Xalidə Mehdi qızı AĞAYEVA, İ.f.d.dos.

İsrafil Ayaz oğlu QURBANOV
Azərbaycan Texnologiya Universitetinin magistrantı

İNSAN RESURSLARININ İDARƏ EDİLMƏSİNDƏ İNFORMASİYA TƏHLÜKƏSİZLİYİNİN ROLU VƏ TƏKMİLLƏŞDİRİLMƏSİ

Xülasə

İnformasiya sistemlərinin müasirləşdirilməsi və onların çatışmazlıqlarının aradan qaldırılması üçün informasiya texnologiyalarından istifadə edilmişdir. Bu, informasiya sistemlərini inkişaf etdirməyə, həyata keçirməyə və qorumağa kömək edən bir vasitədir. O, həmçinin biznes hədəflərinə və biznes məqsədlərinə çatmaq, eləcə də iş proseslərini optimallaşdırmaq üçün bir vasitə kimi istifadə olunur. Bu cür proseslərə təşkilatda insanların işə götürülməsi, öyrədilməsi, inkişafı və mükafatlandırılması daxil olmaqla insan resurslarının idarə edilməsi daxildir. Bu proseslər təşkilatın daxili proseslərinə, əsas səlahiyyətlərinə, müvafiq bazarlara və təşkilati struktura təsir göstərir. Bütün bunlar informasiya təhlükəsizliyi tələb edir. İnformasiya təhlükəsizliyinə nəzarət təşkilatdakı işçilərin və podratçıların öz öhdəliklərini dərk etmələrini, yerləşdirildikləri rollara uyğun olmalarını və təşkilatın saxladığı məlumatı mühafizə etmələrini təmin edir.

Açar sözlər: informasiya təhlükəsizliyi, təhlükəsizlik sistemi, korporativ mədəniyyət, kadrların idarə edilməsi, motivasiya mühiti

Giriş

İnsan resursları istehsalın, iqtisadi artımın və dövlətin rəqabət qabiliyyətinin əsas amili olmaqla cəmiyyətin müasir sənayeləşməsinin əsas xüsusiyyəti kimi çıxış edir. İstehsalın yeni formaları - innovativ texnologiyalar insan resurslarına olan tələbləri dəyişmiş, fərdin yüksək ixtisasına və onun işə yaradıcı yanaşmasına ehtiyac olduğunu vurğulamış, bu da öz növbəsində idarəetmə alətləri və üsullarında dəyişikliklərin əsasını qoymuşdur.

21-ci əsrdə insan resurslarının idarə edilməsi şirkətlərin idarə edilməsində müəyyənedici alətə çevrilir. Şirkət işçilərinin təhsil səviyyəsi, bacarıqları, həmçinin onların təcrübəsi və ixtisasları təşkilatın mövcud resurslardan istifadə etmək qabiliyyətini və işin yekun nəticələrini böyük ölçüdə müəyyən edir. Məhz bunu nəzərə alaraq, ən böyük beynəlxalq şirkətlərin korporativ idarəçiliyinin əsas istiqamətlərindən biri insan resurslarının idarə edilməsi nəzəriyyəsinin uğurla tətbiqi, postulat və müddəalardan istifadə, bacarıqların daim təkmilləşdirilməsi və bu sahədə təcrübənin toplanmasıdır.

İnsan resurslarının idarə edilməsi şirkətdə və ya təşkilatda insanların bizneslərinə rəqabət üstünlüyü əldə etmələrinə kömək etmək üçün onların effektiv və səmərəli idarə edilməsinə strateji və ardıcıl yanaşmadır.

Bu, işə götürənin strateji məqsədlərinə xidmət edən işçilərin performansını maksimuma çatdırmaq üçün nəzərdə tutulmuşdur. İnsan resurslarının idarə edilməsi, ilk növbədə, siyasət və sistemlərə diqqət yetirərək, təşkilatlar daxilində insanların idarə olunması ilə məşğul olur.

