ӘОЖ 004:343.72

ЦИФРЛАНДЫРУ ДӘУІРІНДЕГІ ДЕРБЕС ДЕРЕКТЕРДІҢ ҚОРҒАЛУЫ

Тілеп Т.С., академик Е.А. Бөкетов атындағы Қарағанды университеті, Қарағанды, Қазақстан

Бүгінде әлем жаңа даму сатысына қадам басуда. Ақпараттық саланың жедел өсуі жаһандану үдерісімен одан әрі үдей түсуде. Заманауи технологиялардың, цифрлық және ақпараттық-коммуникациялық құралдардың кеңінен таралуы ақпараттарға қолжетімділік артты. Қазіргі таңда Интернет кеңістігінде адамдар кез-келген ақпаратты таба алады. Және сол ақпараттарға қол жеткізу барысында өздерінің жеке бас мәліметтерін толтыруы жиі кездеседі. Осы тұрғыда елімізде киберқылмыс мәселесі туындап отыр.

Адамның жеке өмірге қол сұғылмаушылық құқығының негізгі құрамдас бөліктерінің бірі оның дербес деректерін қорғау болып табылады. Цифрлық-технологиялардың қарқынды дамуы елімізде киберқылмыстың санының күрт өсуіне алып келуде. Қазіргі таңда азаматтардың дербес деректерінің таралуы қауіп-қатерлер мен онлайн-тәуекелдердің жаңа форматтарының пайда болуына әкеліп соқты. Барлық азаматтар интернет желілерінің белсенді пайдаланушылары болып табылады, бірақ барлығы бірдей интернет кеңістігіндегі қауіпсіздікті біле бермейді.

Дербес деректердің таралуы — күрделі мәселе, себебі құпия ақпараттың әшкере болуы бизнеске, мемлекеттік мекемелерге, ұйымдарға және жеке тұлғаларға ауыр зардаптар тигізуі ықтимал. Бүгінгі таңда елімізде дербес деректердің таралуына байланысты көптеген келеңсіз жағдайлар орын алуда. Бірі интернет желісінде жеке тұлғалардың денсаулығына байланысты ақпараттар болса, бірі интернет желілерінің қарқынды қолданушылары блогерлердің, әншілердің қаражат мәселелеріне қатысты. Бірақ бұл ақпараттардан бөлек, күнделікті өмірде адамдардың жеке ақпараттарының таралуы қарқынды жүруде.

Дербес деректердің қауіпсіздігіне төнетін қауіп-қатерлер деп — оларды жинау мен өңдеу барысында рұқсат етілмеген, оның ішінде кездейсоқ қол жеткізуге мүмкіндік беретін жағдайлар мен факторлардың жиынтығын түсінеміз. Мұндай жағдайлар дербес деректердің жойылуына, өзгертілуіне, бұғатталуына, көшірмесінің алынуына, үшінші тұлғаларға рұқсатсыз берілуіне, таралуына немесе басқа да заңсыз әрекеттерге әкелуі мүмкін.[1]

Интернет-алаяқтар дербес деректерді алу үшін әртүрлі әдістер мен айла-амалдарды қолданады. Фишинг әдісі арқылы - алаяқтар жалған сайттар мен электрондық хаттар арқылы адамды өз логині мен құпиясөзін енгізуге мәжбүрлейді. Smishing & Vishing - смс арқылы зиянды сілтемелерге кіреді. Жалған мобильді қосымшалар - банктік немесе танымал сервистер қолданбалары арқылы жеке мәліметтер жиналады. Data leak - кейде жеке мәліметтер e-gov, казпошта, банктер, дүкендер немесе басқа ұйымдар базалары арқылы таралып кетеді.[2]

Киберқылмыстың құрбандары болып қарт адамдар, ересектер, балаларда табылуда. Әр санат өз қызығушылықтарына байланысты интернет желісі ұсынған ақпараттарды алу кезінде құрбанына айналады.

