iş zamanı obyekt daxili rejim dedikdə kommersiya sirri olan məlumatlar haqqında informasiyanın sızılması imkanını istisna edən iş şəraitinə riayət etmək başa düşülür.

Göstərilən recimə əməl etməyə nəzarəti kommersiya sirrinin saxlanma vəziyyətinin qiymətləndirilməsi və öyrənilməsi məqsədiylə, çatışmamazlıqların və onların səbəblərinin müəyyən etmək və onları aradan götürmək üzrə təkliflər hazırlamaq məqsədiylə həyata keçirirlər. Kommersiya sirri olan məlumatlarla iş zamanı recimin təmin edilməsinə nəzarəti müəssisənin təhlükəsizlik xidməti və struktur bölmənin rəhbəri cari və planlı yoxlamalar yolu ilə həyata keçirirlər.

Yoxlama zamanı «KS» materiallarla işə yaxın buraxılmış iki nəfərdən az olmayan tərkibdə təcrübəli və ixtisaslı işçilərdən dəstəklənən komissiya yaradılır.

Planlı yoxlama ildə 1 dəfədən az olmayaraq komissiyalarla müəssisənin (bölmənin) rəhbərinin sərəncamı yaxud əmri əsasında aparılır. Yoxlama aparanların yoxlanılan məsələlərə aid olan bütün sənədlərlə, kartlarla və digər materiallarla tanış olmağı, həmçinin söhbət aparmağa, mütəxəssislərlə və icraçılarla məsləhətləşməyə komissiyanın səlahiyyətində olan bütün suallar üzrə yazılı izahatlar, arayışlar və hesabatların təqdim edilməsini tələb etməyə hüququ vardır.

Yoxlama zamanı struktur bölmənin rəhbərləri, yaxud da onun müavini iştirak edir.

Yoxlama nəticələrinə görə sənədlərin olması, «KS» materialları ilə işin vəziyyəti, aşkar edilmiş çatışmazlıqlar və onları aradan qaldırmaq təklifləri haqqında akt yaxud arayış tərtib edilir. Akt müəssisənin (bölmənin) rəhbəri ilə təsdiq edilir.

Kommersiya sirri olan sənədlərin itirilməsi yaxud məlumatların aşkar-lanması halları ortaya çıxdıqda müəssisənin rəhbəri və onun təhlükəsizlik üzrə müavini məlumatlandırılır. Göstərilən halların araşdırılması üçün müəssisənin rəhbərinin əmri ilə komissiya yaradılır ki, bu da itirilmiş sənədin məzmununun qoyulmuş «KS» qrifinə uyğunluğunu müəyyən edir və itkinin səbəblərini öyrənir. Komissiyanın iş nəticələrinə görə akt tərtib edilir.

7.4.4.Kommersiya sirri sayılan məlumatlarla işləri müəssisənin əməkdaşlarının vəzifələri və bu sirrin aşkarlanmasına görə məsuliyyəti

Kommersiya sirrini təşkil edən məlumatlara yaxun buraxılan müəssisə əməkdaşları bu məlumatların saxlanmasını təmin etmək məqsədilə onlara olan tələblərin dəqiq yerinə yetirilməsinə görə məsuliyyət daşıyırlar.

Kommersiya sirri ilə bağlı işə yaxın buraxılana qədər, onlar təminatın tələblərini öyrənməli və təhlükəsizlik xidmə-

tində kommersiya sirrinin saxlanması haqqında yazılı öhdəlik verməlidirlər.

Kommersiya sirrinə yaxın buraxılmış müəssisə əməkdaşları borcludurlar:

- kommersiya sirrini ciddi saxlamalıdırlar. Kommersiya sirrini təşkil edən məlumatların sızılmasından xəbər tutduqda, həmçinin «KS» qrifli sənədlərin itməsi haqqında özünün rəhbərinə və təhlükəsizlik xidmətinə məlumat verməlidir;

- «KS» qrifli sənədlərin hamısını təhlükəsizlik xidməti nümayəndələrinin tələbi ilə yoxlama üçün göstərilməlidir, onlarla müəyyən edilmiş iş qaydalarını pozduqları halda müvafiq izahat təqdim etməlidir;