HR departamentləri işçilərin mükafatlarının dizaynına, işçilərin işə qəbuluna, təliminə və inkişafına, fəaliyyətinin qiymətləndirilməsinə və mükafatların idarə edilməsinə nəzarət etmək üçün məsuliyyət daşıyırlar, məsələn, əmək haqqı və işçilərin mükafatlandırma sistemlərinin idarə edilməsi kimi HR təşkilati dəyişikliklər, sənaye əlaqələri və ya təşkilati işlərin balanslaşdırılması ilə də əlaqəlidir. Kollektiv sövdələşmədən və hökumət qanunlarından irəli gələn tələblərlə təcrübələrə, yoxlamaq üçün kotirovkaya ehtiyac var[1.15].

İnsan resurslarının ümumi məqsədi təşkilatın insanlar vasitəsilə uğur əldə edə bilməsini təmin etməkdir. HR mütəxəssisləri təşkilatın insan kapitalını idarə edir və diqqətini siyasət və proseslərin həyata keçirilməsinə yönəldir. Onlar işçiləri tapmaq, işə götürmək, seçmək, öyrətmək və inkişaf etdirmək, habelə işçilərlə münasibətləri və ya faydaları saxlamaqda ixtisaslaşa bilərlər.

Təlim və inkişaf mütəxəssisləri işçilərin təlim keçməsini və davamlı inkişafı təmin edir. Bu, təlim proqramları, performans qiymətləndirmələri

və mükafat proqramları vasitəsilə həyata keçirilir. İşçi münasibətləri siyasətlər pozulduqda, məsələn, təzyiq və ya ayrı-seçkilik halları kimi işçilərin narahatlıqları ilə məşğul olur. İşçilərin müavinətlərinin idarə edilməsinə kompensasiya strukturlarının, valideyn məzuniyyəti proqramlarının, endirimlərin və işçilər üçün digər üstünlüklərin hazırlanması daxildir.

İnkişaf etməkdə olan insan resurslarının idarə edilməsi təcrübələri əsas diqqəti arxa plan yoxlamalarına, təlim və inkişafa, işəgötürən-işçi münasibətlərinə, məsuliyyət və hesabatlılığa və informasiya sistemlərinin təhlükəsizlik resurslarının monitorinqinə yönəldir. İnformasiya sistemlərinin təhlükəsizliyi informasiya təhlükəsizliyi layihələrini effektiv idarə etmək üçün təşkilatda müvafiq resursların və adekvat bacarıqların olmasını təmin edir.

İnformasiya təşkilat üçün mühüm resurs sayılır və onun uğurunun mühüm mənbəyidir. Müxtəlif ekoloji amillərin dəyişməsi, bazarda rəqabətin artması, müəssisələrin üzləşdiyi problemlərin mürəkkəbliyi ənənəvi üsullarla idarə edilməsi çətin olan nəhəng məlumatların toplanması və işlənməsi üçün alətlərə ehtiyacı artırır. Müəssisələr onlara rəqabət üstünlüyü verəcək strategiyalar axtarırlar. Belə strategiyalardan biri də şirkət daxilində informasiya sistemlərinin tətbiqidir. İnformasiya sistemi, rəqabət qabiliyyətini artıra və qərar qəbul etmək üçün daha yaxşı məlumat verə bilən komponentlər qrupudur [2.28].

Müəssisə idarəetmə informasiya sistemləri müəssisədə qərarların qəbulunu asanlaşdırmaq üçün lazım olan dəqiq, vaxtında, aktual və dolğun məlumatları təmin edir. Onlar müəssisənin funksiyalarının səmərəli və məhsuldar həyata keçirilməsinə, planlaşdırma və nəzarətə kömək edir. O, qərar qəbul edənlərə sistem və vəziyyətdən asılı olaraq öz seçimlərini etməyə imkan verən geniş çeşidli qərar alternativləri təqdim edir. Bu, hadisələrin daha tez-tez müsbət nəticələrini təmin edir.

