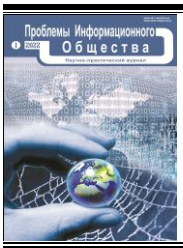


www.jpis.az

13 (1)
2022

Cəmiyyətdə informasiya təhlükəsizliyi mədəniyyətinin formalaşdırılması sahəsində beynəlxalq təcrübənin analizi

Rəsmiyyə Ş.Mahmudova

İnformasiya Texnologiyaları İnstitutu, Azərbaycan Milli Elmlər Akademiyası, B.Vahabzadə küç., 9A, AZ1141, Bakı, Azərbaycan

rasmahmudova@gmail.com

MƏQALƏ HAQQINDA
http://doi.org/10.25045/jpis.v13.i1.10

Məqalənin tarixi:
Təqdim olunub 27 iyul 2021
Rəy formasının alınması
30 oktyabr 2021
Qəbul olunub 10 yanvar 2022

Açar sözlər:
İnformasiya təhlükəsizliyi mədəniyyəti
Kibertəhlükəsizlik mədəniyyəti
İnformasiya təhlükəsizliyi haqqında məlumatlılıq
Kibertəlim
Mediatəhsil
Beynəlxalq təcrübə

XÜLASƏ

İnformasiya – kommunikasiya texnologiyalarının sürətli inkişafı, informasiya mənbələrinin artması, bütün sahələrdə əhaliyə göstərilən bir çox xidmətlərin elektronlaşması, insanlar arasında yeni ünsiyyət vasitələrinin meydana çıxması, müxtəlif informasiya sistemlərində insanların fərdi məlumatlarının toplanması və digər reallıqlar bir tərəfdən cəmiyyətin inkişafı baxımından yeni imkanlar yaradır. Digər tərəfdən isə informasiyadan insanların şüurunu manipulyasiya etmək, cəmiyyətdə xaos yaratmaq üçün istifadə edilməsi cəmiyyətdə informasiya təhlükəsizliyi mədəniyyətinin inkişaf etdirilməsini aktuallaşdırır. Məqalədə informasiya təhlükəsizliyi mədəniyyətinin formalaşdırılması sahəsində inkişaf etmiş dövlətlərin təcrübəsi analiz edilib. BMT, İqtisadi Əməkdaşlıq və İnkişaf Təşkilatı kimi beynəlxalq təşkilatlar tərəfindən bu istiqamətdə qəbul edilmiş sənədlər, çağırışlar və həyata keçirilən tədbirlər çərçivəsində mütəxəssislərin, vətəndaşların və müxtəlif əhali qruplarının, eləcə də təhsil işçilərinin, uşaq və gənclərin informasiya təhlükəsizliyi mədəniyyətinin səviyyəsinin yüksəldilməsi üçün ayrı-ayrı ölkələrin təcrübəsi araşdırılmış və ümumiləşdirilmişdir. Tədqiqatda sistemləşdirmə, ümumiləşdirmə, müqayisəli analiz metodlarından istifadə edilmişdir. Tədqiqatdan əldə edilən nəticələr cəmiyyətdə informasiya təhlükəsizliyinin təmin edilməsinə cavabdeh olan qurumlar üçün faydalı ola bilər.

Analysis of international experience in the formation of a culture of information security in society

Keywords:
Information security culture
Culture of cybersecurity
Awareness of information security
Cyber education
Media education.
International experience

The rapid development of information and communication technologies, the increase in sources of information, the electronization of many services in all areas, the emergence of new means of communication between people, the collection of personal data in various information systems and other realities create new opportunities for development. On the other hand, the use of information to manipulate people's minds, to create chaos in society, actualizes the development of a culture of information security in society. The article analyzes the experience of developed countries in the formation of information security culture. As part of the documents, challenges and measures taken by international organizations such as the UN, the Organization for Economic Cooperation and Development, the experience of individual countries in raising the level of information security culture of professionals, citizens and various groups, as well as educators, children and youth, was studied and summarized. The study used methods of systematization, generalization, comparative analysis. The results of the study may be useful to institutions responsible for ensuring information security in society.

Анализ международного опыта формирования культуры информационной безопасности в обществе.

Ключевые слова:
Культура информационной безопасности
Культура кибербезопасности
Осведомленность об информационной безопасности
Киберучение
Медиаобразование
Международный опыт

Быстрое развитие информационных и коммуникационных технологий, увеличение источников информации, электронизация многих услуг во всех сферах, появление новых средств связи между людьми, сбор персональных данных в различных информационных системах и другие реалии создают новые возможности для развития. С другой стороны, использование информации для манипулирования сознанием людей, создания хаоса в обществе актуализирует развитие культуры информационной безопасности в обществе. В статье анализируется опыт развитых стран по формированию культуры информационной безопасности. В рамках документов, вызовов и мер, принятых международными организациями, такими как ООН, Организация экономического сотрудничества и развития, были исследованы и обобщены опыт отдельных стран по повышению уровня культуры информационной безопасности профессионалов, граждан и различных групп, а также педагогов, детей и молодежи. В исследовании использованы методы систематизации, обобщения, сравнительного анализа. Результаты исследования могут быть полезны учреждениям, ответственным за обеспечение информационной безопасности в обществе.

1. Giriş

Bildiyimiz kimi, artıq informasiya cəmiyyətin bütün əsas subyektlərinin – fərdin, sosial və iqtisadi institutların, dövlətin fəaliyyəti üçün vacib və qiymətli komponentə çevrilmişdir. Böyük əhəmiyyət kəsb edən informasiyaya icazəsiz girişin qarşısını lazımi səviyyədə almaq mümkün olmadıqda, şəxsi, ictimai və ya dövlət səviyyəsində təhlükəsizliyin təmin edilməsi problemləri meydana çıxır. Ona görə də mütəxəssislər informasiya cəmiyyətinin reallıqlarına uyğun olaraq, informasiya təhlükəsizliyi mədəniyyətinin (İTM) formalaşdırılmasını zəruri hesab edirlər.

Məlumdur ki, müasir idarə və təşkilatlar rəqəmsal mühitdə, bir-biri ilə qarşılıqlı əlaqədə fəaliyyət göstərirlər. Bu da onlara əməkdaşlıq və informasiya mübadiləsi üçün geniş imkanlar yaradır. Lakin, eyni zamanda bu qarşılıqlı əlaqə onların daxili və xarici təhdidlərə məruz qalmasına səbəb olur. Daxili təhdidlər müəssisələrin ən çox rastlaşdığı informasiya təhlükəsizliyi problemidir [1]. Əməkdaşlar qəsdən və ya bilməyərəkdən, çox vaxt isə zəruri biliklərin yetərincə olmaması səbəbindən çalışdıqları müəssisəni informasiya təhlü-kəsizliyi baxımından böyük təhlükələrə məruz qoyurlar.