- yalnız yaxın durmalarına icazə verilmiş sənədlərlə tanış olmalı və işləri görməlidir;

- «KS» qrifli sənədlərdən istifadə qaydalarına riayət etməli, onların əsassız yayımına yol verməlidir;

- təhlükəsizlik xidməti işi üzrə yaxud onun səlahiyyətli şəxsindən alınan məlum qrifli sənədlərin hamısını dərhal sənədlərin daxili siyahısına daxil etməlidir (forma 55). Bu siyahıda «KS» uçotu üzrə xüsusi bölmə ayrılır;

- yerinə yetirilmiş giriş sənədləri, həmçinin paylanma, işə tikilmə yaxud məhv edilmə üçün olan sənədləri təhlükəsizlik xidmətinə yaxud təhlükəsizlik xidmətinin səlahiyyətli işçisinə təhvil verilməlidir;

- «KS» qrifli sənədlərlə kənar şəxslərin, həmçinin göstərilən sənədlərə birbaşa münasibəti olmayan öz əməkdaşlarının tanışlıq imkanını istisna edən obyekt daxili rejimin tələblərini yerinə yetirməlidir;

- kənar təşkilatların nümayəndələri ilə, yaxud da hər hansı şəxslərlə işgüzar danışıqlar apararkən onların uğurlu nəticələnməsinə həqiqətən də vacib olan minimal informasiyanın verilməsi ilə məhdudlaşmalıdırlar;

- aşkarlanmış müəssisənin kommersiya sirrinin öz şəxsi xeyrinə istifadəyə, həmçinin rəqabətdə olanların istehsalın bu

kommersiya sirrinin sahibinə ziyan vuran fəaliyyətinə şərait yaratmamalıdır.

Müəssisənin kommersiya sirrini aşkarlamağa görə, sənədlərin itirilməsi yaxud belə məlumatları özündə təcəssüm etdirən məhsulların itirilməsinə

görə məsuliyyət qanunvericiliklə müəyyən edilir.

a) kommersiya sirri olan məlumatları aşkarlamaq – bu məlumatın xidmətdə, işdə etibar edilən şəxsin onu aşkarlaması, yaxud da başqa yolla məlumatlandırılaraq kənar şəxslərə çatmasıdır;

b) kommersiya sirrinə aid olan sənədlərin yaxud da məlumatların (əşyaların) itirilməsi xidməti yerində yaxud işində ona etibar olunmuş sənədlərin yaxud məlumatların əldən verilməsi, nəticədə bu sənədlərin yaxud məlumatların kənar şəxslərin əlinə keçməsi, yaxud da keçə bilməsidir.

RF CM Maddə 183

Kommersiya yaxud bank sirrini təşkil edən məlumatların qanunsuz əldə edilməsi və aşkarlanması.

1. Sənədlərin oğurlanması, rüşvət yaxud hədələmək yolu və s. qanunsuz üsullarla aşkarlamaq, ya da bu məlumatları qanunsuz istifadə etmək məqsədiylə kommersiya, yaxud bank sirri olan məlumatların toplanması 100-dən 200 MROT yaxud da əmək haqqı məbləğində yaxud bir aydan iki aya qədər müddətdə başqa gəlirin ölçüsündə cərimə ilə yaxud azadlıqdan 2 ilə qədər müddətə məhrum edilməklə cəzalandırılır.

2. Sahibinin razılığı olmadan kommersiya yaxud bank sirrini təşkil edən məlumatların şəxsi məqsədlər üçün qanunsuz aşkarlanması və istifadəsi və böyük ziyana səbəb olması – 200-dən 500 MROT ölçüsündə yaxud əmək haqqı ölçüsündə yaxud iki aydan 5 aya qədər digər gəlirin ölçüsündə, yaxud da azadlıqdan 3 ilə qədər müddətə məhrum və 50MROT ölçüsündə, yaxud günahkarın əmək haqqı yaxud başqa gəlirinin 1 ay müddətində ya da onsuz cərimə edilməklə cəzalandırılır.