Şirkətin informasiya sisteminin məqsədi lazımi məlumatları toplamaq və lazımi dəyişikliklərdən sonra qərar qəbul etmək, strateji nəzarət və ya qərarların icrası üçün məlumatı tələb edən şirkətin əməkdaşına ötürülməsini təmin etməkdir.

Beləliklə, menecerin fəaliyyəti müsbət nəticə əldə etmək üçün informasiya sisteminin imkanlarından istifadə etmək bacarığından asılıdır. Ümumi mənada, informasiya sistemi təşkilatda planlaşdırma, nəzarət, koordinasiya və qərar qəbulunu asanlaşdırmaq üçün təşkil edilmiş aparat, proqram təminatı, infrastruktur və təlim keçmiş kadrların məcmusudur. İstənilən xüsusi məlumat sistemi əməliyyatları, idarəetməni və qərar qəbulunu dəstəkləmək məqsədi daşıyır. Rəsmi məlumat sistemi, şirkətin ehtiyaclarına və şirkətin fəaliyyəti üçün zəruri olan məlumatların toplanması, saxlanması, istehsalı, yayılması proseslərinə uyğun olaraq qurulmuş məlumatların məcmusudur, şirkətin öz biznes funksiyalarını yerinə yetirməsi üçün zəruri olan qərarların qəbul edilməsi proseslərinə dəstək verir. strategiyasına uyğun olaraq aparılır. Qeyri-rəsmi informasiya sistemləri də vacibdir, lakin emal nəticəsi deyil; daha doğrusu, onlar təsadüfi məlumat verirlər. Bununla belə, qeyri-rəsmi informasiya kanallarının mövcudluğu, eləcə də onların sürəti diqqətdən kənarda qalmamalıdır. Bəzən onlar müəssisənin öz məqsədlərinə çatmaq üçün inkişaf etdirdiyi və istifadə etdiyi bir çox elementlərdən yalnız biri olan məlumatdan daha tez bir təşkilat vasitəsilə şayiələri yaya bilər və buna görə də, bu məqsədlərlə aydın şəkildə əlaqələndirilməlidir.

İnformasiya sistemləri çox vaxt mənfəətin artmasına səbəb olur. Müvəffəqiyyət həm informasiya sistemlərinin tətbiqi bacarığından, həm də onlardan biznes tərəfdaşları ilə əlaqələr və ya üstün bazar seqmenti bilikləri kimi digər firma resursları ilə birlikdə istifadə edilməsindən asılıdır.

İnsan kapitalı hər bir cəmiyyətin və ölkənin əsas inkişaf meyarlarından biri olmaqla yanaşı, ölkələrin beynəlxalq sahədə əsas silahıdır. Son illərdə Azərbaycanda insan kapitalının inkişafının təmin edilməsi sahəsində görülən işlər ölkə daxilində bir sıra əhəmiyyətli sahələr üzrə səriştəli və peşəkar mütəxəssislərin yetişdirilməsinə vasitə olmuşdur.

İnsan amili müəssisələrin, xidmətlərin, sistemlərin, məlumatların təmin edilməsi, qorunması səylərinin uğur və uğursuzluğuna böyük təsir göstərir [2.56].

Tərtibatçı sistemin təhlükəsizliyini nəzərdən qaçırarsa, İT sistemi həssas olur və təcavüzkar tərəfindən istismar edilə bilər. Sosial mühəndislik hücumçuları insanların zəifliklərini - yəni insanların xüsusiyyətləri və davranışlarına görə təşkilatdakı zəiflikləri hədəf alaraq həssas məlumatları əldə etməyə çalışırlar.

Bu məqalənin məqsədi informasiya təhlükəsizliyi sahəsində insan amilini təhlil etmək, informasiya təhlükəsizliyi anlayışının bu çatışmazlıqları aradan qaldırmaq üçün necə əsas vasitəyə çevrilə biləcəyini təhlil etməkdir.

