İNFORMATİKANIN TƏDRİSİ METODİKASI

UOT 372.800.4.02

Akif Padar oğlu Orucəliyev
fizika-riyaziyyat üzrə fəlsəfə doktoru, dosent
Dövlət Təhlükəsizliyi Xidmətinin Heydər Əliyev adına Akademiyası
https://orcid.org/0000-0003-3274-9502
https://doi.org/10.5281/zenodo.6449734

Nigar Mirzəbala qızı Məmmədova
müəllim
Dövlət Təhlükəsizliyi Xidmətinin Heydər Əliyev adına Akademiyası
https://orcid.org/0000-0002-1711-8035

İNFORMATİKA FƏNNİNİN TƏDRİSİNDƏ İNFORMASİYA TƏHLÜKƏSİZLİYİ VƏ İNFORMASİYANIN MÜHAFİZƏSİ HAQQINDA

Акиф Падар оглы Оруджалиев
доктор философии по физико-математическим наукам, доцент
Академия Службы Государственной Безопасности им. Г. Алиева

Нигяр Мирзабала гызы Мамедова
преподаватель Академии Службы Государственной Безопасности им. Г. Алиева

ОБ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ И ЗАЩИТЕ ИНФОРМАЦИИ ПРИ ПРЕПОДАВАНИИ ИНФОРМАТИКИ

Akif Padar Orujaliyev
doctor of philosophy in physical and mathematical sciences, associate professor
Academy of the State Security Service named after H. Aliyeva

Nigar Mirzabala Mammadova
lecturer at the Academy of the State Security Service named after H. Aliyeva

ON INFORMATION SECURITY AND INFORMATION PROTECTION WHEN TEACHING COMPUTER SCIENCE

Xülasə. Məqalədə təhsil müəssisələrində informasiya təhlükəsizliyinin həlli yolunun təyin edilməsi dövrümüzün mühüm problemlərindən birinin şüurlu şəkildə dərk edilməsi kimi nəzərdən keçirilir. İnformasiya texnologiyalarının imkanlarının sürətlə genişləndiyi bir şəraitdə kiberfəzada müxtəlif təhdid və təhlükələrlə qarşılaşa bilən şagirdlərin bu təhlükələrdən mühafizəsinin vacibliyi vurğulanır, texniki vasitələrdən istifadə zamanı müvafiq qayda və qanunların şüurlu dərk edilməsinin zəruriliyi qeyd edilir. Belə bir şəraitdə ən mühüm məsələlərdən biri də ondan ibarətdir ki, informatika fənnini tədris edən müəllimlərin üzərinə böyük məsuliyyət düşür və onlar müəllim hazırlığı üçün zəruri tələblərə cavab verməlidirlər.

Açar sözlər: *informasiya, informasiya təhlükəsizliyi, informasiya texnologiyaları, kiberfəza, informatika*

Резюме. В статье рассматривается обозначение пути решения информационной безопасности в образовательных учреждениях как осознанное понимание одной из важных проблем нашего времени. Далее подчеркивается важность защиты учащихся от различных угроз и опасностей, которым они могут подвергаться в киберпространстве, при условиях стремительного развития возможностей информацио-

нных технологий, а также отмечается необходимость сознательного понимания соответствующих норм и правил безопасности при применении технических средств. Один из самых важных вопросов при таких обстоятельствах заключается в том, что учителя, которые преподают информатику, несут большую ответственность и должны соответствовать необходимым требованиям для подготовки учителей.

Ключевые слова: *информация, информационная безопасность, информационные технологии, киберпространство, информатика*

Summary. The article discusses the importance of a conscious understanding of information security as a solution to one of the biggest problems of our time in educational institutions. In the context of the rapid spread of information technology capabilities, the importance of protecting a student in cyberspace from various threats and dangers is emphasized, as well as the need for a conscious understanding of technical means, relevant norms and rules. In such circumstances, one of the most important issues is that teachers who teach computer science have a great responsibility and the training of teachers must meet the necessary requirements.