7.4.5. Kommersiya sirri sayılan məlumatlarla iş zamanı rejimin təmin olunmasına nəzarətin təşkili və aparılması prinsipləri

Kommersiya sirrini təşkil edən məlumatlarla iş zamanı rejimin təmin edilməsinə nəzarət kommersiya sirrinin qorunmasının faktiki vəziyyətini öyrənmək və qiymətləndirmək məqsədiylə, «KS» qrifli materiallarla iş zamanı rejimin çatışmazlıqlarını və pozuntularını aşkar etmək, bu cür çatışmazlıqların və pozuntuların səbəblərini müəyyən etmək və onların aradan götürülməsi və qabağının alınmasına yönəldilmiş təkliflərin işlənib hazırlanması məqsədiylə həyata keçirilir.

«KS» qrifli materiallarla iş zamanı rejimin təmin edilməsinə nəzarəti təhlükəsizlik xidməti və struktur bölmə rəhbərləri həyata keçirir.

«KS» qrifin materiallarla iş zamanı rejimin təmin edilməsini yoxlamaq üçün kommersiya bu işlə yaxın buraxılan iki nəfərdən az olmayan təcrübəli və ixtisaslı işçilərdən təşkil edilir. Yoxlamada iştirak yoxlayanların bu məlumatlardan xəbərdarlığının əsassız artmasına gətirib çıxarmamalıdır.

«KS» qrifi materiallarla iş zamanı rejimin təmin edilməsinin yoxlanması direktorun yaxud onun istiqamətlər üzrə müavininin imzaladığı təlimat əsasında komissiyalar tərəfindən ildə 1 dəfədən az olmayaraq aparılır.

Yoxlamalar struktur bölmə rəhbərinin yaxud da onun müavininin iştirakı ilə aparılır.

Yoxlama aparanların yoxlanılan məsələlərə aid bütün sənədlərlə, kartlarla və digər materiallarla tanış olmağa, həmçinin söhbət aparmağa, mütəxəssislər və icraçılarla məsləhətləşməyə, komissiyanın səlahiyyətində olan bütün suallar üzrə yazılı izahatlar, arayışlar və hesabatların təqdim edilməsini tələb etməyə hüququ vardır.

Yoxlama nəticələrinə görə sənədlərin olması, «KS» materialları ilə iş vəziyyəti, aşkar edilmiş çatışmazlıqlar və onların aradan qaldırılmaq təklifləri haqqında akt, yaxud arayış tərtib edilir.

Direktorun yaxud onun müavininin aktı təsdiqlənliyindən sonra onunla struktur bölmənin rəhbəri tanış olaraq imza atır.

Yoxlama nəticəsində aşkar edilmiş «KS» materialları ilə iş zamanı rejimin çatışmazlıqları və pozuntularının aradan qaldırılması və təkliflərin yerinə yetirilməsi haqda bölmə rəhbəri komissiyanın müəyyən etdiyi müddətdə təhlükəsizlik xidməti rəisinə xəbər verir.

«KS» qrifli sənədlərin, işlərin və nəşrlərin itirilməsi faktı aşkar olunduq-da, yaxud onlarda olan məlumatlar aşkarlandıqda yubanmadan direktor, istiqamətlər üzrə müavini və təhlükəsizlik xidmətinin şöbə rəisi məlumatlan-dırılır. Göstərilən halların araşdırılması üçün müəssisənin rəhbərinin əmri ilə komissiya yaradılır ki, bu da itirilmiş sənədlərin itirilməsi faktını araşdıraraq nəticələri bu komissiyanı yaradan rəhbərə təsdiqlənmək üçün təqdim edir.

«KS» qrifli itirilmiş sənədlərə, işlərə və nəşrlərə akt tərtib edilir. Uçot sənədlərinə müvafiq qeydlər edilir.

İtirilmiş işlərə tutulmuş aktlar direktor və onun istiqamətlər üzrə müavini tərəfdən təsdiqləndikdən sonra arxivə verilir.

7.5. Qapalı müzakirələr və danışıqların keçirilmə qaydası

Kommersiya sirri olan suallar üzrə müzakirələrin və danışıqların keçirilməsinə razılığı firmanın rəhbərləri və onların səlahiyyət verdikləri şəxslərin icazə verməyə hüquqları vardır.