İnsan resurslarının idarə edilməsi təşkilatlarda işə qəbul, təlim, yüksəliş, sosial təminat xidmətləri, fəaliyyətin qiymətləndirilməsi, əmək haqqının idarə edilməsi və kollektiv söv-dələşmələr və işçilərin saxlanılması kimi inzibati HR funksiyalarını yerinə yetirməklə mühüm rol oynayır. HRM təcrübələri daha yüksək işçi performansı əldə etmək üçün strateji alətlərdir. Təşkilatların qarşıya qoyulmuş məqsədlərinə çatmasında işçilərin bilik və bacarıqlarına investisiya qoymaq üçün strateji planlar çox vacibdir. İnsan resurslarının idarə edilməsi təcrübələri cari işçi qüvvəsinin potensialının ölçülməsində və insan resurslarından ehtiyatlı istifadənin qiymətləndirilməsində strateji olmalıdır. Buna görə də, təşkilatların işçi qüvvəsinə sərmayə qoymaqla insan kapitalını təşkilatın strateji planlaşdırmasına daxil etmələri vacibdir [3.17].

Güclü təhlükəsizlik nəzarəti olmadan bizneslər maliyyə itkisi, hüquqi məsuliyyət, nüfuza zərər və milli təhlükəsizliyə təsir ehtimalı riskini daşıyır. Buna görə də, inkişaf etməkdə olan informasiya sistemlərinin təhlükəsizliyi araşdırmaları, işçiləri insan resurslarının idarə edilməsi təcrübələrindən istifadə edərək daha təhlükəsiz təhlükəsizlik davranışları ilə məşğul olmağa həvəsləndirərək təşkilati təhlükəsizliyi yaxşılaşdırmağın yollarını kəşf edir. İnformasiya təhlükəsizliyi idarəetmə sistemi informasiya texnologiyaları ilə əlaqədar risklərlə bağlı siyasətlər toplusudur. İnformasiya təhlükəsizliyi idarəetmə sistemi müxtəlif təhlükəsizliklə bağlı təhdidlərin və zəifliklərin təşkilata göstərə biləcəyi təsirləri aradan qaldırmaq və ya minimuma endirmək üçün müvafiq tədbirlərin həyata keçirilməsini hədəfləyir.

İnformasiya sistemlərinin təhlükəsizliyi və məlumatların məxfiliyi üzrə təlimlər təşkilatın informasiya ehtiyatlarının qorunması üçün kritik nəzarət rolunu oynaya bilər, təşkilatlarda informasiya təhlükəsizliyi insidentlərinin əsas səbəbləri kimi işçilərin məlumatsızlığını, səhlənkarlığını, müqavimətini, itaətsizliyini, laqeydliyini və yaramazlığını müəyyən edir.

İnformasiya texnologiyalarının artan təhdidləri yeni texnologiyaya əsaslanan həllərin yaranmasına səbəb olur, insan faktorları ilə bağlı tədqiqatlar isə məhduddur. Təşkilatlar çox vaxt insan amilinə əhəmiyyət vermirlər. Cisco Systems-in təhlükəsizlik araşdırması göstərdi ki, uzaqdan işləyən istifadəçilər hələ də təhlükəsizliyi təhdid edən fəaliyyətlərlə məşğul olacaqlar. İşçilərin davranışı ilə bağlı araşdırma göstərdi ki, şübhəli e-məktub aldıqdan sonra 37% yalnız e-poçtu açmır, həm də linkə klikləyir, 13% isə əlavə edilmiş faylı açır. Bundan əlavə, adi e-məktub aldıqdan sonra 42% keçidə klikləyərək məxfi məlumat verdi, 30% isə kompüterin işini yaxşılaşdıracağı güman edilən faylı açıb [4.95].

Növbəti bir neçə ay ərzində onların əsas prioritetlərini müəyyən etmək üçün təhlükəsizlik mütəxəssisləri və İT departamentləri arasında sorğu keçirilib.

Respondentlərin təxminən 44%-i İT və təhlükəsizlik komandalarının vaxtlarının 20%-dən azını gündəlik əməliyyat təhlükəsizliyinə sərf etdiyini bildirib. Digər 32 faiz isə vaxtlarının 20-40 faizini təhlükəsizliyə həsr etdiklərini bildirib. İştirakçıların yalnız 20 faizi gündəlik və həftəlik inzibati fəaliyyətlərinin əhəmiyyətli bir hissəsini sistemlərinin və şəbəkələrinin təhlükəsizliyinə həsr etmişdir.