Key words: *information, information security, information technologies, cyberspace, informatics*

İnformasiya texnologiyalarının və İnternetin insan həyatının bütün sahələrində, o cümlədən təhsil sferasında geniş miqyaslı tətbiqi, şagird potensialının maksimal realizasiyasını, onun təhsil və tərbiyəsinin, ləyaqətli həyat perspektivlərinin formalaşdırılmasını, eləcə də sosial pozitiv yaradıcılığının maksimallaşdırılmasını nəzərdə tutur. Bu məqsədin tələb olunan səviyyədə reallaşdırılması, yəni şagirdlər üçün tədrisi zəruri informasiyanı daha rahat şəkildə əldəetmə mühitinin yaradılması digər bir məsələni, daha dəqiq desək, şagird təhsil və tərbiyəsi ilə uyuşmayan informasiyanın yayıla bilməsi risklərinin də aktuallığını önə çıxarır. Bu risklərin yaratdığı təhdidlərə misal olaraq kiberfəzada mövcud ekstremist xarakterli kontentin, eləcə də böyüklər üçün nəzərdə tutulan kontentin yaratdığı təhdidləri, kiberbulinqi, fərdi verilənlərin mübadiləsini, tanımadığı adamlarla tanışlıq imkanlarını göstərmək olar. Bütün bunlar İnternetdən istifadə edən şagirdin təhlükəsizliyinə yarana bilən təhdidlərdir. Yüksək texnologiyaların tətbiqinin yaratdığı bu təhdidlər şagirdlərin arzuolunmaz kontent qarşısında mühafizəsini xüsusilə aktual edir. Dərkolunma prosesində olan şagirdin sonsuz informasiya mühitində ziddiyyətli, aqressiv və neqativ xarakterli informasiya ilə qarşılaşması onların sosial-mənəvi oriyentasiyasında ciddi pozuntular yarada bilər. Bu isə şagirdlərin mühafizəsi üçün təxirəsalınmaz qayda və qanunları tələb edir.

Şagirdin informasiya təhlükəsizliyi təhsil sisteminin, təhsili idarəetmə orqanlarının, təhsil cəmiyyəti və şuralarının tədrisin keyfiyyətinə qoyulan tələblər əhatəsində kifayətedici və qorunan informasiya ehtiyatları ilə təminindən, şagird şüur və təfəkküründə pis təsir göstərə bilən neqativ kompüter informasiyasına təhdid və təhlükələri dərketmə, fərdi və qruplar halında bu təhdid və təhlükələrlə qarşılaşdıqda təhlükəsiz davranma bacarığının formalaşdırılması qabiliyyətidir. Azərbaycan Respublikasında informasiya təhlükəsizliyinin qorunması istiqamətində hüququn əsas mənbəyi ölkə Konstitusiyasıdır. Konstitusiyanın 50-ci maddəsinə əsasən hər kəsin istədiyi məlumatı qanuni yolla axtarmaq, əldə etmək, ötürmək, hazırlamaq və yaymaq azadlığı vardır. "İnformasiya əldə etmək haqqında" Azərbaycan Respublikası Qanununda isə deyilir: "Azərbaycan Respublikasında informasiyanın əldə olunması azaddır" (1, maddə 2). İnformasiya əldə etmək azadlığı heç də o demək deyildir ki, hər bir şagird yerləşmə mənbəyini bilmədiyi intəhasız informasiya ehtiyatlarında istədiyi informasiyaya müraciət edə bilər və bu zaman informasiya sistemlərinin əsas elementlərindən olan onların proqram və texniki təminatında, eləcə də hüquqi normalarında pozuntulara yol verə bilər. Unudulmamalıdır ki, kompüter ehtiyatlarından, kompüter şəbəkəsindən və ya şəbəkə qurğusundan cinayət məqsədi ilə qanunsuz istifadə, yəni kibercinayətkarlıq Azərbaycan Respublikası Cinayət Məcəlləsi ilə cəzalandırılır. Belə ki, "EHM-lər üçün ziyanverici proqramlar yaratma, onlardan istifadəetmə və ya onları yayma" (2, maddə 272), eləcə də "EHM-lərin, EHM sistemlərinin və ya onların şəbəkələrinin işinin qaydalarını pozma" (2, maddə 273) kompüter cinayətkarlığı hesab olunur. "İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında" Azərbaycan Respublikası qanununda yazıldığı kimi :"İnformasiya ehtiyat-