Belə danışıqların keçirilməsinə icazəni rəhbər, cavabdeh şəxs təyin edir. O, öz şöbəsində danışıq iştirakçılarının soyadı, adı və atasının adı, vəzifəsi və müəssisəni göstərməklə siyahı tərtib edir.

Danışıqlara yalnız siyahıda adı olan şəxslər buraxılır.

Danışıqları aparan şəxs kommersiya sirrini sax-lamaq vacibliyini görüş iştirakçılarının yadına salmalıdır və konkret olaraq hansı məlumatların mühafizə olunduğunu dəqiqləşdirməlidir. Bu danışıqların protokolunda qeyd olunur.

Danışıqlar vizual-optik, akustik və digər binanın özündə, yaxud da ondan kənarda pisniyyətlə tətbiq edilmə imkanını istisna edən xüsusi otaqlarda aparılmalıdır.

Kommersiya sirri olan suallarla əlaqədar hər danışıqda məruzənin, informasiyanın, çıxışın, sualların, qərarların soyadı üzrə qeydiyyata salınan protokol (yazılı yaxud maqnit) aparılır.

Kommersiya sirləri sualları üzrə ayrı-ayrı danışıqlar danışıq yazıları şəklində qeydə alınır.

Bütün materialların surətləri təhlükəsizlik xidmətinin xarici fəaliyyətin təhlükəsizliyini təmin edən qrupuna ötürülür.

7.6. Konfidensial sənədlərin arxivdə saxlanılmasının təşkili

Cari istehsal işi sənədləri il qurtardıqdan sonra müəssisənin arxivinə saxlanılmaq üçün ötürülə bilər.

«KS» qrifli sənədlərin tərtib edilməsi və ötürülməsi arxivdə, konfidensial informasiyası olan işlərin saxlanması təşkili üzrə təlimatın tələblərinə uyğun həyata keçirilir.

İşlərin saxlanmasının təşkili üzrə təlimat əsas texniki əməliyyatları əks edir, o cümlədən:

- konfidensial informasiyalı işlərin arxivə qəbulu;
- konfidensial informasiyası olan işlərin siyahısının tərtib edilməsi və yazılması;
- şəxsi heyət üzrə siyahının tərtib edilməsi və yazılması;
- konfidensial informasiyası olan sənədlərin uçotu.

FƏSİL VIII

MÜHƏNDİS-TEXNİKİ TƏHLÜKƏSİZLİK ŞÖBƏSİ

İnformasiyanın mühəndis-texniki müdafiəsinin başlıca vasitələrinə aiddir:

- müdafiənin fiziki vasitələri;
- müdafiənin aparat vasitələri;
- müdafiənin proqram vasitələri;

- müdafiənin riyazi (kriptoqrafik) metodları.

Göstərilən vasitələr aşağıdakı məsələrin həlli üçün tətbiq edilir:

- ərazinin mühafizəsi və ona nəzarət edilməsi;
- binaların, daxili otaqların mühafizəsi, onlara nəzarət edilməsi;
- avadanlıqların, anbarların və hərəkət edən informasiya daşıyıcılarının mühafizə edilməsi;
- qorunan zonalara, mühafizə olunan otaq və anbarlara nəzarətli girişin həyata keçirilməsi;
- vizual müşahidə, dinləmə və fotoşəklini çəkməyə maneələr yaradılması;
- kənar elektromaqnit şüalanmaları və tuşlamalarının neytrallaşdırılması;
- rabitə vasitələri, informasiya işlənməsi və elektron-hesablama texnikasının elektromaqnit şüalanmalarının mümkün tutulması imkanının istisna edilməsi.

Bu vəzifələrin yerinə yetirilməsi üçün mühəndis-texniki təhlükəsizlik şöbəsi təşkilati, təşkilati-texniki və texniki tədbirlər həyata keçirir.

