

Кімге: Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрлігі
Автор: Қожабай Айсұлтан Рахатұлы, Ұлытау ауданы әкімі аппаратының құжаттамалық қамтамасыз ету, ақпараттық бақылау бөлімінің бас маманы
Күні: 22.04.2025

АНАЛИТИКАЛЫҚ ЖАЗБА

Тақырыбы: Киберқауіпсіздік деңгейі және халықтың ақпараттық қауіпсіздік мәдениеті

Кілт сөздер: киберқауіпсіздік, дербес деректер, фишинг, ақпараттық қауіпсіздік, цифрлық мәдениет

Кіріспе

Қазіргі заман – цифрлық технологиялар дәуірі. Ақпарат ағынының артуы, интернетке тәуелділіктің күшеюі, сондай-ақ онлайн қызмет түрлерінің дамуы қоғам өмірінің барлық саласына әсер етуде. Осындай өзгерістер жағдайында ақпараттық қауіпсіздік мәселесі, соның ішінде киберқауіпсіздік өзекті тақырыптардың біріне айналды. Алайда техникалық қауіпсіздік шараларының дамуына қарамастан, көп жағдайда қауіптің негізгі көзі – қоғам мүшелерінің ақпараттық қауіпсіздік мәдениетінің төмендігі болып отыр.

Бұл зерттеудің мақсаты – қазіргі қоғамдағы киберқауіпсіздік деңгейін бағалау және қоғамның ақпараттық қауіпсіздік мәдениетінің қалыптасу деңгейіне талдау жасау. Сонымен қатар, қоғамдағы қауіпсіздікке деген қатынас пен ақпараттық сауаттылықтың киберқауіпсіздікке қалай әсер ететінін анықтау көзделеді[1].

Мәселенің өзектілігі – кибершабуылдар санының жыл сайын артуында ғана емес, сонымен қатар адамдардың жеке деректерін, қаржылық ақпараттарын қорғау бойынша білімінің жеткіліксіздігінде. Бұл қауіп жеке азаматтармен қатар, мемлекеттік және коммерциялық құрылымдарға да кері әсерін тигізуде.

Зерттеу әдістері ретінде:

- ашық статистикалық деректерге шолу,
 - отандық және шетелдік тәжірибелерді салыстырмалы талдау,
 - аналитикалық мақалалар мен сарапшылар пікірлеріне сүйену
- қарастырылды.

Негізгі бөлім

Соңғы жылдары кибершабуылдар саны күрт артып келеді. Қазақстанда 2023 жылы ғана 20 мыңнан астам кибероқиға тіркелген. Бұл – тек тіркелген жағдайлар, ал тіркелмеген немесе мойындалмаған оқиғалар одан да көп болуы мүмкін. Мемлекеттік құрылымдар, банктер, оқу орындары мен жеке тұлғалар шабуыл нысанына айналууда.

Мемлекеттік деңгейдегі шаралар ретінде «Киберқалқан» бағдарламасы іске қосылды. Сонымен қатар, “CERT-KZ” ұлттық компьютерлік инциденттерге әрекет ету қызметі жұмыс істейді. Бұл құрылымдар техникалық тұрғыдан қауіпсіздікті қамтамасыз етуде маңызды рөл атқарады[2].

2. Қоғамның ақпараттық қауіпсіздік мәдениеті

Халықтың көп бөлігінде ақпараттық қауіпсіздікке қатысты базалық білім мен дағдылар жетіспейді. Мысалы:

- Қиын емес құпиясөздер қолдану;
- Белгісіз сілтемелерге өту;
- Жалған интернет дүкендерге сену;
- Wi-Fi желілерін тексерусіз пайдалану;
- Әлеуметтік желілердегі фейк аккаунттардан сақтанбау.

Осындай әрекеттер кибершабуылға жол ашады. Бұл мәселенің басты себебі – ақпараттық сауаттылықтың төмендігі және бұл бағытта жүйелі білім берудің жеткіліксіздігі.