ları – informasiya sistemlərində (kitabxanalarda, arxivlərdə, fondlarda, məlumat banklarında və s.) olan sənədlər və sənəd massivləri, habelə ayrıca mövcud olan sənədlər və onların massivləridir" (3, maddə 2). İnformasiya ehtiyatları informasiya sistemlərinin fəaliyyətinin nəticəsi olub, istifadəçinin tələbinə uyğun hazırlanan, yayılma və tətbiqi üçün təyin olunmuş sənədlər, informasiya massivləri, verilənlər bazası və informasiya xidmətləridir. Bu mənada şagird sağlamlığına, onun normal şəxsiyyət kimi formalaşmasına ziyan vuran və bütövlükdə təhsilalanlar üçün qadağan olunmuş informasiya ehtiyatlarını yaratmaq və yaymaq da kompüter cinayətkarlığı kimi qiymətləndirilə bilər. Ona görə də təhsil müəssisələrində informasiya təhlükəsizliyi problemi təhsil sisteminin qarşısında duran vacib problemlərdən biridir.

Müasir rəqəmsal dünyada daha çox informasiyanın onlayn rejimdə olması, xüsusilə də koronavirus infeksiyası pandemiyası (COVİD-19) səbəbindən distant təhsilə keçid təhsil müəssisəsinin informasiya təhlükəsizliyi qarşısında yeni-yeni tələblər qoyur, daha dəqiq desək, onlayn rejimdə informasiyanın təhlükəsiz istifadəsinə və qorunmasına tələblər də artır. 10-15 il əvvəl informasiya təhlükəsizliyində aktuallıq iqtisadi aktuallıq üzərində qurulurdusa, indi bütün proseslərin rəqəmsallaşdırıldığı, yəni elektronlaşdırıldığı bir dövrdə informasiya təhlükəsizliyi bütövlükdə ictimai həyatın təhlükəsizliyinə çevrilmişdir. Bəs bu təhlükəsizliyin təmin olunmasında, onun olduğu səviyyədə dərk olunması üçün təhsil sahəsində təhlükəsizlik məlumatlılığında (*ing. security awareness*) nələrə diqqət edilməlidir? Onu da qeyd edək ki, rusdilli mənbələrdə *security awareness dedikdə* istifadəçilərin informasiya təhlükəsizliyi sahəsində məlumatlılığının artırılması kimi tərcümə edilməsinə baxmayaraq, bəzi mütəxəssislərə görə, kiberfəzada istifadəçi hərəkətlərinin dərk olunmasının artırılmasıdır (4, s. 38). Bu məqalədə bizim məqsədimiz informasiya təhlükəsizliyinə məhz şüurlu yanaşmanın əhəmiyyətini izah etməkdir.

Hər bir istifadəçi kompüterdə iş zamanı nə etdiyini, nəyə görə etdiyini dərk etməli, bu hərəkətlərin nə ilə nəticələnə biləcəyini təsəvvür edə bilməlidir. Bunun üçün o, kompüter virusunun, şəbəkə qurdunun, spamların nə olduğunu, fişinq hücumlarının, məntiqi bombanın (*ing. logic bomb*), casus proqram təminatının (*ing. Spyware*) varlığını, eləcə də onların hansı fəsadlara gətirib çıxara biləcəyini bilməli, virusa yoluxma hallarında necə hərəkət etmək lazım olduğunu dəqiq bilməsə də ilkin tədbirləri görə bilməlidir. Başqa sözlə desək, əgər istifadəçi kiberfəzada, yəni istifadəçilər, təşkilatlar, şəbəkələr, qurğular, informasiya sistemlərini əhatə edən, onlar arasında və vasitəsilə fəaliyyəti həyata keçirən virtual mühitdə özünü dərk edilmiş kimi aparırsa, onda onu aldatmaq və ya kənar hərəkətlərə sövq etdirmək olduqca çətin məsələyə çevrilir. Ona görə də informasiya təhlükəsizliyinə yalnız şüurlu münasibət istifadəçini, bütövlükdə təhsil ocağını mövcud təhdidlərdən və təhlükələrdən qoruya bilər. Məsələ ondadır ki, heç bir şeydən şübhələnməyən istənilən kompüter istifadəçisi tədricən çox təhlükəli insayderə çevrilə bilər. Xüsusi halda informasiya təhlükəsizliyi qaydalarına riayət etməyən şagirdin yol verdiyi təhlükəsizlik pozuntularına görə həmin kompüterdə işləyə bilən digər şagird üçün proqram boşluqları, proqram təminatında nasazlıqlar, arzuolunmaz kontent və digər qadağan edilmiş informasiya ehtiyatlarına çıxış kimi fəsadlar yarana bilər. Bütün bunların baş verməməsi üçün, təhsil müəssisələrində şagirdlərdə informasiya təhlükəsizliyinə şüurlu dərketmənin formalaşdırılmasının zəruriliyi bir daha aydın olar. *Bəs şagirdlərdə kompüterdən istifadə zamanı təhlükəsizlik qayda və qanunlarına şüurlu dərketməni necə formalaşdırmaq olar?*