8.1. Təşkilati tədbirlər

Təşkilati tədbirlərə məhdudlaşdırıcı xarakterli, əsasən girişin reqlamenləşdirilməsinə və ənənəvi və avtomatlaşdırılmış rejimlərdə məxfi informasiyanın təhlükəsizliyinin təmin edilməsinin texniki vasitələrindən istifadə edilməsinə gətirilən tədbirlər aid edilir. Onlar, bir qayda olaraq, sadə təşkilati tədbirlər və bunun üçün mümkün olan texniki vasitələrdən istifadə edərək təhlükəsizlik xidmətinin gücü ilə aparılırlar.

Təşkilati tədbirlər aşağıdakıları nəzərdə tutur:

- mühafizə edilən zonanın (ərazinin) sərhədlərinin müəyyən edilməsi;
- mühafizə edilən zona (ərazi) daxilində məxfi informasiyanın işlənməsi üçün istifadə edilən texniki vasitələrin müəyyən edilməsi;

- informasiya sızması kanallarının yaranması və ya texniki vasitələr vasitəsilə icazəsiz informasiyadan istifadə üsullarının mümkünlüyü nöqteyi-nəzərindən təhlükəli nöqtələrin müəyyən edilməsi;

- məxfi informasiyanın mümkün sızma kanallarının və ya informasiyadan icazəsiz istifadə (İİÜ) üsullarının qarşısının alınması və ya yol verilməməsi tədbirlərinin reallaşdırılması;

- kənar elektromaqnit şüalanması və tuşlamaları və ya xüsusi olaraq bunun üçün istifadə edilən siqnallar hesabına yaranan mümkün idarə olunmaz təhlükəli siqnallara nəzarət edilməsinin (axtarılması və aşkar edilməsi) təşkil edilməsi; özündə məxfi informasiyanın alınması və ötürülməsinin texniki vasitələrini əks etdirən hər hansı əşyaların, qurğuların, vasitələrin, mexanizmlərin mühafizə edilən zonaya gətirilməsi və aparılması üzərində ciddi nəzarətin təşkil edilməsi.

8.2. Təşkilati-texniki tədbirlər

Təşkilati-texniki tədbirlər informasiyanın istehsal və əmək fəaliyyətinin təmin edilməsinin texniki vasitələrindən mümkün sızma kanallarının binanın konstruksiyası elementlərində, otaqlarda və texniki vasitələrdə quraşdırılmış və potensial informasiya sızması kanalını təşkil edən xüsusi texniki vasitələrin köməyilə qarşısını kəsir.

Bu məqsədlə aşağıdakılardan istifadə etmək olar:

- passiv mühafizənin texniki vasitələri: süzgəclər, məhdudlaşdırıcılar və s., elektromaqnit və elektrik siqnallarının ayrılması vasitələri, elektrik təchizatı, radio və çasofikasiya (saatlaşdırma) şəbəkələrinin müdafiə sistemi və s.

- fəal mühafizənin texniki vasitələri: akustik küylərin və elektromaqnit maneələrinin ötürülcüləri.

8.3. Texniki tədbirlər

Texniki tədbirlər istehsal fəaliyyəti prosesində kənar şüalanma və tuşlanmalardan qorunan, məxfi informasiyanın işlənməsinin xüsusi texniki vasitələrinin və ya qorunan ərazidə normaları ötməyən KEŞT vasitələrinin əldə edilməsini, quraşdırılmasını və onlardan istifadə edilməsini təmin edir.

Texniki müdafiə vasitələri:

❖ *Mühafizə vasitələri*
- Mühafizə və yanğın-mühafizə siqnalizasiyası
- Mühafizə televiziyası
- Girişə nəzarət sistemi
- Xətti təhlükəsizlik vasitələri

❖ *İnformasiyanın qorunması vasitələri*
- İS (informasiya sızması) və İG (icazəsiz giriş) hallarının aşkar edilməsi vasitələri
- Müdafiə və əks təsir vasitələri
- Sistemli tədqiqat vasitələri

❖ *Proqramların qorunması vasitələri*
- Proqram
- Aparat
- Kombinələşdirilmiş

❖ *Nəzarət vasitələri*
- Radioloji
- Toksikoloji
- Pirotexnik
- Metal aşkar etmə

8.4. Texniki vasitələrin köməyilə informasiyanın icazəsiz əldə edilməsinin qarşısının alınması üzrə tədbirlər

Məxfi informasiyanın texniki vasitələrin köməyilə icazəsiz əldə edil-məsinin qarşısının alınması üzrə tədbirlər aşağıdakı başlıca istiqamətlərə gətirilir:
- müşahidə və fotoşəkil çəkilmədən qorunma
- dinlənilmədən qorunma

- tutulmadan qorunma.