3. Негізгі сын-қатерлер мен қиыншылықтар

- Техникалық тұрғыдан артта қалу – көптеген мекемелер ескі жүйелермен жұмыс істейді;
- Мамандар тапшылығы – білікті киберқауіпсіздік сарапшылары жетіспейді;
- Құқықтық регламенттердің әлсіздігі – кибершабуыл жасаушыларға қатысты нақты жазалау тетіктері әлі де жетілмеген;
- Халықтың немқұрайлылығы – көпшілік киберқауіпсіздік мәселесін тек IT мамандарының міндеті деп санайды[3].

4. Даму сценарийлері

1. Пессимистік сценарий – ақпараттық қауіпсіздік мәдениетін дамытуға мән берілмесе, кибершабуылдар саны арта береді. Бұл жеке деректердің таралуына, қаржылық шығындарға, тіпті ұлттық қауіпсіздікке қатер төндіруі мүмкін.

2. Оптимистік сценарий – мемлекет пен қоғам бірлесе отырып ақпараттық сауаттылықты арттырса, ақпараттық қауіпсіздік мәдениеті қалыптасып, шабуылдарға қарсы тұру қабілеті артады.

3. Базалық сценарий – тек техникалық қорғаныс шараларын жетілдіру арқылы мәселенің бір бөлігін ғана шешу. Бұл уақытша нәтиже береді, бірақ қоғамда түбегейлі өзгеріс болмайды[4].

Халықаралық тәжірибе

Әлем елдері киберқауіпсіздікті қамтамасыз ету мен ақпараттық қауіпсіздік мәдениетін дамытуда түрлі тәсілдер қолдануда. Олардың кейбір табысты тәжірибелері Қазақстан үшін үлгі бола алады.

Эстония – цифрлық мемлекеттің озық үлгісі. 2007 жылы бұл елге қарсы кең ауқымды кибершабуыл жасалғаннан кейін, үкімет киберқауіпсіздік саясатын түбегейлі қайта қарап, ұлттық киберқауіпсіздік орталығын құрды. Сонымен қатар:

- Цифрлық сауаттылық мектеп қабырғасынан бастап үйретіледі;
- e-Government (электронды үкімет) жүйесінде көпсатылы аутентификация қолданылады;
- Мемлекеттік қызметкерлер регулярлы түрде киберқауіпсіздік бойынша оқудан өтеді[5].

Израиль – әлемдегі ең дамыған киберқауіпсіздік инфрақұрылымына ие елдердің бірі.

- Елде киберқауіпсіздік әскери сала деңгейінде қарастырылады;
- Университеттер мен жоғары оқу орындарында киберқауіпсіздікке маманданған бөлімдер бар;
- Мемлекет пен жеке сектор арасында ақпарат алмасудың тиімді жүйесі жолға қойылған[6].

Сингапур үкіметі 2016 жылы Ұлттық киберқауіпсіздік стратегиясын жариялап, киберқауіпсіздік бойынша инновациялық экожүйе құрды.

- Cyber Security Agency (CSA) арқылы мемлекеттік және жеке секторлармен тығыз жұмыс жүргізіледі;
- Азаматтарға арналған “Cyber Safe” бағдарламасы арқылы киберсауаттылықты арттыру жолға қойылған;
- Балабақшадан бастап мектептерге дейін цифрлық қауіпсіздік ережелері үйретіледі.

АҚШ-та киберқауіпсіздікке қатысты саясат көп деңгейлі:

- CISA (Cybersecurity and Infrastructure Security Agency) – елдің негізгі инфрақұрылымын кибершабуылдардан қорғайды;
- Жеке секторда киберқауіпсіздікке миллиардтаған доллар инвестиция бөлінеді;
- Ақпараттық қауіпсіздік мәдениеті HR саясатының бір бөлігі ретінде қарастырылады (яғни әр қызметкердің киберқауіпсіздік бойынша жауапкершілігі бар)[7].