Bu məqsədin reallaşdırılması, ilk növbədə, texniki mühafizə vasitələrindən istifadə ilə həyata keçirilə bilər. Bunun üçün İnternet bağlantısı olan kompüter sinifləri xarici mühafizə vasitəsi olaraq xüsusi proqram komplekslərindən, sorğu verilən internet-kontentin məzmununun analizinə görə girişə icazə verən proksi-serverlərdən, eləcə də antivirus proqramları ilə təmin olunmalıdır. Bu məqsədlə təhsil müəssisəsinin vahid kontent-filtrasiya sisteminə (KFS) birləşdirilməsi qaydalarına müvafiq olaraq əlaqədar orqanlara müraciət olunmalıdır. Bu zaman kontent-filtrasiya sistemlərinə aşağıdakı tələblər qoyulur:

1) İnternetə çıxışı olan təhsil müəssisənin bütün kompüterlərinə belə vasitə quraşdırılmalıdır;

2) KFS–lər internet-ehtiyatlara təhsil məqsədlərinə zidd olan girişə məhdudiyyət qoymaq sahəsində vahid siyasəti yerinə yetirməlidir;

3) KFS-lər internet-ehtiyatlardan istifadənin monitorinqini təmin etməlidir;

4) KFS-lər Təhsil Nazirliyi tərəfindən təklif olunan kateqoriya siyahıları üzrə kontentin filtrasiyasını təmin etməlidir.

Təhsil müəssisələrində informasiya təhlükəsizliyini yalnız texniki vasitələrin köməyi ilə təmin etmək mümkün deyildir. Məsələ ondadır ki, texniki vasitələrin texniki və alqoritmik məhdudiyyətləri səbəbindən bu vasitələr tam mühafizəni təmin etmir, bəzi hallarda isə zəruri informasiyaya girişə imkan vermədiyinə görə hətta tədris prosesini dayandıra da bilər.

Digər tərəfdən, istənilən informasiya təhlükəsizliyi sisteminin ən zəif bəndi insan amili hesab olunur. Məhz insan amilinə əsaslanan bədniyyətli sosial mühəndislik üsullarından məharətlə istifadə edərək şəbəkəyə birləşdirilmiş istənilən kompüterə müvəffəqiyyətli hücumlar da edə bilər. Bəs nə etməli? Burada informatika fənnini tədris edən müəllim üzərinə xüsusi məsuliyyət düşür. Belə ki, tədris prosesinin aparıcısı kimi müəllim kompüter sinfində yarana biləcək müxtəlif xarakterli neqativ halları vaxtında aşkarlamalı və müvafiq tədbirlər görmək imkanında olmalıdır. Bu zaman xüsusilə diqqətli olmaq tələb olunur. İnformasiya təhlükəsizliyi probleminin həlli istiqamətində aparılan araşdırmalar nəticəsində belə fikir formalaşmışdır ki, istifadəçilər, o cümlədən şagirdlər informasiya texnologiyalarını düzgün tətbiq etmirlər və onları buraxdıqları səhvlərə görə cəzalandırmaq zəruridir.