Müşahidə və fotoşəkil çəkilmədən qorunma aşağıdakıları nəzərdə tutur:

- informasiyanın sənədləşdirilməsi, çoxaldılması və əks etdirilməsi (FEHM monitorlarında) (fərdi elektron hesablayıcı maşınlar) vasitələri üçün birbaşa və ya distansion müşahidənin (şəklinin çəkilməsi) istisna edilməsi məqsədilə optimal yerin seçilməsi;
- işıqkeçirməyən şüşələrdən, pərdələrdən, bəzəklərdən, plyonkalardan və başqa qoruyucu material və konstruksiyalardan (barmaqlıqlar, bəndlər, jalüzlər və s.) istifadə edilməsi;
- pəncərələri təhlükəliz zonalara, istiqamətlərə tərəf olan otaqların seçilməsi;
- FEHM-nın ekranlarını müəyyən müddətdən bir söndürən proqram vasitələrindən istifadə edilməsi (vaxt rejimi ilə iş).

Dinlənilmədən qorunma aşağıdakı şəkildə reallaşdırılır:

- səsuducu divar üzlüklərinin, qapı yerlərinin xüsusi təbillərinin, ikili pəncərə çərçivələrinin tətbiqi ilə;
- həcm və səthlərin (divarlar, pəncərələr, istilik radiatorları, ventilyasiya kanalları) akustik küy yaradan vasitələrindən istifadə edilməsi;
- ventilyasiya kanallarının, otaqlara istilik, elektrik enerjisi, telefon və ra-
diokommunikasiya kanallarının daxil olması sistemlərinin, mühafizə-yanğın sisteminin bağlanılması;
- məxfi informasiyanın sızması kanallarının meydana çıxmasını istisna edən xüsusi testləşdirilmiş otaqlardan istifadə edilməsi.

Kənar elektromaqnit şüalanmaları və ən müxtəlif xarakterli digər tuşlanmaların tutulmasından qorunma aşağıdakı şəkildə təmin edilir:

- KEŞT mənbələrini qorunan (nəzarətdə saxlanılan) zonanın sərhədlərindən maksimal mümkün uzaqlıqda yerləşdirilməsi;

- Otağın kanal kommunikasiyalarının köməyilə ekranlaşdırılması (sipərlə qorunması);

- Məkan və xətti elektromaqnit küyləndiricilərindən istifadə edilməsi;

- Qorunan ərazidən kənara çıxışı olmayan avtonom telefon sistemlərindən, lokal EHM sistemlərindən (o cümlədən, təkrar çasofikasiya sistemlərindən, radiofikasiya (radiolaşdırma) sistemlərindən, daxili istifadə üçün olan telefon sistemlərindən, dispetçer sistemlərindən, enerji təminatı sistemlərindən və s.) istifadə edilməsi;

- Mühafizə edilən zona daxilində yerləşdirilmiş elektrik enerjisi və torpaqlaşma zəncirlərinin açılması;

- İnformasiya zəncirlərində, enerji və torpaqlaşma zəncrlərində boğucu süzgəclərdən istifadə edilməsi.

8.5. Qorunan binaların attestasiyası

Texniki tədbirlərlə qorunan otaqların attestasiyasının məqsədi bu otaqlarda istehsal və əmək fəaliyyətinin təmin edilməsinin texniki vasitələrinin qurulması və onların xarakteristikalarının təhlükəsizlik tələblərinə cavab vermə səviyyəsinin müəyyənləşdirilməsindən ibarətdir.

Hər bir belə otaq üçün içərisində texniki vasitələrin, onların tipləri, nömrələri, real texniki xarakteristikaları və birləşdirici rabitə, enerji, torpaqlaşma xətləri və onların vəziyyətlərinin göstərildiyi texniki pasport tərtib edilir.