Осы мысалдардан көріп отырғанымыздай, дамыған елдер киберқауіпсіздікті тек техникалық мәселе емес, қоғамдық мәдениеттің бір бөлігі ретінде қарастырады. Бұл тәжірибе Қазақстан үшін де өзекті, әрі бейімделуге болатын бағыт.

Қорытынды

Киберқауіпсіздік – бұл тек техникалық сала емес, ол бүкіл қоғамның мәдениеті мен санасына тікелей байланысты. Қазақстандағы киберқауіпсіздік саласында айтарлықтай жұмыстар атқарылғанымен,

халықтың ақпараттық қауіпсіздікке деген қатынасы, білім деңгейі мен тәжірибесі әлі де жеткіліксіз.

Зерттеу барысында анықталған негізгі мәселелердің бірі – ақпараттық қауіпсіздік мәдениетінің қалыптаспауы. Бұл өз кезегінде кибершабуылдардың жиілеуіне, жеке және мемлекеттік деңгейдегі ақпараттардың таралуына, қаржылық шығындарға және ұлттық қауіпсіздікке қатер төндіруі мүмкін.

Халықаралық тәжірибе көрсеткендей, ақпараттық қауіпсіздік мәдениетін ерте жастан бастап қалыптастыру, мемлекеттің жүйелі саясаты мен қоғамның белсенді қатысуы ғана бұл мәселеге нақты шешім бола алады. Тек техникалық шешімдермен шектелу – уақытша әрі әлсіз қорғаныс.

Сондықтан, киберқауіпсіздікке жауапкершілікті тек мемлекетке немесе IT мамандарына жүктемей, әрбір азамат өзінің ақпараттық қауіпсіздік деңгейін көтеруге тиіс. Бұл — болашақта қауіпсіз әрі сенімді цифрлық қоғам құрудың басты алғышарты.

Ұсынымдар

Қоғамдағы ақпараттық қауіпсіздік мәдениетін дамыту және киберқауіпсіздік деңгейін арттыру үшін келесі бағыттарда нақты шаралар қабылдау қажет:

1. Ақпараттық сауаттылықты арттыру
 - Мектеп пен жоғары оқу орындарында цифрлық қауіпсіздік негіздерін міндетті пән ретінде енгізу;
 - Қоғамға арналған онлайн курстар мен семинарлар ұйымдастыру арқылы тұрғындардың білімін арттыру.
2. Жүйелі мемлекеттік саясат жүргізу
 - Киберқауіпсіздікке қатысты ұлттық стратегияны жаңарту және оны кезең-кезеңімен іске асыру;
 - Мемлекеттік құрылымдарда жұмыс істейтін мамандардың цифрлық қауіпсіздік бойынша біліктілігін арттыру.
3. Жеке сектор мен мемлекеттік ұйымдар арасында серіктестік орнату
 - Ақпарат алмасу және бірлескен қауіпсіздік шараларын жүзеге асыру үшін мемлекет–бизнес серіктестігін дамыту;
 - Бизнеске арналған киберқауіпсіздік стандарттарын енгізу және бақылау.
4. Құқықтық және техникалық базаны жетілдіру
 - Кибершабуыл жасағандарға арналған заңнамалық жауапкершілікті қатаңдату;
 - Ақпараттық жүйелердің қауіпсіздігін тексеру үшін регулярлы аудиттер жүргізу.
5. Қоғамдық сана мен мәдениетті қалыптастыру

- Ақпараттық қауіпсіздікке бей-жай қарамау үшін әлеуметтік жарнама мен БАҚ арқылы насихат жүргізу;
- Әрбір азаматтың өз деректеріне жауапкершілікпен қарауын қалыптастыру.

Пайдаланылған дереккөздер тізімі

- 1.ҚР Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрлігі
- 2.ЦАРКА – Кибершабуылдарды талдау және тергеу орталығы
- 3.Stat.gov.kz – Ұлттық статистика бюросы
- 4."Цифрлық Қазақстан" бағдарламасы
- 5.Cybersecurity Guide 2023, OECD
- 6.Estonian Information System Authority – www.ria.ee
7. McAfee Cybersecurity Report, 2023