Kiberhücumları analiz edən beynəlxalq hesabatlar və ekspert rəyləri təsdiq edir ki, insan faktoru kibertəhlükəsizlik sahəsində vacib elementlərdən biridir [2]. Parolların idarə edilməsi, fişinq hücumlarının qarşısının alınması kimi təhlükəsizlik tədbirləri vacib olsa da, müəssisələrdə təhlükəsizlik risklərinin idarə olunması üçün, informasiya təhlükəsizliyi mədəniyyəti də yüksək səviyyədə olmalıdır. Hazırda insanların şüurunu manipulyasiya etməklə qiymətli informasiyanın əldə edilməsi üçün sosial mühəndislik üsullarından məharətlə istifadə olunur [3].

İnformasiya təhlükəsizliyi geniş anlayışdır, özündə, informasiyanın qorunması, yəni birbaşa informasiyanın təhlükəsizliyinin təmin edilməsi ilə yanaşı, subyektlərin neqativ informasiya təsirlərindən qorunmasını təmin edən informasiya-psixoloji təhlükəsizliyi də ehtiva edir [4]. Eyni zamanda, informasiya resurslarından istifadə edərkən hüquqi və etik normalara əməl edilməməsi də informasiya təhlükəsizliyi problemidir.

Göründüyü kimi, informasiya təhlükəsizliyi mədəniyyəti informasiya təhlükəsizliyi sahəsində texnoloji mədəniyyət, informasiya-psixoloji mədəniyyət və hüquqi-etik mədəniyyətin məcmusundan ibarətdir.

Hazırda müasir dünyada qlobal kibertəhlükəsizlik mədəniyyətinin formalaşdırılmasına böyük səy göstərilir. Bu da onu deməyə əsas verir ki, informasiya təhlükəsizliyinin təmin edilməsi günümüzün vacib qlobal problemlərindən birinə çevrilmişdir. Qlobal kibertəh-lükəsizlik mədəniyyətinin işlənib hazırlanmasına aparıcı beynəlxalq təşkilatlar böyük töhfə vermişlər. Bu problemə böyük maraq göstərən ilk beynəlxalq təşkilat Birləşmiş Millətlər Təşkilatı (BMT) olmuşdur. Ona görə ki, İTM bütün beynəlxalq ictimaiyyətin təhlükəsizliyinin təmin edilməsi üçün böyük əhəmiyyət kəsb edir. Digər tərəfdən isə BMT həmişə informasiya texnologiyalarının inkişafına və informasiya mübadiləsi məsələlərinə diqqət yetirmişdir. Məsələn, 1971-ci ildə BMT-nin Baş Assambleyası tərəfindən "İnformasiya azadlığı: insan hüquqları və elmi-texniki inkişaf" adlı bəyannamə qəbul edilmişdir. İTM-in formalaşdırılması problemləri də daim BMT-nin diqqət mərkəzində olmuşdir ki, bunun da nəticəsində 20 dekabr 2002-ci ildə BMT-nin Baş Assambleyası tərəfindən "Qlobal kibertəhlükəsizlik mədəniyyətinin yaradılması" Bəyannaməsi qəbul edilmişdir [5].

İqtisadi Əməkdaşlıq və İnkişaf Təşkilatı (İƏİT) tərəfindən 2002-ci ildə qəbul edilmiş "İnformasiya sistemlərinin və şəbəkələrinin təhlükəsizliyi üzrə idarəedici prinsiplər: təhlükəsizlik mədəniyyətinə doğru" ("*OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security"*) [6] adlı tövsiyələr inkişaf etmiş ölkələrdə İTM-in formalaşdırılması üçün təkan olmuşdur.

İnternetin, yüksək məhsuldarlıqlı fərdi kompüterlərin, müxtəlif mobil qurğuların geniş yayıldığı bir şəraitdə əhalinin bütün təbəqələrində İTM-in formalaşdırılması zərurətə çevrilir. Bu mədəniyyətin əsas prinsipləri İƏİT-in tövsiyələrində öz əksini tapmışdır, bunlar "məlumatlılıq" və "məsuliyyət"dir. Bunun mahiyyəti ondan ibarətdir ki:

- məlumatlılıq – bütün vətəndaşlar informasiya təhlükəsizliyini təmin etməyin vacib olması barədə məlumatlandırılmalıdır;
- məsuliyyət – bütün vətəndaşlar informasiya təhlükəsizliyinə görə məsuliyyət daşıyırlar.

2. İnformasiya təhlükəsizliyinə cavabdeh şəxslərin və mütəxəssislərin bilik və bacarıqlarının inkişaf etdirilməsi tədbirləri

İqtisadi cəhətdən inkişaf etmiş ölkələrdə, xüsusən də Avropa Birliyi (AB) və ABŞ-da informasiya təhlükəsizliyinin təmin edilməsi sahəsində bacarıq-

ların inkişaf etdirilməsi və qiymətləndirilməsi sahəsindəki təcrübəni analiz etməyə çalışaq. AB-də informasiya təhlükəsizliyi üzrə bacarıqların inkişaf etdirilməsi sistemli xarakter daşıyır və təlim proqramlarının işlənib hazırlanmasından başlayaraq, özünü qiymətləndirmə də daxil olmaqla, bacarıqların qiymətləndirilməsi vasitələrinin yaradılmasına qədər ardıcıl şəkildə həyata keçirilir.

AB-də informasiya təhlükəsizliyi üzrə müxtəlif təlimlərin keçirilməsinə cavabdeh olan aparıcı təşkilat 2004-cü ildə yaradılmış Avropa Şəbəkə və İnformasiya Təhlükəsizliyi Agentliyidir (European Network and Information Security Agency, ENISA, 2019-cu ildən - The European Cybersecurity Agency). Agentliyin fəaliyyətinin əsas istiqamətlərindən biri AB-yə üzv ölkələrdə informasiya-kommunikasiya texnologiyalarından (İKT) təhlükəsiz istifadə üçün təlim və təşviqat fəaliyyətinin dəstəklənməsi, AB vətəndaşlarının hazırlıq səviyyəsinin yüksəldilməsidir.

ENISA tərəfindən informasiya təhlükəsizliyi məsələləri üzrə məlumatlılıq səviyyəsinin artırılması üçün müxtəlif proqramlar həyata keçirilir. Məsələn, 2010-cu ildə agentliyin hazırladığı "Yeni istifadəçilər üçün təlimat: informasiya təhlükəsizliyi üzrə məlumatlılığı necə yüksəltməli" adlı sənəd informasiya təhlükəsizliyi sahəsində məlumatlılığın yüksəldilməsi proqramlarının planlaşdırılması və həyata keçirilməsi üçün praktiki təlimatdır [7].

Bu sahədə zəruri bilik və bacarıqlara gəlincə, AB-nin vətəndaşlar üçün tövsiyələrində informasiyaya münasibətdə kibertəhlükəsizlik təhdidlərinə və onunla bağlı risklərə – yalan məlumatlar, kiberbullinq və radikallaşdırmaya aksent olunur. Kritik risk kimi isə dövlət idarəetmə sistemində informasiya təhlükəsizliyinin pozulması qeyd edilir.