Otaqların texniki pasportları mühəndis-texniki mühafizə qrupunda saxlanılır. Hər hansı texniki vasitələrin qurulması və ya ləğv edilməsi zamanı otağın pasportunda mütləq dəyişiklik edilməlidir.

Hər bir otağın texniki vasitələrinin tərkibi orada KEŞT-larının olub-olmamasını müstəqil olaraq mühəndis-texniki

qrup tərəfindən və ya bu işlə məşğul olmaq üçün lisenziyaya, lazımi nəzarət-ölçü cihazlarına və xüsusi tədqiqatların aparılmasının lazımi metodlarına malik olan ixtisaslaşmış təşkilatın cəlb edilməsilə tədqiq etməklə müəyyən edilir.

Mühafizə olunan otaqlardakı texniki vasitələrin tərkibinin təhlili nəticələrinin və onların xüsusi tədqiqinin aparılması nəticələrinin nəzərə alınması ilə bu və ya digər qurğunun mühafizə edilən informasiyanın potensial sızma kanalı kimi təhlükəliliyi təyin edilir və onların aradan qaldırılması üçün məqsədəuyğun tədbirlər işlənib hazırlanır.

NƏTİCƏ

Müəllif firmanın təhlükəsizlik problemlərini və təhlükəsizlik xidmətinin fəaliyyətinin bütün aspektlərini təşkil edən bütün məsələlər çoxluğunun tam və hərtərəfli şərh edilməsinə çalışmamışdır.

Cəmiyyətin artan kriminallaşması kimi təhlükə amillərini vaxtında aydınlaşdırmaq və buna müqavimət göstərmək zəruridir. Hazırki dövrdə sahibkarlıq strukturlarının mühafizəsində kifayət qədər təcrübə yoxdur, bununla əlaqədar, həm dövlət, qanunverici səviyyədə, həm də konkret firma səviyyəsində bir çox tövsiyə və qaydalar işlənib hazırlanmalıdır. Təcrübə zamanla toplanır. Onu da bilmək lazımdır ki, həyatın bütün hadisələri üçün hər zaman hazır həll variantları ola bilməz. Bu gün verilmiş sahədə gündəlik sistematik işə hazır olmaq və təsadüfdən-təsadüfə yox, daimi olaraq təhlükəsizlik məsələlərinə qayğı ilə yanaşmaq lazımdır. Müəllif ümid edir ki, bu kitab oxucuya verilmiş problemə öz münasibətini müəyyən etməyə və irəli sürülən tövsiylər əsasında praktiki nəticələr

çıxarmağa kömək edəcəkdir. Oxuculara təhlükəsiz biznes arzu edirik. Yadda saxlayın: təhlükəsizlik heç vaxt artıq olmur.

M ü n d ə r i c a t

Giriş **3**

Fəsil I

Sahibkarlığa təhlükələr və hədələr.................... **5**

1.1. İqtisadi hədələr... **6**

1.2. Sosial hədələr.. **22**

1.3. İnformasiya hədələri... **22**

1.4. Korrupsiya sahibkarlığa hədə amili kimi.............. **24**

1.5. Hüquqi hədələr... **26**

1.6. Kriminal hədələr **28**

1.7. Təsərrüfat cinayətkarlığı **31**

1.8. Siyasi hədələr **32**

1.9. Kiçik sahibkarlığın təhlükəsizliyinin real vəziyyəti **33**

Fəsil II

Lhğğukışnf ğcüıışıüdükştşt eürdcküışədşnşt eüğşt uvşdğüıştşt üıfı şıeşyfğüedükş **38**