Дербес деректер – мәліметтер негізінде айқындалған немесе айқындалатын дербес деректер субъектісіне қатысты, электрондық, қағаз және (немесе) өзге де материалдық жеткізгіште тіркелген сол мәліметтер. Қазақстан Республикасы дербес деректерді қорғауды Қазақстан Республикасының 2013 жылғы 21 мамырдағы № 94-V «Дербес деректер және оларды қорғау туралы» Заңында белгіленген құқықтық, ұйымдастырушылық және техникалық шаралар кешені арқылы қамтамасыз етеді. Бұл шараларға деректерді жинау мен өңдеуге шектеу қою, оларды сақтау мен беру кезінде криптографиялық құралдар арқылы қауіпсіздігін қамтамасыз ету, жауапты тұлғаларды тағайындау, дерек иелерінің құқықтарын сақтау, сондай-ақ құқықбұзушылықтар үшін әкімшілік және қылмыстық жауапкершілікке тарту жатады. Аталған шараларға талдау жасайтын болсақ, дербес деректермен жұмыс істейтін операторлар олардың ұйымдастырылуы, сақталуы және қауіпсіздігі үшін жауапты қызметкерлерді міндетті түрде тағайындауы қажет. Сонымен қатар, дербес деректермен жұмыс істеу тәртібін айқындайтын ішкі нормативтік құжаттарды әзірлеп, бекітуі тиіс. Персонал қолданыстағы заңнама талаптарымен және ұйым ішіндегі деректерді қорғау саясаты бойынша міндетті түрде таныстырылып, оқытылуы қажет. Деректерге қол жеткізуге рұқсаты бар қызметкерлердің нақты тізімі анықталып, бекітілуі тиіс. Сонымен бірге, пайдаланушылардың әрекеттерін тіркеу және қадағалау үшін оқиғалар журналын жүргізу тәртібі қарастырылуы қажеттігі құқықтық қорғау кешеңінің мәнін ашпақ.[3]

Сонымен қатар, ұйымдастырушылық кешеніне тоқталатын болсақ, дербес деректерді өңдеуші операторлар деректердің сақталуы мен қауіпсіздігін қамтамасыз ету үшін жауапты тұлғаларды тағайындауы тиіс. Сонымен қатар, персоналмен жұмыс істеу тәртібін анықтайтын ішкі нормативтік құжаттарды әзірлеп, бекіту міндетті. Қызметкерлер қолданыстағы заңнамалық талаптармен және ұйымның деректермен жұмыс істеу саясатына сәйкес міндетті түрде таныстырылып, оқытылуы қажет. Дербес деректерге қол жеткізе алатын қызметкерлер тізімі нақты айқындалуы тиіс. Сондай-ақ, пайдаланушылардың әрекеттерін тіркеу және бақылау мақсатында арнайы журналдар жүргізілуі қажет.

Ал техникалық шаралар ретінде, дербес деректерді сақтау және беру кезінде, әсіресе шектеулі қолжетімділігі бар ақпаратпен жұмыс істегенде, криптографиялық қорғау құралдарын міндетті түрде қолдану талап етіледі. Ақпараттық жүйелерді қорғау үшін антивирус бағдарламалары, жүйелік қалпына келтіру құралдары, деректердің тұтастығын бақылау жүйелері, сондай-ақ пайдаланушыларды сәйкестендіру және аутентификациялау құралдары кеңінен қолданылады. Сонымен қатар, ақпараттық ресурстар мен деректерді өңдеуге арналған бағдарламалық және техникалық құралдарға қолжетімділікті шектеу де маңызды шаралардың бірі болып саналады. Бұған қоса, дербес деректер сақталатын серверлер мен физикалық нысандардың күзеті қамтамасыз етілуі тиіс.