İnsan və təşkilati amillər texniki informasiya təhlükəsizliyi ilə bağlı ola bilər.

Kompüter təhlükəsizliyinə təsir edən amillər insan faktoru və təşkilati faktor olmaqla iki kateqoriyaya bölünür. İnsan faktorları digər amillərdən daha vacibdir.

Onlar aşağıdakı qruplara bölünür:

1. İdarəetmə ilə əlaqəli amillər, yəni işçilərin iş yükü və zəif fəaliyyəti;
2. Son istifadəçi amilləri.

Aşağıda biz istifadəçi davranışına əhəmiyyətli təsir göstərən dörd insan amilinə diqqət yetirəcəyik.

1. Motivasiyanın olmaması

Bir çox təşkilatlar hesab edir ki, işçilər informasiya aktivləri ilə təhlükəsiz davranmaq üçün motivasiya edilməlidir və rəhbərlik onların işçilərini nəyin motivasiya etdiyini müəyyən edə bilməlidir.

2. Şüurun olmaması

Şüurun olmaması hücumlar haqqında ümumi məlumatın olmaması ilə əlaqələndirilir. Məlumatsızlığın ümumi nümunələri ola bilər: istifadəçilər casus proqramları necə müəyyənləşdirəcəklərini və güclü parol təmin etməyin vacibliyini bilmirlər.

Onlar nə şəxsiyyət oğurluğundan, nə də digər istifadəçilərin kompüterlərinə girişinə nəzarət edə bilmirlər.

3. İnandırma

Riskli inancların ümumi nümunələri bunlardır: istifadəçilər antivirus proqramının quraşdırılmasının onların informasiya təhlükəsizliyi problemlərini həll etdiyinə inanırlar.

4. Texnologiyadan savadsız istifadə

İnsanların davamlı əməkdaşlığı və bu texnologiyadan səmərəli istifadə etmədən ən yaxşı texnologiya belə informasiya təhlükəsizliyi problemlərinin həllində uğur qazana bilməz. Texnologiyadan sui-istifadənin ümumi nümunələri aşağıdakılardır: sistemlərin icazəsiz yenidən konfiqurasiyası, başqalarının parollarına daxil olmaq, etibarsız məlumatların əldə edilməsi. Kompüter təhlükəsizliyi riskləri bir neçə yolla imtiyazların artırılması, səhvlər və nöqsanlar, xidmətdən imtina, sosial mühəndislik, icazəsiz giriş, şəxsiyyət oğurluğu, fişinq, zərərli proqram və icazəsiz surətlər kimi təsnif edilə bilər [4.98].

İnsan Resursları departamentləri kibertəhlükəsizlik prosedurlarında həlledici rola malik ola bilər, onların əməkdaşları haqqında məlumatların idarə edilməsini nəzərə alırlar. İnsan resurları departamentləri də işçilərin davranışlarına çox təsir edir və onların işi vasitəsilə kibergigiyena davranışlarına təsir göstərə bilər.

Haker bir kod sətri yazmadan verilənlər bazanıza və maliyyə əməliyyatlarınıza giriş əldə edə bilər. Onların etməli olduğu yeganə amil əsas işçini aldatmaq və parolları onlara verməkdir. İnsanlar kibertəhlükəsizliklə bağlı bir çox məsələdə əsas amil olduğundan, hər bir amili nəzarətdə saxlamaq insan resurları departamentinin işidir.

İnsan resursları departamentləri öz işlərində bu cür həssas məlumatlarla məşğul olduqlarına görə, öz işçiləri üçün düzgün mühafizə üsullarını başa düşmək və icra etmək məsuliyyəti olmalıdır.