2.1. Rcyqyş ğcrfaşəü **39**

2.2. Eüjkşdfeş ğcrfaşəü **43**

2.3. Ğcrütvşı-euçtşkş ğcrfaşəü **51**

2.4. Ğcüıışıütşt eürdcküışədşnştşt eüğşt uvşdğüıştşt qtşmukıfd eüvişkdükş **53**

Fəsil III

Kommersiya müəssisəsinin təhlükəsizlik konsepsiyasının əsas müddəaları **54**

3.1. Təhlükəsizlik sisteminin məqsəd və vəzifələri....... **58**

3.2. Müdafiə obyektləri **60**

3.3. Kommersiya müəssisəsinin maraqlarına təhlükənin əsas növləri **61**

3.4. Təhlükəsizliyin idarə edilməsi **63**

3.5. Təhlükəsizliyin mühəndis-texniki təminatı **67**

Fəsil IV

Firmanın təhlükəsizlik xidməti **74**

4.1. Təhlükəsizlik xidmətinin əsas vəzifələri **75**

4.2. Təhlükəsizlik xidmətinin ümumi funksiyaları........ 76
4.3. Təhlükəsizlik xidmətinin tərkikbi 78
4.4. Təhlükəsizlik xidməti əməkdaşlarının hüquqları, ödəlikləri və məsuliyyətləri 82
4.5. Təhlükəsizlik xidmətinin ştatdankənar strukturları.. 83
4.6. Təhlükəsizlik xidmətinin fəaliyyətinin avtomatlaşdırılması.. 84
4.7. Təhlükəsizlik xidmətinin hüquq-mühafizə orqanları ilə qarşılıqlı hərəkətinin prinsip və istiqamətləri.......... 85
4.8. Təhlükəsizliyin idarə edilməsi 87
4.9. Təhlükəsizlik xidmətinin rəisi 90
Fəsil V
Təhlükəsizlik xidmətinin rejim və mühafizə şöbəsi.. **95**
5.1. Obyektdaxili rejimin tələbləri 96
5.2. Buraxılış rejimi 98
5.3. Stasionar obyektlərin mühafizəsinin təmin edilməsi.. 104
5.4. Mühafizə rejimi 108
5.5. Mühafizəçilər...................... 112
5.6. Maliyyə vəsaitlərinin mühafizəsi........................ 114
5.7. İnkassasiya şöbəsi.................................... 117
5.8. Heyətin təhlükəsizliyinin təmin edilməsi............... 122
Fəsil VI Kadrlar şöbəsi................................... **127**
6.1. Məxfi informasiya ilə işləməyə buraxılmış əməkdaşlarla işin xüsusiyyətləri 127
6.2. Məxfi informasiya ilə işləməyə buraxılmış şəxslərin şəxsi işlərinin aparılması qaydası 129
Fəsil VII
Xüsusi şöbə. Kommersiya sirrinin təhlükəsizliyinin təmin edilməsi.. **135**
7.1. Kommersiya sirri... 137
7.2. Kommersiya sirri sayılan informasiyanın və onun «həyat» müddətinin müəyyən edilməsi qaydası.......... 139
7.3. Məxfi informasiyaya qanunsuz yiyələnmə üsulları.. 142
7.4. Konfidensial informasiyaya mütəxəssislərin bura-

xılma qaydası…………………………………………. 149
7.5. Qapalı müzakirələr və danışıqların keçirilmə qaydası……………………………………………………... 161
7.6. Konfidensial sənədlərin arxivdə saxlanılmasının təşkili………………………………………………….. 161
Fəsil VIII
Mühəndis-texniki təhlükəsizlik şöbəsi……………... 164
8.1. Təşkilati tədbirlər ………………………………….. 164
8.2. Təşkilati-texniki tədbirlər ………………………….. 165
8.3. Texniki tədbirlər …………………………………… 165
8.4. Texniki vasitələrin köməyilə informasiyanın icazəsiz əldə edilməsinin qarşısının alınması üzrə tədbirlər .. 166
8.5. Qorunan binaların attestasiyası ………………….. 168
Nəticə.. 169

Uçebnoe izdanie

Əroçkin Vladimir İvanoviç
Buzanova Əna Valerğeva

OSNOVI BEZOPASNOSTİ BİZNESA
İ PREDPRİNİMATELĞSTVA

Çapa imzalanıb20.02. 2008. Kağız formatı 60x84 1/16.
Həjmi 11ç.v. Sifariş 06 . Sayı 500.

" İqtisad Universiteti " nəşriyyatı.
AZ 1001, Bakı, İstiqlaliyyət küçəsi, 6

Qrant layihəsi əsasında qeyri-kommersiya
xarakterli nəşr