величиною витрат на виготовлення товару, рівень цін багато в чому повинен враховувати психологічне сприйняття покупцем і можливу подальшу поведінку при зіставленні параметрів ціна/цінність [2].

Найбільш ефективна така цінова політика, яка не лише служить інструментом загальної ринкової політики підприємства, але й спрямована на облік усіх можливих вимог потенційних споживачів з точки зору формування і застосування ціни. На перше місце в цьому випадку виходить оцінка корисності продукту і умов його споживання.

При розробці цінової політики підприємства в сучасних умовах господарювання необхідно спиратися на методи з орієнтацією на попит: головним орієнтиром в цьому методі є споживач, його споживчі очікування і можливості обліку аспектів психології цін.

Таким чином, формування ефективної цінової політики підприємства як частини короткострокової фінансової політики повинні забезпечити не лише поточне виживання організації, максимізацію поточного і майбутнього прибутку, завоювання лідерства на ринку але й враховувати економічну ситуацію в країні, її вплив на цінову політику, а також можливості громадян купувати продукцію. Грамотне ціноутворення - найважливіша умова підвищення ефективності діяльності підприємства і дієвий механізм, що дозволяє при обґрунтованому застосуванні підвищити рівень життя громадян в державі, та якісно поліпшити споживчий кошик населення.

Література:

1. Балабанова Л. В., Митрохіна Ю. П. Управління збутовою політикою. Київ : Центр учбової літератури, 2017. 240 с

2. Вачевський М. В. Долішній М. І., Скотний С. Г. Маркетинг для менеджера. Київ : Просвіта, 2016. 139 с.

UNİVERSİTETDƏ İNFORMASİYA TƏHLÜKƏSİZLİYİNİN TƏMİNATINA DAİR

Leyla İsmayılzadə
Mingəçevir Dövlət Universiteti, Azərbaycan

Bu gün İnternetdən geniş isitfadə olunduğu və kommunikasiyaların sürətli inkişaf etdiyi bir dövrdə yaşayırıq: bununla əlaqədar gündəlik həyatımıza – əmək fəaliyyətimizə, məişətimizə yeni texnika və texnologiyalar daxil olur və buna uyğun olaraq, nitqimizdə də yeni anlayşlardan, yeni ifadələrdən istifadə edirik. Hamımız üçün artıq "hakerlər", "məlumatların pozulması", "kiber fırıldaqçılıq", "informasiyanın qorunması", "informasiya təhlükəsizliyi", "İT təhlükəsizliyi", "kibertəhlükəsizlik" kimi anlayışlar tez-tez işlətdiyimiz ifadələrə çevrilmişdir.

Bununla bağlı bir məqama diqqət yetirmək və dəqiqləşdimə aparmağı vacib hesab edirik: bu anlayışların tərifləri necədir, onlar arasında oxşarlıq və fərq nədir? Cavab belədir ki, hal-hazırda, bir qayda olaraq, bu anlaşıyları bərabərləşdirirlər, lakin kibertəhlükəsizliyə nisbətən, informasiya təhlükəsizliyi məlumatların qorunmasının

təmin edilməsinə daha kompleksli yanaşmanı əhatə edə bilər. Bir misal göstərək. Təsəvvür edək ki, hava limanında rəhbər şəxsdən mühüm məlumatların olduğu sərt disk və ya fləş-kart oğurlanıb. Mahiyyət etibarilə, əslində, məlumat oğurlanıb, lakin oğurluq üsulu rəqəmsal deyil, adidir, klassikdir. Bu məsələyə kibertəhlükəsizlik rəhbərinin nöqteyi-nəzərindən baxsaq, deyə bilərik ki, bu, onun məsuliyyət dairəsindən kənardadır, belə ki, heç bir İT sistemi sındırılmayıb, sadəcə, fiziki hücum baş verib. Lakin bu situasiyaya məhz "klassik" informasiya təhlükəsizliyi baxımından baxsaq, onda insident göz qabağındadır – rəqəmsal formada olan məlumatlar oğurlanıb və oğurluq üsulu artıq ikinci dərəcəli məsələdir.

Beləliklə, kibertəhlükəsizlik məhz texniki mühafizə tədbirləri, informasiya təhlükəsizliyi isə hər üç aspekt üzərində cəmləşmişdir. Buna görə də, ümumiyyətlə, deyə bilərik ki, kibertəhlükəsizlik İT-təhlükəsizliyinin sinonimi olsa da, informasiya təhlükəsizliyi və ya onun sinonimi – informasiyanın mühafizəsi ilə müqayisədə daha kiçik məsuliyyət və vəzifələr dairəsini ehtiva edir.

İT-nin bu qədər sürətlə inkişaf etməsi və həyatımıza durmadan nüfuz etməsinə baxmayaraq, bu gün universitet tələbələrinin gözləntiləri ilə təhsil müəssisələrinin onlara təklif edə biləcəyi imkanlar arasında hələ də ciddi fərqlər var. Ali təhsildə iş üsulları sosial dəyişikliklərə və texnoloji inkişafa uyğun olaraq daim təkmilləşdirilməlidir. Eyni zamanda, həm tədris materiallarının və digər məlumatların, həm də İT infrastrukturunun özünün təsadüfi və ya hədəflənmiş hücumlardan qorunmasının təmin edilməsi aktual məsələ olaraq qalır.