Əgər hər hansı bir istifadəçi, o cümlədən şagird informasiya texnologiyalarını təhlükəsiz tətbiq edə bilmirsə, deməli onların bu istiqamətdə biliklərində boşluqlar vardır və yaxşı olar ki, bu boşluqlar vaxtında aşkarlanıb aradan qaldırılsın. Digər tərəfdən, əgər şagird kompüterdə işi zamanı təhlükəsizlik qaydalarına riayət etmədiyinə görə müəyyən şəkildə cəzalandırılarsa, onda bu hərəkətlərin daha ciddi fəsadlara gətirib çıxara biləcəyini də unutmaq olmaz.

Təhlükəsizlik qaydalarına əməl etmədiyinə görə xəbərdarlıq və ya töhmət almış şagird növbəti işi zamanı ona aydın olmayan müxtəlif xarakterli vəziyyətlər haqqında, eləcə də işlədiyi kompüterin ziyanverici proqramlarla yoluxması haqqında informasiyanı gizlətməyə çalışa bilər ki, belə hərəkətlərin də sonda nəyə səbəb ola biləcəyini təsəvvür etməmək mümkün deyildir. Bu isə o deməkdir ki, kompüter siniflərində iş zamanı informatika müəllimlərinə cəza orqanı kimi baxılması da yaxşı hal kimi qiymətləndirilə bilməz.

Yalnız öz hərəkətlərinə şüurlu yanaşma, onların nə ilə nəticələnə biləcəyini dərketmə ilə kompüter siniflərində informasiya təhlükəsizliyini təmin etmək olar. Bu məsələdə bir məqamı da qeyd etmək yaxşı olardı. Belə ki, istənilən auditoriyada informasiya texnologiyalarından digərlərinə nisbətdə kifayət qədər məlumatlı, daha bilikli şagird ola bilər ki, onlar da təhlükəsizlik qaydaları üzrə edilən iradları heç də həmişə yaxşı qarşılamır, əksinə, təhlükəsizlik qaydalarından yan keçməyə cəhd edə bilərlər. Belə bir halda da nəinki bir kompüterdə, bütövlükdə birbiri ilə lokal şəbəkədə birləşdirilmiş bütün kompüterlərdə və nəticədə təhsil müəssisəsinin kompüter şəbəkəsinin normal işində müxtəlif fəsadlar, o cümlədən təhsil müəssisəsinə aid konfidensial məlumatların itkisi və ya saxtalaşdırılması baş verə bilər.

Bütün bunlar onu qeyd etməyə əsas verir ki, informasiya təhlükəsizliyində şüurlu yanaşma ilə, onu tam şəkildə təsəvvür etməklə, onun fəsadlarını dərk etməklə kiberfəzada təhlükəsizliyə nail olmaq olar. Başqa sözlə desək, təhlükəli internet-kontentdən, ziyanverici kodlara yoluxma hallarından, müxtəlif kompüter fəsadlarından qaçmaqda ən yaxşı filtr bilavasitə şagirdin beynində şəbəkə təhlükəsizliyi üzrə mövcud təsəvvürlər əsasında formalaşdırılan şüurlu yanaşmanın səviyyəsidir ki, onun da tənzimlənməsi informatika müəlliminin peşəkarlıq səviyyəsindən asılıdır.

Beləliklə, internetə birləşdirilmiş kompüter siniflərində hər bir şagirdin işlədiyi kompüterdə baş vermiş fəsadlar zamanı, eləcə də bədniyyətli hücumlar zamanı özlərini necə aparmalarının əhəmiyyəti olduqca böyükdür. Bu zaman hər bir istifadəçiyə informasiya əldə etməyin təhlükəsiz qaydaları, fərdi verilənlərin, eləcə də konfidensial informasiyanın nə olduğu, kimin onları necə işlətməli olması diqqətlə izah edilməli, bu tələbləri pozan hər bir istifadəçini mövcud qayda və qanunlar üzrə hansı cəza gözlədiyi də başa salınmalıdır.