Yaxşı nəzarət tədbiri fon identifikasiyası və işə qəbul üçün bütün müraciət edənlərin səriştələrinin yoxlanılmasını əhatə edir. Bütün müvafiq qaydalar və etika nəzərə alınmalı, biznes tələblərinə, yəni əldə ediləcək məlumatın təsnifatı və əlaqədar risklərə uyğun olmalıdır. HR, təsadüfi və ya zərərli təhdidlərin ehtimalını azaldacaq şəkildə təşkilatda məşğulluq müavinətlərinin bütün mərhələlərinə nəzarət edir. Risklərin qarşısını almaq üçün ardıcıl olaraq prosedurların olması vacibdir. İdeal olaraq, bu, təşkilatın ümumi işə qəbul prosesi ilə əlaqəli olacaqdır [5.32].

İşçilər və podratçılarla bağlanmış müqavilədə onların və təşkilatın informasiya təhlükəsizliyi ilə bağlı öhdəlikləri göstərilməlidir. Bu müqavilə vacibdir və qanuni əhəmiyyət daşıyan ümumi və fərdi öhdəlikləri ehtiva edir.

Bütün işçilər və əlaqəli podratçılar işlərini yaxşı və təhlükəsiz şəkildə yerinə yetirmək üçün müvafiq məlumatlılıq təhsili və təlim almalıdırlar. Onlar dəyişdirildikdə təşkilati siyasət və prosedurlarda ardıcıl yeniliklər almalıdırlar, həmçinin öz rollarında onlara təsir edən müvafiq qanunvericiliyə yaxşı baxmalıdırlar. Hər bir təşkilat təlim və uyğunluğun nəzərdən keçirildiyini sübut etməli, işçilərə və podratçılara başa düşmək üçün ən yaxşı şans verməklə təlim və maarifləndirmənin necə aparıldığını qeyd etməlidir.

İşə xitam verildikdən və ya iş müddəti ərzində dəyişdirildikdən sonra etibarlılığını davam etdirən informasiya təhlükəsizliyi vəzifə və öhdəlikləri aydın olmalı, işçilərə və ya podratçılara çatdırılmalı və həyata keçirilməlidir. İşlərə təşkilata aid olan məlumatların öz daxilində saxlanması və gizli saxlanılması daxildir.

İşçi və ya podratçı təşkilatı tərk etdikdən sonra məlumatın qorunub saxlanmasını təmin etmək vacibdir, çünki insanlar özləri məlumat mağazalarında gəzirlər. Müqavilənin şərtləri bunu vurğulamalı və məzuniyyətin müqaviləsinə xitam vermə prosesi fərdlərə, hətta ayrıldıqdan sonra da təşkilat qarşısında öhdəliklərinin olduğunu xatırlatmalıdır.

İşdən çıxma və işdən çıxma ilə yanaşı, əgər işçi rolları dəyişirsə, məsələn, əməliyyatdan satışa keçərsə, onların yeni rolunda məcburi olmayan məlumat aktivlərinə artıq çıxışı olmaması təmin edilməlidir.

İnsan resurslarının idarə edilməsində informasiya təhlükəsizliyinin rolu və təkmilləşdirilməsi üçün HR-ın kibertəhlükəsizlik təliminə və prosedurlarına daxil edilməsi əsas amil sayılır:

1. Ofisdə kibertəhlükəsizlik mədəniyyəti yaratmaq
2. Daha əhatəli kibertəhlükəsizlik siyasətinin hazırlanmasına kömək etmək
3. İşçilərin qeydləri ilə bağlı riskə məruz qalma səviyyəsini müəyyən etmək
4. İşçiləri kibertəhlükəsizlik riskləri ilə bağlı maarifləndirmək

5. Daxili hücumlara qarşı əlavə qorunma qatı əlavə etmək

İnsan resursları departamentlərinə gəldikdə, informasiya təhlükəsizliyi ilə bağlı görüləcək ən vacib amil reaktiv olmaqdan daha çox fəal olmaqdır [5.37].