İnformasiya təhlükəsizliyi üzrə qiymətləndirmə və eyni zamanda təlim ümumavropa təlimləri (Cyber Europe) çərçivəsində həyata keçirilir. Təlimlərdə kibertəhlükəsizlik sahəsində ixtisaslaşmış ekspertlər tərəfindən işlənib hazırlanmış, reallığın modelləşdirilməsinə əsaslanan texnologiyalardan istifadə olunur.

Rəqəmsal savadlılığın inkişaf etdirilməsi üzrə AB-nin apardığı işlərin miqyası və sistemliliyi iştirakçıların sayı (18 milli korporasiya, 300-dən artıq layihəni işləyib hazırlayanlar və 7 milyondan çox vətəndaş) və İnnovativ Təhsil Texnologiyalarından İstifadəni Təşviq Etməklə Səmərəli Təlim Özünüanaliz (Self-reflection on Effective Learning by Fostering the use of Innovative Educational technologies, SELFIE) alətinin tətbiqinə istiqamətlənən tədbirlərin sayı (11 növ) ilə də müəyyən oluna bilər [8].

ABŞ-da bütün əməkdaşlara informasiya təhlükəsizliyinin əsaslarının öyrədilməsi ilə bağlı təlimlərin keçirilməsi üzrə dövlət təşkilatlarının vəzifələri qanunvericilik səviyyəsində müəyyən edilib. 2002-ci ildə "Elektron hökumət haqqında Qanun"un III bölməsi olan Federal İnformasiya Təhlükəsizliyinin İdarəedilməsi Aktında (Federal Information Security Management Act, FISMA) informasiya sistemləri ilə işləyən bütün əməkdaşların informasiya təhlükəsizliyi məsələləri üzrə məlumatlılığının yüksəldilməsi ilə bağlı vəzifələr müəyyənləşdirilmişdir. İnformasiya təhlükəsizliyi üzrə kompetensiyalarının inkişaf proqramının həyata keçirilməsi və qiymətləndirilməsi üçün əməkdaşlar 2 qrupa bölünür: "informasiya texnologiyaları üzrə mütəxəssislər" və "istifadəçilər". İnformasiya təhlükəsizliyi siyasətinin və prosedurunun həyata keçirilməsinin səmərəliliyinin yoxlanılması və biliklərin yoxlanılması periodik olaraq həyata keçirilir. İnformasiya təhlükəsizliyi sahəsində məlumatlılığın təkmilləşdirilməsi və onların yoxlanılması üsulları üzrə tələblər xüsusi sənəddə öz əksini tapmışdır [9].

ABŞ-da 2003-cü ildə hazırlanmış "İnformasiya texnologiyalarının təhlükəsizliyi ilə tanışlıq və təlim proqramının hazırlanması" adlı sənəddə bütün əməkdaşlara çatdırılmalı olan informasiya təhlükəsizliyinin əsasları mövzusu ətraflı şəkildə şərh olunur.

ABŞ-da mütəmadi olaraq biliklərin yoxlanılıb qiymətləndirilməsi informasiya təhlükəsizliyi üzrə məlumatlılığın yüksəldilməsi proqramının vacib tərkib hissəsidir. Bu zaman əsasən test üsulundan istifadə olunur, bununla yanaşı qəfil yoxlamalar, xüsusi hazırlanmış göndərişlərdən istifadə edilməsi, qəbul edilmiş informasiya təhlükəsizliyi siyasətinin və qaydalarının pozulmasının və onların qeydiyyatının monitorinqi kimi əlavə yoxlama üsulları tətbiq olunur.

2011-ci ildə ABŞ-ın Kadrlar İdarəsi tərəfindən hazırlanmış "Kibertəhlükəsizlik üçün bacarıqlar modeli"ndə [10] müxtəlif profilli informasiya təhlükəsizliyi mütəxəssisləri üçün vacib kompetensiyalar toplusu müəyyən edilmişdir.

Bu sənəddə təklif edilmiş yanaşma ABŞ-ın bir çox dövlət müəssisələrində informasiya təhlükəsizliyi mütəxəssisləri tərəfindən yerinə yetirilən əmək funksiyalarının standartlaşdırılması, onların ilkin ixtisasına tələblərin unifikasiyası və əlavə təhsilə tələbatın müəyyən edilməsi üçün istifadə olunur.

2017-ci ildə qəbul edilmiş "Kibertəhlükəsizlik sahəsində təhsil üzrə milli təşəbbüslər (National Initiative for Cybersecurity Education, NICE):

Kibertəhlükəsizlik üzrə kadr resurslarının strukturu" [11] adlı sənədə əmək funksiyalarını yerinə yetirən müxtəlif profilli informasiya təhlükəsizliyi mütəxəssislərindən tələb olunan dərəcənin müəyyən edilməsi modeli daxil edilmişdir. Sənəddə informasiya təhlükəsizliyinin təmin edilməsi ilə məşğul olan 52 funksional ixtisaslaşma qeyd edilmiş və onların hər biri üçün tapşırıqlar siyahısı verilmiş və uyğun bilik, bacarıq və vərdişlər formalaşdırılmışdır.

Hazırda genişmiqyaslı milli və transmilli kibertəlimlərin təşkili və keçirilməsi məsələləri ilə bir sıra aparıcı beynəlxalq təşkilatlar məşğul olur (cədvəl 1.).

Qeyd olunan təşkilatlar içərisində AB xüsusi yer tutur, bu təşkilat Avropa Komissiyası tərəfindən qəbul edilmiş xüsusi sənədlər əsasında kibertəlimlər təşkil edir və keçirir. Bu təlimlərin keçirilməsi AB Komissiyası tərəfindən qəbul edilmiş bir sıra sənədlərə əsaslanır.

Məsələn, 2009-cu ildə Avropa İttifaqı Şurasının qəbul etdiyi qətnamə AB ölkələrinin "milli kibertəlimlər keçirməsinə" hüquqi zəmin yaratdı, eyni zamanda beynəlxalq transmilli kibertəlimlərdə fəal iştirak üçün çağırış idi. AB tərəfindən ilk kibertəlim 2010-cu ildə (Cyber Europe 2010), ABŞ və AB-nin ilk birgə kibertəlimi isə 2011-ci ildə keçirilmişdir.

"Avropa 2020" Strategiyasının tərkib hissəsi olan "İnam və təhlükəsizlik" (*Pillar III*: *Trust and Security*) üzrə Avropanın Rəqəmsal Gündəliyində müəyyən edilmiş kibertəhlükə-sizliyin əsas inkişaf istiqamətlərinə aşağıdakılar daxildir [12]:

- şəbəkə və informasiya təhlükəsizliyi sferasında siyasətin gücləndirilməsi;
- kritik əhəmiyyətli dövlət və kommersiya infor-masiya sistemlərinə müasir kiberhücum-ların qarşısının alınması;
- kibercinayətlərlə mübarizə üzrə Avropa platformasının təsis edilməsi;
- kibercinayətlərlə mübarizə üzrə Avropa mərkəzinin yaradılması zəruriyyətinin araşdırılması;
- təhlükəsizlik sisteminin pozulması (fərdi məlumatların və digər konfidensial informasiyanın itməsi, oğurlanması və dəyişdirilməsi) hallarında istifadəçilərin məlumatlandırılması üsullarının öyrənilməsi;
- İnternetdə məxfilik qaydalarına əməl edilməsinə nəzarət;
- qanunazidd onlayn kontent haqqında məlumatlandırma mexanizminin dəstəklənməsi və uşaqlar üçün təhlükəsiz İnternet haqqında məlumatlılığın yüksəldilməsi;
- AB-yə üzv dövlətlər tərəfindən, qanunazidd kontentin aşkarlanması haqqında məlumatların qəbul edilməsi üçün qaynar xətlərin fəaliyyətinin təmin edilməsi;
- AB miqyasında təhlükələr haqqında milli məlumatlandırma sisteminin (national alert platforms) yaradılması;
- Və s.