Bundan başqa, proqram yükləmələrinə ehtiyac olduğu təqdirdə yalnız rəsmi saytların proqramlarından istifadə etmək, şübhəli internet-resurslarına daxil olmamaq, elektron-poçtla iş za-

manı tanış olmayan ünvanlardan gələn məktubları açmamaq tövsiyə olunmalıdır. Şagirdlərə saxta saytlar nədir, eləcə də elektron poçtdan istifadə zamanı hansı kibertəhlükələrlə, o cümlədən ziyanverici proqram təminatının yüklənməsi, məqsədli fişinq hücumları və spamlarla qarşılaşabilmə təhlükələri izah olunmalıdır. Bu tövsiyələrə əməl olunmadığı təqdirdə onların təhsil və tərbiyəsinə ziyan vura bilən təhlükəli kontentlə qarşılaşacağı xüsusilə vurğulanmalıdır.

Hər bir kompüter sinfində informasiya təhlükəsizliyi üzrə aşağıdakı minimal qaydalara əməl olunmalıdır:

1. Təhsil müəssisəsinin təhlükəsizlik siyasətinə;
2. Parolların seçilməsi, dəyişdirilməsi və istifadəsi qaydalarına;
3. Konfidensial informasiyalarla işləmək qaydalarına;
4. Baş vermiş insidentlər, istifadə olunan proqram təminatındakı boşluqlar, səhvlər və dayanmalar haqqında vaxtında məlumat vermək proseduralarına.

İnformasiya təhlükəsizliyi əsaslarının sadaladığımız bu minimal qaydaları hər bir təhsil ocağında öyrədilməli və inkişaf etdirilməlidir. Hər şeydən əvvəl informasiya təhlükəsizliyi standartının gənc nəsli təhlükəsiz kontentdən qorumağa xidmət edən məktəb tətbiqini nəzərdə tutan müəyyən təhlükəsizlik siyasətinin olması zəruridir. Başqa sözlə desək, hər bir şagird təhsil müəssisəsinin rəhbər tutduğu əsas hərəkət istiqamətlərindən biri olan təhlükəsizlik siyasətinin, yəni informasiya təhlükəsizliyinin təmini üçün təsdiq olunmuş plan və ya hərəkət üsullarının, eləcə də təhlükəsizlik proseduralarının nədən ibarət olduğunu və nə üçün iş zamanı onlara riayət olunmalı olduğunu aydın təsəvvür etməli və uyğun vəziyyətlərdə hansı müvafiq zəruri addımların atılmalı olduğunu da bilməlidir. Ona görə də şagirdlər informasiya təhlükəsizliyi üzrə mütəmadi olaraq təlimatlandırılmalıdırlar. Bu prosesin kəsilməsi və ya müntəzəmliyinin pozulması İnternetə birləşdirilmiş kompüter siniflərində bədniyyətlilərin real hücumları zamanı ciddi pozuntularla müşayiət oluna bilər. Bu zaman alman psixoloqu German Ebbinqauzun ictimai həyatın bütün sahələrində, xüsusilə də təhsil sahəsində prinsipial bir qanun kimi tanınan məşhur "unutqanlıq qanunu" yaddan çıxarılmamalıdır. Bu qanuna görə: "Təhsil yalnız ilk 3 gün səmərəli olur, sonralar isə tədris olunmuş material praktiki möhkəmləndirilmirsə, onun 90%-i unudulur"(5, s. 58). Nəzərə alsaq ki, digər problemlərdən fərqli olaraq informasiya təhlükəsizliyinin təmini qayda və qanunlarında unutqanlıq şagird təlim və tərbiyəsində daha böyük əyintilərə səbəb ola bilər, onda unutqanlıq qanununa etinasızlığın yolverilməz olması bir daha aydın olar.

Göründüyü kimi, XXI əsrin ən böyük problemlərindən biri olan informasiya təhlükəsizliyi probleminin həllində bu problemin ayrı-ayrı elementlərinin təhsil müəssisələrində müntəzəm tədrisi xüsusilə zəruridir. Belə ki, bugünkü şagirdin cari anda əldə etdiyi istifadəçi vərdiş və bacarıqları onların gələcək təhsil və peşəkar fəaliyyətlərində kiberfəzada daha təhlükəsiz işləmələri, bütövlükdə isə cəmiyyətin informasiya təhlükəsizliyi üçün qarant ola bilər.