Universitetlərdə informasiya təhlükəsizliyinin təminatı sahəsində qarşıya çıxan problemləri aşağıdakı kimi təsnifatlaşdırmaq olar:

1-ci problem: müxtəlif istifadəçi qrupları

Müasir universitet və onun şəbəkəsi müxtəlif istifadəçi qruplarının maraqları və məlumatlarının toqquşduğu bir mühitdir. Universitet şəbəkəsində informasiya təhlükəsizliyi üzrə müxtəlif tələbləri olan istifadəçilərin aşağıdakı kateqoriyalarına rast gəlmək olar: universitet tələbələri və universitetə mübadilə yolu ilə gəlmiş tələbələr (əsasən əcnəbilər); müəllimlər və rəhbərlik; universitetin təklif etdiyi ödənişli kurslara və ixtisasartırma kurslarına gələnlər, eləcə də universiteti kommersiya sifarişləri ilə təmin edən təşkilatların nümayəndələri.

2-ci problem: giriş metodlarının transformasiyası və "İstənilən qurğu" konsepsiyası

Universitetin ənənvi şəbəkəsinin sərhədləri yoxa cıxdıqca və universitet mühiti tədricən sərhədlərini itirdikcə, smartfonlar, planşetlər, digər terminal qurğular və veb tətbiqləri dünyanın istənilən yerindən – universitetin auditoriyalarından, yataqxanasından, şəxsi evdən, kampusundan, tələbələrin təcrübə mübadiləsi üçün getdiyi digər universitetdən və s.-dən tədris materiallarına daxil olmaq imkanı verən tədris prosesini dönməz şəkildə dəyişir.

Eyni zamanda, "İstənilən qurğu" konsepsiyası tətbiq edilərkən informasiya təhlükəsizliyi ilə bağlı bir sıra məsələlər ortaya çıxır. Bu halda aşağıdakıları təmin etmək lazımdır:

- şəbəkə abunəçi qurğularının: stasionar kompüterlərin (iş stansiyaları və ya iş stansiyaları), noutbukların (mobil iş stansiyaları), mobil qurğuların (Android və iOS

sistemləri ilə işləyən planşet kompüterlər), şəbəkə printerlərinin və IP-telefonların universitet şəbəkəsinə icazəsiz qoşulmasının qarşısının alınması;

- informasiya təhlükəsizliyi üzrə mövcud tələb və tövsiyələrinin yerinə yetirilməsi, o cümlədən universitet şəbəkəsinə qoşulmuş mobil cihazların informasiya təhlükəsizliyi üzrə mövcud tələblərə cavab verib-vermədiyinə məsafədən nəzarətetmə imkanlarının təmin edilməsi;

- bundan əlavə, müxtəlif istifadəçi qruplarının abunəçi cihazlarını, həmçinin mobil qurğuları (Android və iOS ilə işləyən planşet kompüterləri) şəbəkəyə qoşmaq üçün qonaq zonalarını və məhdud giriş zonalarını bir-birindən ayrılması, bu məqsdlə mövcud infrastrukturu (yəni mövcud şəbəkənin seqmentlərə bölünməsini) dəyişdirmədən universitet şəbəkəsinin təhlükəsizlik zonalarına məntiqi bölünməsinin təşkili təmin edilməlidir.

3-cü problem: informasiya sistemlərinin və əlçatanlığı məhdudlaşdırılmış məlumatların qorunması

Müasir universitet qorunması tələb olunan müxtəlif məlumatların anbarıdır. Bu məlumatlar aşağıdakı kimi qruplaşdırmaq olar:

· Tələbələrin, müəllimlərin, rəhbərliyin və digər kateqoriyalı istifadəçilərin şəxsi məlumatları;

· Universitetin kommersiya sirrini təşkil edən və onun daha yaxşı təhsil və təhsil proqramları, eləcə də daha mütərəqqi tədris metodları ilə təminatı sahəsində digər universitetləri qabaqlamağa imkan verən məlumatlar;

· Universitet tərəfindən işlənib hazırlanmış tədris materialları, onlara giriş ya məhdud, ya da nəzarət altında olmalıdır, belə ki, onlar əqli mülkiyyət hesab olunur;

· Universitet tərəfindən alınmış proqram təminatı və ya lisenziyalar, bunların oğurlanması rəqabət mübarizəsində təhsil müəssisəsinin vəziyyətini pisləşdirə bilər və yaxud cinayət məsuiyyətinə və ya inzibati məsuliyyətə gətirib çıxara bilər.

- Nəhayət, universitetin kommersiya və ya dövlət müştərilərinin sifarişi ilə həyata keçirə biləcəyi elmi-tədqiqat layihələrinin nəticələri qorunmalıdır.

Əlçatanlığı məhdud olan məlumatların qorunması ilə yanaşı, tədris prosesinin informasiya sistemlərinin təhlükəsizliyi də təmin edilməlidir. Bu sistemlərin təsadüfən və ya qəsdən sıradan çıxarılması tədris prosesini poza bilər.