Cədvəl 1. Kibertəlimlər keçirən beynəlxalq təşkilatların siyahısı

Kiber təlimlər keçirən təşkilatın adı	İnternet saytı
Asiya-Sakitokean İqtisadi Əməkdaşlıq Təşkilatı (Asia-Pacific Economic Cooperation, APEC)	www.apec.org
Cənub-Şərqi Asiya Dövlətləri Assosiasiyası (Association of SouthEast Asian Nations, ASEAN)	www.asean.org
Avropa Birliyi (European Union, EU)	www.europa.eu
Council of Europe (Avropa Şurası)	www.coe.int
Avropol (Europol)	www.europol.europa.eu
İnformasiya Təhlükəsizliyi İnsidentlərinə Reaksiya Komandalarının Forumu (Forum of Incident Response and Security Teams, FIRST)	www.first.org
Səkkizlər qrupu (Group of eight, G8)	www.g8russia.ru
Elektrotexnika və Elektronika Mühəndisləri İnstitutu (Institute of Electrical and Electronics Engineers, IEEE)	www.ieee.org
Beynəlxalq Elektrotexnika Komissiyası (International Electrotechnical Commission, IEC)	www.iec.ch
Beynəlxalq Standartlaşdırma Təşkilatı (International Organiza-tion for Standardization, ISO)	www.iso.org
Beynəlxalq Telekommunikasiya İttifaqı (International Telecommunication Union, ITU)	www.itu.int

İnternetdə domen adların və zonaların verilməsini həyata keçirən qeyri- kommersiya təşkilatı (Internet Corporation for Assigned Names and Numbers, ICANN)	www.icann.org
İnternet mühəndisliyi üzrə işçi qrupu (Internet Engineering Task Force, IETF)	www.ietf.org/about/mission.html
İnternet İdarəçilik Forumu (Internet Governance Forum, IGF)	www.intgovforum.org/cms

3. Vətəndaşların və müxtəlif əhali qruplarının informasiya təhlükəsizliyi mədəniyyətinin səviyyəsinin yüksəldilməsi

Artıq hər kəsə məlumdur ki, informasiya cəmiyyətinin inkişafı istiqamətində əsas problemlərdən biri dövlətin, cəmiyyətin və bu cəmiyyətin üzvü olan fərdlərin informasiya təhlükəsizliyinin təmin edilməsidir. Hər kəs informasiya təhlükəsizliyi sahəsində müəyyən zəruri biliklərə malik olmalıdır ki, get-gedə artan informasiya təhdidlərinə qarşı mübarizə apara bilsin, kibercinayətkarlar, kiberfırıldaqçılar, kiberxuliqanlardan və s. özünü qoruya bilsin. Bunun üçün istifadəçilər ilk növbədə İnternetdə işləyərkən, müxtəlif elektron xidmətlərdən istifadə edərkən üzləşə biləcəkləri təhlükələr barədə məlumatlı olmalıdırlar.

İTM-in formalaşdırılması və bu sahədə bacarıqların inkişaf etdirilməsi üçün insanların kütləvi təlimlərə cəlb edilməsi ilə yanaşı, geniş təbliğat-təşviqat işlərinin aparılması, "qaynar xətlər"in yaradılması mexanizmlərindən istifadə edilir.

Dünya ölkələri informasiya cəmiyyətinin inkişaf səviyyəsinə görə bir-birindən fərqlənsələr də, bütün ölkələrin informasiya təhlükəsizliyi problemləri, demək olar ki, oxşardır. Bu problemlərin həllinə yanaşmalar isə ölkənin mədəni səviyyəsindən və bu sahədəki milli hüquqi bazadan asılı olaraq fərqlənir.

Ölkələrin əksəriyyəti vətəndaşların ilk növbədə informasiya məkanında qarşılaşdıqları təhlükələr və bu təhlükələrdən qorunma mexanizmləri barədə məlumatlandırılması, onların İTM-nin səviyyəsinin artırılması üçün müxtəlif tədbirlər həyata keçirirlər. Bu cür tədbirlərdə ümumi informasiya təhlükəsizliyi məsələlərindən tutmuş, fərdi məlumatların qorunması, elektron imza, elektron şəxsiyyət vəsiqəsi, elektron tibbi xidmətlər, təhlükəsizlik risklərinin idarə edilməsi kimi konkret məsələlərə diqqət yetirilir [13].

Aparılan maarifləndirmə tədbirləri adi vətəndaşlardan tutmuş dövlət təşkilatlarında və özəl sektorda işləyən mütəxəssislərə qədər müxtəlif sosial qrupları əhatə edir.

İnkişaf etmiş ölkələrdə hakimiyyət tərəfindən dövlət qulluqçularının İTM-nin səviyyəsini artırmaq üçün, özəl sektorun nümayəndələri və bəzən vətəndaşlar da daxil olmaqla, çoxsaylı konfrans və seminarlar təşkil edilir. İTM-in formalaşdırılması üsullarından biri də pulsuz informasiya materiallarının, tövsiyə və təlimatların hazırlanması və yayılmasıdır. Təhlükəsizlik üzrə materialların yayılmasında çox vaxt televiziyanın imkanlarından, sosial şəbəkələrdən və SMS göndərişlərdən istifadə edilir.

Vətəndaşların informasiya təhlükəsizliyi məsələləri üzrə məlumatlılıq səviyyəsinin yüksəldilməsi istiqamətində ölkələr tərəfindən müxtəlif tədbirlər həyata keçirilir (şək. 1.).

Bu istiqamətdə ən geniş həcmli layihə ABŞ-da həyata keçirilmişdir. Orada istifadəçilərə öz kompüter sistemlərinin təhlükəsizliyini qorumasına dəstək məqsədilə, vaxtında faydalı informasiya verən Milli Kibermə lumatlandırma Sistemi (*National Cyber Awareness System*) yaradılmışdır. Məlumatlandırma sistemi kompüter hazırlığının müxtəlif səviyyəsinə malik istifadəçilər üçün (həm professionallar, həm də ev kompüterlərindən istifadə edən adi istifadəçilər üçün) nəzərdə tutulub. Bununla yanaşı, ABŞ-ın Federal ticarət komissiyası istehlakçıların maarifləndirilməsinə daha yaxşı töhfə vermək, informasiya təhlükəsizliyi ilə bağlı olan mövzulara aid çap nəşrlərinin və veb-nəşrlərin yayılmasını genişləndirmək məqsədi ilə uzun illərdir ki, Fişinqlə mübarizə üzrə İşçi Qrup, Milli Kibertəhlükəsizlik Alyansı və s. kimi koalisiyalarla əməkdaşlıq edir [14].