Beləliklə, şagirdlərin informasiya təhlükəsizliyinə hazırlığı və onu tənzimləmək bacarıqlarının formalaşdırılması müasir təhsil sisteminin əsas vəzifələrindəndir. Bu məsələnin həlli informasiya mühitinin bütün səviyyələrində həyata keçirilməlidir. Başqa sözlə desək, informasiya mühitinin ailə səviyyəsindən, təhsil müəssisəsinin səviyyəsindən, təhsil müəssisəsinin aid olduğu rayon və ya əyalətin səviyyəsindən və ümumölkə səviyyəsindən asılıdır. Aydın məsələdir ki, bütün bu səviyyələrdə aparıcı qüvvə müəllim və onun hazırlıq səviyyəsidir. Belə ki, informasiyaya məhdud giriş şəraitindən qeyri-məhdud giriş şəraitinə keçirildiyi müasir təhsildə informatika müəllimlərinin üzərinə xüsusilə böyük məsuliyyət düşür. Bu zaman hər bir informatika müəllimi informasiya təhlükəsizliyi üzrə hansı əsas qanunvericilik aktlarının mövcudluğundan və onların məzmunundan xəbərdar olmalı, eləcə də informasiya təhlükəsizliyi məsələləri üzrə şagird və valideynlərlə iş üçün xüsusi hazırlığa malik olmasını dərk etməlidir. Elə bu səbəbdən də informatika müəllimlərin peşəkarlığının artırılması problemi müasir təhsilin aktual məsələlərindən biri olmalıdır.

Problemin aktuallığı. Müasir şagirdin İnternetə qeyri-məhdud giriş imkanlarının mövcud olduğu bir şəraitdə informasiya təhlükəsizliyinin baza prinsiplərinin müntəzəm tədrisi zəruridir.

Problemin elmi yeniliyi. Şagirdlərin informasiya təhdid və təhlükələrinə hazırlığının və onun tənzimlənməsi bacarığının formalaşdırılması müasir

təhsil sisteminin əsas vəzifələrindən biri kimi informasiya mühitinin bütün səviyyələrində, o cümlədən ailə mühitindən başlayaraq ölkə səviyyəsinədək həyata keçirilməlidir.

Problemin praktik əhəmiyyəti şagirdlərin informasiya təhlükəsizliyinin təmini üçün, internet xidmətlərinə müraciət mədəniyyətinin formalaşdırılmasıdır. Yalnız informasiya təhlükəsizliyi sahəsində zəruri biliyə malik şagird öz şüurlu münasibəti sayəsində onlayn-serverlərdən təhlükəsiz necə istifadə edildiyini və bu server və saytlardan fikirləşmədən istifadənin isə hansı fəsadlara gətirib çıxara biləcəyini başa düşə bilər.

Ədəbiyyat:

1. "İnformasiya əldə etmək haqqında" Azərbaycan Respublikasının Qanunu. 30 sentyabr 2005-ci il.
2. "Azərbaycan Respublikası Cinayət Məcəlləsi".
3. "İnformasiya, informasiyalaşdırma və informasiyanın mühafizəsi haqqında" Azərbaycan Respublikasının Qanunu. 03 aprel 1998-ci il.
4. "Information Security/Информационная безопасность", 2021, № 5, ноябрь
5. "Information Security/Информационная безопасность",2021, № 3, июль
6. "Information Security / Информационная безопасность", 2021, № 4, сентябрь,
7. Вестник кибербезопасности, 2021, № 9 (69), сентябрь,

E-mail: akiforuc@rambler.ru
E-mail: nigar.mirzayeva@mail.ru
Rəyçilər: *tex.ü.fəls.dok., dos.* **Z.M. Əmirov**
riy. ü.fəls.dok.,dos. **Z.A. Səmədova**
Redaksiyaya daxil olub: 21.02.2022.