4- cü problem: təhdidlərin sayının artması

Şəbəkə təhlükəsizliyinə təhdidlər mühiti daim inkişaf edir. Bu mühitdə aparıcı mövqeləri ənənəvi üsul və qorunma vasitələrinə getdikcə daha çox qalib gəlməyə nail olan xüsusi olaraq yazılmış, gizli təhdidlər tutur. Bu təhdidlər şəbəkənin içərisinə nüfuz edir: nüvə səviyyəsində, paylaşma səviyyəsində, təhlükədən qorunma və görünmənin minimum səviyyədə olduğu istifadəçi girişi səviyyəsində. Oradan bu təhlükələr asanlıqla öz hədəflərini - konkret resursları və hətta universitetdəki konkret insanları seçir. Müasir kibertəhlükələrin məqsədi şöhrət və şöhrət qazanmaq, hətta gəlirli botnet yaratmaq deyil, rəqabət üstünlüyünə nail olmaq üçün əqli mülkiyyət və ya kommersiya və digər sirləri ələ keçirmək və oğurlamaqdır.

Universitetlər bu təhdidlərdən özlərini qorumaq üçün həyata keçirməli olduğu əsas tədbirlər üzləşə biləcəkləri riskləri tam müəyyənləşdirmək, bu riskləri azaltmaq və ya yumşaltmaq üçün qabaqlayıcı tədbirlər görmək, nəzarətetmə mexanizmi işləyib hazırlamaq və tətbiq etməkdir. “İnformasiya Texnologiyaları - Təhlükəsizlik

Texnologiyaları - İnformasiya Təhlükəsizliyinə Nəzarət üçün Təcrübə Kodeksi" adlanan ISO 27002 Beynəlxalq standartı bu sahədə bir sıra nəzarət vasitələrini ehtiva edir.

Statistik məlumatlar göstərir ki, son illər kiberhücumlar daha tez-tez baş verir. Bu da bütün təşkilatlar kimi, alitəhsil müəsssisələrini də yüksək kvalifikasiyalı mütəxəssisləri işə götürməyə vadar edir. Bu isə real əmək bazarında sözügedən sahədə peşəkarların tapılmasını olduqca çətinləşdirir. Müvafiq tədbirlər görmək zərurəti yaranıb. Bu zərurəti COVID-19 pandemiyası ilə bağlı yaranmış vəziyyət və uğurlu kiberhücumların sayının dəhşətli şəkildə artması bu zərurəti daha kəskinləşdirib. Kibertəhlükəsizlik sahəsində ali təhsilli kadr hazırlaığı kvalifikasiyalı işçi qüvvəsi yaradılması zərurəti ilə ayaqlaşa bilmir. Nə qədər qəribə olsa da, bu bir faktdır ki, belə kadr hazırlığını aparan universitetlər özləri də bu "defisit" ilə üz-üzə qalırlar.

Bunun səbəbləri çox və müxtəlifdir. Universitet səviyyəsində kibertəhlükəsizlik üzrə mütəxəssislərin sayı son illər ərzində durmadan artıb, lakin məzunların sayı hələ də sənayenin tələb etdiyi səviyyəyə çatmır. Yüksək kvalifikasiyalı mütəxəssislərin yetişdirilməsi xeyli vaxt tələb edən məsələdir, onların praktiki iş təcrübəsi əldə etmələri üçün daha çox vaxt lazımdır.

Sadalanan problemlərin həllinə nail olmaq üçün universitet ən azı üç məsələni həll etməlidir:

1) universitetin inzibati-texniki heyətində təşkilati təhlükəsizlik və əməliyyatların idarə edilməsi və dəstəklənməsi üzrə kvalifikasiyalı mütəxəssislər olmalıdır;

2) heyətdə təhlükəsizlik sistemləri, təhlükəsizlik proqram və alətləri hazırlaya bilən kibermühəndisləri olmalıdır;

3) universitetin hər bir təşkilati səviyyəsində kibertəhlükəsizlik haqqında ümumi məlumatlılıq olmalıdır ki, hər bir əməkdaş, hətta tələbə kibertəhdidlər və risklər barəsində baza biliklərinə malik olsun.

Bununla bağlı böyük çin filosofu Sun Tzu "Döyüş sənəti" adlı traktatından məşhur kəlamı xatırlatmaq yerinə düşür: "Əgər düşmənizi də, özünüzü də tanısanız, yüz döyüşdə qalib gələcəksiniz. Əgər özünüzü tanısanız, düşmənizi isə tanımasanız, onda gah qalib gələcəksiniz, gah da məğlub olacaqsınız. Əgər düşmənizi də, özünüzü də tanımırsınızsa, onda hər döyüşdə məğlub olacaqsınız."

26 əsr bundan öncə yazılsa da, yazıldığı dövr üçün olduğu qədər bu gün də aktuallığını saxlayan və tətbiq oluna bilən postulatdır! Bu, universitetdə informasiya təhlükəsizliyinin təminatına aiddir.