Koreya, Finlandiya, ABŞ və s. kimi bir sıra ölkələrdə vətəndaşların mövcud informasiya təhlükəsizliyi təhdidləri və onlardan qorunmaq üsulları haqqında məlumatlılıq səviyyəsini artırmaq məqsədi ilə mütəmadi olaraq informasiya təhlükəsizliyi həftəsi və ya günü təşkil olunur. Məsələn, Koreyada bununla yanaşı, informasiya təhlükəsizliyinin yaxşı

səviyyədə olmasını dəstəkləyən universitetlər və kompaniyalar üçün "İnformasiya təhlükəsizliyi mükafatı" təsis edilmişdir. Bundan başqa, Koreyada milli öyrədici turlar təşkil etmək, ən yeni informasiya təhlükəsizliyi texnologiyaları və siyasəti məsələlərini yaymaq üçün müxtəlif seminarlar təşkil etmək yolu ilə vətəndaşların İTM-nin səviyyəsini artırmağa çalışırlar.

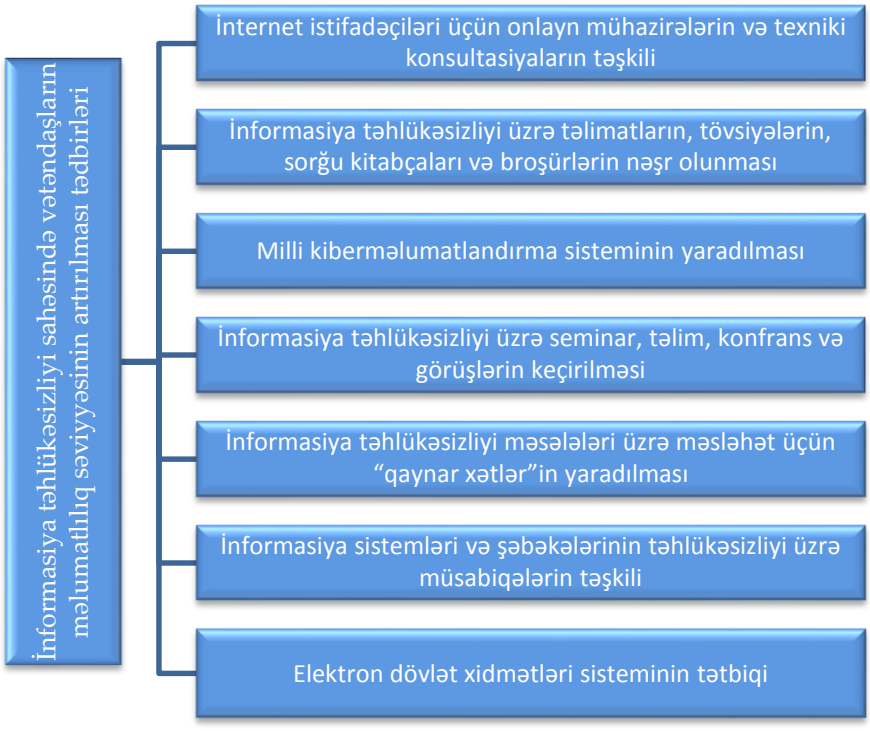
Kanadada vətəndaşlar üçün həm Kanada hökuməti, həm də qeyri-hökumət təşkilatları tərəfindən təqdim olunan bütün informasiya və xidmətlərə çıxışı təmin edən şlüz (*İstehlakçı İnformasiya Şlüzü - Consumer Information Gateway*) yaradılmışdır. Burada kibertəhlükəsizlik, kiberməkanda maliyyə konfidensiallığının qorunması, elektron alış-verişin təhlükəsizliyi, fərdi məlumatların qorunması, spamdan qorunma ilə bağlı çoxlu sayda nəşrlər təklif edilir.

Finlandiyada vətəndaşlarla informasiya təhlükəsizliyi məsələləri üzrə interaktiv diskussiyaların keçirilməsi məqsədi ilə onlayn forum yaradılmışdır. Bu forum vətəndaşların hökumət orqanları ilə ünsiyyətinə imkan yaradır. İnformasiya təhlükəsizliyi üzrə məsələlərin müzakirəsində informasiya təhlükəsizliyinin idarə edilməsi üzrə Hökumət Şurasının üzvləri fəal iştirak edirlər.

Qeyd edək ki, Finlandiyada informasiya təhlükəsizliyi siyasətinin işlənib hazırlanmasına və həyata keçirilməsinə cavabdeh olan dövlət qurumları Nəqliyyat və Kommunikasiya Nazirliyi və Verilənlərin Qorunması Ombudsmanıdır.

Yaponiyanın İqtisadiyyat, Ticarət və Sənaye Nazirliyi və Milli Polis Agentliyi qeyri-hökumət təşkilatları ilə birgə mütəmadi olaraq seminarlar keçirir və istifadəçilərə kompüter viruslarından və informasiyaya icazəsiz müdaxilədən qorunma üsulları barədə məlumatlar verilir. Eyni zamanda, Milli Polis Agentliyinin təhlükəsizlik portalında İnternet istifadəçiləri üçün təhlükəsizlik məsələləri üzrə onlayn mühazirələr və texniki konsultasiyalar təqdim edilir.

Norveçdə və İspaniyada da vətəndaşların informasiya təhlükəsizliyi sahəsində məlumatlılıq səviyyəsinin artırılması üçün saytlar fəaliyyət göstərir. Norveçdə yaradılan saytda müxtəlif təbəqədən olan insanlar (biznes nümayəndələri, yaşlılar, məktəblilər, müəllimlər, valideynlər və s.) üçün kurslar təklif edilir.



Şək 1. Vətəndaşların məlumatlılıq səviyyəsinin artırılması tədbirləri

Eyni zamanda, İnternetdə məxfiliyin (hesabların, fərdi məlumatların, şəkillərin) qorunması, sosial şəbəkələrdə və çatlarda davranış qaydası ilə bağlı məsləhətlər, İnternet-mağazalarda təhlükəsiz alış-verişlə, etibarlı parolların seçilməsi ilə, informasiya mübadiləsinin təhlükəsizliyinin təmin edilməsi ilə, viruslardan, kiberhücumlardan, troyanlardan, şpion proqram təminatlarından qorunma üsulları ilə bağlı tövsiyələr yerləşdirilir.