Nəticə

Texnologiya və pozuntular potensialı bu gün biznesin hər tərəfində üstünlük təşkil edir. İşçilərin məlumat itkisi və bunun qarşısının alınması barədə məlumatlı olduğundan əmin olmaq üçün İT departamentinizə etibar etmək kifayət deyil.

Təşkilat işçilərin məlumatların təhlükəsizliyində rolları barədə məlumatlandırılması üçün təlimlərin keçirilməsini təmin etməlidir. Onlar təhlükəsizlik protokollarının nə olduğunu, güclü parolların necə hazırlanması və istifadə olunacağını, eləcə də, problemdən şübhələndikdə və ya biznes üçün istifadə etdikləri cihazı itirdikdə prosesin nə olduğunu bilməlidirlər.

İnsan Resursları mütəxəssisləri işçilərin təhlükəsizlik siyasətlərinə riayət etmələrini təmin etmək üçün məsuliyyət daşıyırlar. İnsan resursları departamenti informasiya təhlükəsizliyi siyasətlərinin düzgün təqdim edilməsini, sənədləşdirilməsini, çatdırılmasını və tətbiq edilməsini təmin etmək üçün vacibdir.

ƏDƏBİYYAT SİYAHISI:

1. James Riddle. Devolutions. “Kibertəhlükəsizlikdə HR-nin rolu nədir və bu niyə vacibdir?” 31 iyul 2019-cu il. https://blog.devolutions.net/2019/07/whats-the-role-of-hr-in-cybersecurity-and-why-is-it-important

2. Net At Work Komandası. İşdə Net. “Kibertəhlükəsizlik Təhdidlərinin Azaldılmasında HR-nin Rolu”. https://www.netatwork.com/the-role-of-hr-mitigating-cyber-security-threats/

3. İqtisadiyyatda informasiya sistemləri: dərslik, red. G.A. Titorenko, 2-ci nəşr, M.: 2008, - 463s.

4. “İnformasiya texnologiyaları”. Dərslik, red. V. V. Trofimova. M.: Yurayt nəşriyyatı, 2011, 624s.

5. Bazarov T. Y. “Kadrların idarə edilməsi”. V nəşr, stereotipik. M.: Akademiya, 2007. - 224 s.

Халида Мехди кызы Агаева, PhD, доцент
Исрафил Аяз оглы Гурбанов
Азербайджанский Технологический Университет

Роль и совершенствование информационной безопасности в управлении человеческими ресурсами

Резюме

Информационные технологии использовались для модернизации информационных систем и устранения их недостатков. Это инструмент, который помогает разрабатывать, внедрять и поддерживать информационные системы. Он также используется в качестве инструмента для достижения бизнес-целей и бизнес-задач, а также для оптимизации бизнес-процессов. Такие процессы включают управление человеческими ресурсами, в том числе набор, обучение, развитие и компенсацию людей в организации. Эти процессы влияют на внутренние процессы организации, основные компетенции, соответствующие рынки и организационную структуру.

Все это требует информационной безопасности. Средства контроля информационной безопасности гарантируют, что сотрудники и подрядчики в организации понимают свои обязанности, соответствуют ролям, в которые они входят, и защищают информацию, хранящуюся в организации.

Ключевые слова: информационная безопасность; система безопасности; корпоративная культура; Управление персоналом; мотивационная среда

Khalida Mehdi Aghayeva, PhD, assoc.prof.
Israfil Ayaz oglu Gurbanov
Azerbaijan Technology University

The role and improvement of information security in human resource management

Summary

Information technologies were used to modernize information systems and eliminate their shortcomings. It is a tool that helps to develop, implement and maintain Information Systems. It is also used as a tool to achieve business goals and business objectives as well as to optimize business processes. Such processes include the management of human resources, including the recruitment, training, development and compensation of people in the organization.

These processes affect the organization's internal processes, core competencies, relevant markets and organizational structure. All this requires information security. Information security controls ensure that employees and contractors in the organization understand their responsibilities, are appropriate for the roles they are placed in, and protect the information held by the organization.

Key words: information security; security system; corporate culture; personnel management; motivational environment