İspaniyada İnternet İstifadəçiləri Assosiasiyası tərəfindən informasiya təhlükəsizliyi məsələləri üzrə təbliğat kompaniyaları həyata keçirilir. Geniş ictimaiyyət üçün informasiya təhlükəsizliyi məsələləri ilə bağlı müxtəlif məlumatları özündə əks

etdirən sayt və portallar yaradılmışdır. Onlardan biri də "Kompüter təhlükəsizliyi və viruslar haqqında ilkin məlumat mərkəzi" tərəfindən yaradılan saytdır ki, burada İnternet istifadəçilərinə viruslar haqqında ətraflı məlumat və aktual xəbərdarlıqlar verilir. Saytda, həmçinin kompüter təhlükəsizliyi haqqında ümumi məlumatlardan, proqram təminatının təhlükəsizliyi üçün yeniləmələrdən, ekspertlərin konsultasiyalarından və diskussiya forumlarından yararlanmaq imkanı var.

Bir sıra inkişaf etmiş ölkələrdə kiçik və orta biznes nümayəndələrinin informasiya təhlükəsizliyi məsələləri üzrə məlumatlandırma səviyyəsinin artırılması üçün tədbirlər həyata keçirilir:

- Kiçik və orta biznes müəssisələri üçün təhlükəsizlik üzrə təlimat və tövsiyələrin hazırlanması;
- İnformasiya təhlükəsizliyi məsələləri üzrə seminarların təşkili;
- Sayt və portalların hazırlanması;
- Kiçik biznes üçün kompüter təhlükəsizliyi üzrə resurs mərkəzinin yaradılması;
- Biznesdə və idarəetmədə elektron vərdişlər proqramının həyata keçirilməsi;
- Və s.

İqtisadi Əməkdaşlıq və İnkişaf Təşkilatına üzv dövlətlər tərəfindən təhsil sferasında da şagird və müəllimlərin, valideynlərin, yeniyetmələrin İTM-nin formalaşdırılması üçün müxtəlif məlumatlandırma və təbliğat-təşviqat tədbirləri həyata keçirilmişdir.

4. Təhsil sferasında informasiya təhlükəsizliyi mədəniyyətinin formalaşdırılması tədbirləri

Əhalinin ən həssas qrupu olan uşaq və yeniyetmələrin İnternetdə təhlükəsizliyinin təmin edilməsi həm ölkələrin, həm də beynəlxalq təşkilatların diqqət mərkəzindədir. AB məkanında bu istiqamətdə bir sıra mühüm işlər görülmüşdür ki, onlardan biri də 1999-cu ildə qəbul edilmiş "Təhlükəsiz İnternet" Proqramı (Safer Internet Programme) idi [15]. Proqramın məqsədi qanunazidd kontent və şəbəkədə destruktiv davranışla mübarizə və uşaq və yeniyetmələrin məlumatlılıq səviyyəsinin artırılmasına nail olmaqla onların təhlükəsizliyinin təmin edilməsi idi. "Təhlükəsiz İnternet" Proqramının həyata keçirilməsinin əsas istiqamətləri bunlar idi:

- uşaq və yeniyetmələr üçün təhlükəsiz onlayn mühitin yaradılmasına yönəlmiş layihələrin maliyyələşdirilməsi;
- Təhlükəsiz İnternet Gününün dəstəklənməsi;
- Təhlükəsiz İnternet Forumunun təşkili;
- korporativ özünütənzimləmənin dəstəklənməsi və stimullaşdırılması;
- digər beynəlxalq təşkilatlarla qarşılıqlı əməkdaşlıq.

"Təhlükəsiz İnternet" Proqramı 1999-cu ildən başlayaraq mərhələli şəkildə (1999–2004-cü illər; 2005–2008-ci illər; 2009–2013-cü illər və s.) həyata keçirilmişdir.

Bütün Avropada vətəndaşların, o cümlədən uşaq və yeniyetmələrin İnternetdən təhlükəsiz istifadə qaydaları haqqında məlumatlılıq səviyyəsinin artırılması üçün AB-yə daxil olan ölkələrdə üç növ Təhlükəsiz İnternet Mərkəzləri (TİM) yaradılmışdır:

- məlumatlandırma mərkəzləri (awareness centers) – informasiya materialları yayır, uşaqların, valideynlərin, tərbiyəçilərin və müəllimlərin iştirakı ilə müşavirələr keçirirlər ki, uşaqların qarşılaşa biləcəyi potensial onlayn risklər və onların İnternetdə təhlükəsizliyinin təmin edilməsi üsulları barədə məlumatlılıq səviyyəsinin artırılmasına nail olsunlar;
- yardım xətləri (helplines) – şəbəkədə təhlükəsizliyin necə təmin edilməsi ilə bağlı uşaqlar, valideynlər və müəllimlər üçün fərdi konsultasiyalar keçirirlər;
- qaynar xətlər (hotlines) – İnternetdə aşkarlanmış qeyri-leqal kontentlə bağlı məlumatları qəbul edir.

Avropa ölkələrində informasiya təhlükəsizliyi sahəsində əhalinin məlumatlandırılması işini həyata keçirən TİM-lərin fəaliyyətini koordinasiya etmək üçün məlumat mərkəzlərini və yardım xətlərini əhatə edən "Insafe" Avropa Təhlükəsiz İnternet Mərkəzləri Şəbəkəsi yaradılmışdır [15]. Onlar ildə bir neçə dəfə bir araya gələrək təcrübələrini bölüşür, həmçinin informasiya və resurs mübadiləsi aparırlar. Şəbəkə İnternetdən təhlükəsiz istifadəni təmin etmək üçün ev və məktəb arasındakı əməkdaşlığın inkişaf etdirilməsinin vacib olmasını təbliğ etmək üçün məktəblər, ailələlər və digər əlaqədar təşkilatlarla əməkdaşlıq edir. Vətəndaşların, əsasən də uşaq və gənclərin hüquq və ehtiyaclarının qorunması məsələsinə münasibətdə məsuliyyətin hökumət, müəllimlər, valideynlər, kütləvi informasiya vasitələri və digər bu işə cəlb edilmiş qurumlar arasında bölünməsi vacib məsələlərdən biridir.

Uşaqlar və gənclər yaşlı nəslə nisbətən müasir texnologiyalar dövründə doğulduqları üçün texniki vərdişləri daha asanlıqla qavrayır və texnologiyalardan istidadədə çətinlik çəkmirlər. Buna görə də Məlumatlandırma Mərkəzləri informasiya təhlükəsizliyi haqqında məlumatlandırmanı daha səmərəli həyata keçirmək üçün gənclərin bilik və bacarıqlarından, potensialından da istifadə edirlər. Hazırda Məlumatlandırma Mərkəzlərinin strukturu çərçivə-

sində fəaliyyət göstərən gənclər qrupunun (youth panel) üzvləri həmyaşıdlarını və böyükləri İnternetin təhlükələrindən mühafizə üsulları barədə məlumatlandırırlar, ölkələrindəki milli İnternet şəbəkəsinin liderləri ilə görüşlər təşkil edir və onların xidmətlərini gənclər üçün necə faydalı və maraqlı etmək barədə müzakirələr aparırlar. Həmçinin faydalı, maraqlı, intellektual resursları seçir və istifadə üçün tövsiyə edirlər, İnternetin yaxşı və pis tərəfləri ilə bağlı müxtəlif videoçarxlar, komikslər və dərsliklər hazırlayırlar.

Təhlükəsiz İnternet Proqramı 2014-cü ildən "Uşaqlar üçün daha yaxşı İnternet" (ing. Better Internet for Kids) adlanır [16].

Bir çox dövlətlərdə artıq məktəb partasından kibertəhlükəsizlik üzrə mütəxəssis hazırlamağa başlayırlar. Belə ki, İsrail məktəblərində uşaqlar dördüncü sinifdən proqramlaşdırmanı öyrənirlər. Bu fənndən uğur qazanan məktəblilərə sertifikasiya mərkəzlərində kriptoqrafiya və kibertəhlükəsizlik üzrə əlavə dərslər tövsiyə olunur.

İngiltərədə gənclər arasında ildə bir dəfə kibertəhlükəsizlik üzrə yarışlar keçirilir. İngiltərə qanunvericiliyinə görə, hər il məktəb personalına təhlükəsizlik məsələlərinin, o cümlədən də İnternet təhlükəsizliyinin öyrədilməsi tələb olunur. İngiltərənin TİM ölkədə yeni təhsil texnologiyalarını dəstəkləyən və İnternetdə uşaqların təhlükəsizliyinin təmin edilməsi sahəsində aparıcı təşkilat olan SWGfL ilə birgə məktəblər, uşaq və gənclərlə işləyən digər təşkilatlar üçün elektron təhlükəsizlik üzrə bütün ölkəni əhatə edən geniş spektrli məşğələlər keçirirlər [17].

SWGfL tərəfindən hazırlanan 360 Degree Safe proqramı məktəblərə şəbəkədə özlərinin məxsusi təhlükəsizlik tədbirlərini qiymətləndirməyə, digərləri ilə müqayisə etməyə, yaxşılaşdırma tələb edilən sahələrdə prioritetləri müəyyən etməyə, eyni zamanda irəli getmək üçün məsləhət və dəstək almağa imkan verir.

Avstraliyada 2018-ci ildən etibarən blokçeyn və kriptoalqoritmlərin aşağı siniflərdən başlayaraq tədris edilməsinə başlanılmışdır. Bu da uşaqlara rəqəmsal təhsil almağa, həmçinin uşaqlar və böyüklər arasında rəqəmsal fərqliliyi aradan qaldırmağa imkan verir.

Amerikanın Milli Təhlükəsizlik Agentliyi tələbələr, məktəblilər, hətta uşaq bağçalarının tərbiyəçiləri üçün yay düşərgələri təşkil edir. İnformasiya texnologiyalarını yaxşı bilən məktəblilərin də daxil olduğu "ağ hakerlər" adlanan dəstələrin yaradılması təcrübəsindən geniş istifadə olunur. Bu dəstələr proqram təminatlarını müxtəlif boşluqlara görə test edirlər. İnformasiya təhlükəsizliyi üzrə mütəxəssislərin bacarıqlarının təkmilləşdirilməsi üçün informasiya təhlükəsizliyi və sistem administratorluğu üzrə CTF (Capture the flag) komanda yarışmaları təşkil olunur.

2008-ci ildə Koreya Respublikasında Beynəlxalq Kiberidman Federasiyası yaradılmışdır və o, hazırda dünyanın bir çox ölkələrində böyük populyarlıq qazanmışdır. Kompüter idmanı üzrə həm professional idmançılar, həm də həvəskarlar, o cümlədən tələbələr və şagirdlər arasında yarışlar keçirilir. Bununla yanaşı, bir çox təhsil müəssisələri oyun texnologiyaları sahəsində kompüter elmləri üzrə tədris proqramları həyata keçirirlər. Finlandiyanın (Orivesi) Ahlman professional kolleci üç istiqamət üzrə təhsil təşkil edir: "kompüter oyunlarının işlənib hazırlanması texnologiyaları", "kompüter oyunlarının dizaynı", "kiberidman" [18].

2021-ci ildə Yunanıstanın TİM-i təhsilin hər bir səviyyəsi üçün yeni rəqəmsal materiallar hazırlayıb [19]. "Yenidən məktəbə" adlı paket TİM-in veb-saytında yeləşdirilib, bu vəsait kiçik yaşlı uşaqlardan tutmuş, yuxarı sınıf şagirdləri, valideynlər və pedaqoqlara qədər hər kəsə ünvanlanıb. Bu materialların köməyi ilə orta məktəb şagirdlərinin İnternetdə nifrət dili mövzusu üzrə məlumatlandırmağa cəhd edilir, hansı ki, son dövrlərdə İnternetdə geniş yayılıb. Müxtəlif tədbirlər vasitəsilə təhsil alanlara nifrət dilini tanımağı və şəraitdən asılı olaraq ona eyni dərəcədə reaksiya verməyi öyrədirlər. Bu il tələbələrin kiberdələduzluq haqqında məlumatlandırılmasına xüsusi əhəmiyyət verilib: onları dələduzlardan necə qorumaq olar və onlar bu halla üzləşdikdə necə reaksiya verməlidirlər. İnteraktiv təqdimatlar və viktorinaların köməyi ilə təhsil alanlar viruslar və onlardan qorunma üsulu barədə, məsələn, etibarlı parollardan istifadə etmək, e-məktubun və ya məlumatın təhlükəli olub-olmamasını müəyyən etmək, fişinqdən necə müdafiə olunmaq barədə məlumat əldə edirlər. Hətta kiçik yaşlı uşaqlara da nağıl qəhrəmanlarının köməyi ilə İnternetdən düzgün istifadə qaydaları aşılanır.

Portuqaliyanın Milli Kibertəhlükəsizlik Mərkəzi tərəfindən bütün sahələrdə, eyni zamanda təhsil sahəsində çalışan işçilər üçün genişmiqyaslı onlayn açıq kurslar təşkil edilir. 2019-cu ildə "Vətəndaş kibertəhlükəsizlikdə" adlı kurs işlənib hazırlanmışdır [16]. Bu iqtisadiyyatın müxtəlif sahələrində çalışan sıravi işçilər üçün "kiber-gigiyena"ya aid tövsiyələr, praktiki vərdişlər aşılayır, birinci ildə 30 mindən çox vətəndaş bu kurslarda iştirak etmişdir. Kursda iştirak edənlərin rəyləri, arzuları və qeydləri əsasında dezinformasiya, onlayn rejimdə alış-veriş və sosial şəbəkələrdən təhlükəsiz istifadə mövzuları kursun proqramına daxil edilmişdir.

2017-ci ildə Brüsseldə keçirilən kibertəhlükəsizlik üzrə tədbirdə [20] AB ölkələrinə çağırış edilib ki, onlar kibertəhlükəsizliyi akademik və professional hazırlıq üzrə tədris proqramlarına daxil etmələri ilə bağlı özlərinə öhdəlik götürsünlər. Qeyd edilir ki, uşaq və gənclərin kritik təfəkküründü möhkəmləndirmək, onların mediasavadlılıq səviyyəsini yüksəltmək lazımdır ki, saxta məlumatların məzmununda olan təhdidlərə, kiber hədə-qorxulara, kibertəhlükəsizlik təhdidlərinə və dələduzluğa adekvat reaksiya verə bilsinlər.

Sənəddə deyilir ki, kibertəhlükəsizliyin tədrisi yalnız İT-mütəxəssislərlə məhdudlaşmamalı, mühəndis işi, biznes-menecment, hüquq və digər sahələr üzrə tədris proqramlarına da daxil edilməlidir. Nəhayət, müəllimlər və orta məktəblərin şagirdləri kibercinayətkarlıq və kibertəhlükəsizlik üzrə məlumatlandırılmalıdırlar. İnsidentlərin 95%-i qəsdən və ya bilməyərəkdən, insan səhvi üzündən baş verdiyi üçün, kibertəhlükəsizlik üzrə məsuliyyət hər kəsin üzərinə düşür.

5. Nəticə

İnformasiya cəmiyyətinin hərtərəfli inkişafına nail olmaq, rəqəmsal iqtisadiyyata keçidin, eyni zamanda həm dövlət və kommersiya müəssisələrinin, həm də vətəndaşların informasiya təhlükəsizliyinin təmin edilməsi üçün cəmiyyətdə İTM-i inkşaf etdirmək olduqca vacibdir.

Beynəlxalq təşkilatlar və ayrı-ayrı ölkələrdə cəmiyyətdə İTM-in səviyyəsinin artırılması və inkişaf etdirilməsi üçün bir neçə istiqamətdə tədbirlər həyata keçirilir: mütəxəssislərin informasiya təhlükəsizliyi üzrə kompetensiyalarının artırılması və onun qiymətləndirilməsi; dövlət işçilərinin, kiçik və orta biznes nümayəndələrinin informasiya təhlükəsizliyi sahəsində məlumatlılıq səviyyəsinin artırılması; yaşlı insanlar da daxil olmaqla, vətəndaşların məlumatlılıq səviyyəsinin yüksəldilməsi; təhsil sistemində uşaq və gənclərin, müəllimlərin, valideynlərin informasiya təhlükəsizliyi riskləri və onlardan qorunma üsulları, eyni zamanda etik davranış normaları və s. barədə məlumatlandırılması.

Xarici təcrübənin təhlili və ölkəmizdə də son dövrlərdə İnternetdə müxtəlif kibercinayətlər (kiberbullinq, feyk məlumatların yayılması, vətəndaşların bank kartlarına aid məlumatların ələ keçirilməsi, videogörüntülərlə şantaj, sosial şəbəkələrdə insanların təhqir olunması və s.) onu deməyə əsas verir ki, bu problemin həlli yolu vətəndaşlara kütləvi şəkildə İnternetdə təhlükəsiz davranış bacarıqlarının öyrədilməsi sisteminin yaradılmasından keçir. Eyni zamanda bu təlim fasiləsiz olmalı və uşaq bağçalarından başlamış ali təhsil müəssələrinə qədər təhsilin bütün səviyyələrini əhatə etməlidir.

Ədəbiyyat

1. Okere I., Van Niekerk J.F., Carroll M. (2012). Assessing information security culture: A critical analysis of current approaches. Information Security for South Africa, October 2012, (pp.1—8). https://doi.org/10.1109/ISSA.2012..6320442
2. Alvarez-Dionisi, L. E., Urrego-Baquero, N. (2019). Implementing a Cybersecurity Culture. ISACA Journal, 2., 1-7.
3. Corradini I., Nardelli E. (2020). Social Engineering and the Value of Data: The Need of Specific Awareness Programs. International Conference on Applied Human Factors and Ergonomics. Advances in Human Factors in Cybersecurity, (pp.59—65). https://doi.org/10.1007/978-3-030-20488-4_6
4. Mahmudova R.Ş. (2021). Fərdin və cəmiyyətin informasiya təhlükəsizliyi mədəniyyətinin bəzi aspektləri haqqında. İnformasiya cəmiyyəti problemləri, 1, 56-66. https://doi.org/10.25045/jpis.v12.il.05.
5. Петренко, С.А., Петренко, А.А. (2015). Киберучения: методические рекомендации ENISA. Вопросы кибербезопасности: научно-практический журнал, 3(11), 2-14.
6. OECD Guidelines for the Security of Information Systems and Networks: Towards a Culture of Security. https://www.oecd.org/sti/ieconomy/15582260.pdf.
7. Сладкова, Н.М., Ильченко, О.А., Степаненко, А.А., Шапошников, В.А. (2021). Особенности оценки компетенций по информационной безопасности государственных муниципальных служб. Вопросы государственного и муниципального управления, 1, 122-149.
8. AB Kibertəhlükəsizlik Agentliyinin rəsmi saytı. https://www.enisa.europa.eu/publications/raising-awareness-of-cybersecurity/@@download/fullReport.
9. Двинских, Д.Ю., Талапина, Э.В. (2019). Риски развития оборота данных в государственном управлении. Вопросы государственного и муниципального управления, 3, 7–30.
10. Competency Model for Cybersecurity (2011). https://www.chcoc.gov/content/competency-model-cybersecurity.
11. National Initiative for Cybersecurity Education (NICE): Cybersecurity Workforce Framework. 2017. https://nvlpubs.nist.gov/nistpubs/specialpublications/nist.sp.800-181.pdf
12. Secure Trust Bank PLC Annual Report & Accounts 2020. https://www.securetrustbank.com/images/InvestorRelations/r2020/STB-Pillar-3-Annual-Disclosures-2020-Final.pdf
13. Малюк, А.А., Полянская, О.Ю. (2016). Зарубежный опыт формирования в обществе культуру информационной безопасности. Безопасность информационных технологий, 4, 25-37.
14. Cybersecurity&Infrastructure Security Agency. https://www.cisa.gov/uscert/ncas.
15. Safer Internet Programme: Emprowering and Protecting Children Online. Europe's Information Society. http://ec.europa.eu/ information_society/activities/sip/index_en.htm
16. AB-nin "Better Internet for Kids" Proqramı. https://www.betterinternetforkids.eu/en-GB/home
17. İngiltərədə uşaqların İnternetdə təhlükəsizliyini təmin edən təşkilatın saytı. https://swgfl.org.uk/.

18. Finlandiyanın Ahlman Kollecinin rəsmi saytı. https://www.ahlman.fi/
19. Yunanıstanın Təhlükəsiz İnternet Mərkəzinin rəsmi saytı. https://www.betterinternetforkids.eu/en-GB/sic/greece
20. Joint Communication of the European Commission and European External Action Service: Re-silience, Deterrence and Defence: Building strong cybersecurity for the EU. https://ec.europa.eu/digital-single-market/en/news/building-strong-cybersecurity-europe

Rasmiya Sh. Mahmudova
Azerbaijan National Academy of Sciences, Institute of Information Technology, B. Vahabzade str., 9A, AZ1141, Baku, Azerbaijan

Расмия Ш.Махмудова
Национальная Академия Наук Азербайджана, Институт Информационных Технологий, ул. Б.Вахабзаде, 9A, AZ1141, Баку, Азербайджан
0000 – 0002 – 5816 – 9373