Кибершабуыл әдістері туралы хабардар болғанына қарамастан, көптеген адамдар алаяқтардың алдында осал болып қалады. 2025 жылғы қаңтар-наурыз аралығында Қазақстанда ақпараттық қауіпсіздік саласында 30 мың оқиға

тіркелді-бұл өткен жылдың сәйкес кезеңімен салыстырғанда 2 есе көп. Елімізде киберқылмысқа байланысты бірқата шаралар жүргізілуде. Мемлекеттік органдар азадамттарға жеке ақпараттармен инетрент желісінде бөліспеуін, дербес деректерін үшінші тараптарға таратпауын, онлайн дүкендерге тіркелерде жеке ақпараттарын тотырмаулары жөнінде ұдайы ақпарат ұсынып отырады.[4]

Қазақстанда дербес деректердің таралу фактілері бойынша Қылмыстық кодекстің 211-бабы және Әкімшілік құқық бұзушылық туралы кодекстің 79-бабы аясында қылмыстық және әкімшілік істер қозғалады. Зардап шеккен азаматтар моральдық зиянды өтеу және келтірілген шығынды қалпына келтіру үшін сотқа жүгіну құқығына ие. Ал деректердің таралуына жол берген ұйымдар айыппұл түрінде жауапкершілікке тартылады.

ҚР Қылмыстық Кодексінің 211-бабы «Қолжетімділігі шектелген электрондық ақпараттық ресурстарды құқыққа сыйымсыз тарату». Бұл бап азаматтардың дербес деректері немесе заң бойынша немесе меншік иесі белгілеген қолжетімділігі шектелген басқа да ақпараттарды қамтитын электрондық ақпараттық ресурстарды заңсыз таратуға жауапкершілік жүктейді. Объектісі болып Ақпараттық қауіпсіздік пен азаматтардың жеке өмірге қол сұғылмау, дербес деректерді қорғау саласындағы құқықтық қатынастар табылады. Объективтік жағы қолжетімділігі шектелген электрондық ақпараттық ресурстарды құқыққа қайшы тарату фактісі. Субъектісіне 16 жасқа толған, есі дұрыс жеке тұлға, жеке немесе заңды тұлғаның өкілі болуы мүмкін (мысалы, қызметкер, ақпарат иесі, техникалық қолжетімділігі бар адам). Субъективтік жағы тікелей қасақаналық. Мақсат – пайда табу, зиян келтіру немесе жай қызығушылықтан тарату болуы мүмкін. Санкциясы:Айыппұл салу – 2 000 АЕК-ке дейін; Қоғамдық жұмыстарға тарту – 600 сағатқа дейін; Түзеу жұмыстары – 2 жылға дейін; Бас бостандығын шектеу – 2 жылға дейін; Бас бостандығынан айыру – 2 жылға дейін.[5]

ҚР Әкімшілік құқық бұзушылық туралы Кодексінің 211-бабы «Қазақстан Республикасының дербес деректер және оларды қорғау туралы заңнамасын бұзу». Бұл баптың қорғалатын қоғамдық қатынастары — дербес деректердің заңды түрде қорғалуы мен олардың өңделуінің дұрыс жүргізілуі. Нақтырақ айтсақ, халықтың жеке ақпараттары (деректері) жинау, өңдеу, сақтау, жеткізу, қорғау мәселелері. Объективтік жағы дербес деректерді заңсыз жинау немесе өңдеу; Дербес деректерді қорғау шараларын сақтау міндетін бұзу (мысалы, ақпараттық қауіпсіздік немесе техникалық/ұйымдастырушылық шараларды қолданбау); Бұл іс-әрекеттер қылмыстық жауапкершілікке жатпайтын жағдайларда жүзеге асырылады; яғни, әкімшілік шарамен жауаптылық қарастырылған жағдайлар. Субъектісі қатарына жеке тұлғалар, Лауазымды тұлғалар;Медиация, адвокаттар, жеке нотариустар, жеке сот орындаушылары; Шағын, орта және ірі кәсіпкерлік субъектілері; Үкіметтік емес ұйымдар және басқа да ұйымдар, деректерді оператор ретінде немесе олардың өңдеушілері ретінде әрекет еткендер. Субъективтік жағы қасақана немесе немқұрайды түрде құқық бұзу ниеті. Санкциясы Жеке тұлғаларға — белгілі бір айлық есептік көрсеткіштер (АЕК) мөлшерінде; Лауазымды тұлғалар, шағын кәсіпкерлер, адвокаттар және т.б. ұйымдарға — айтарлықтай үлкенірек мөлшер; Орта және ірі кәсіпкерлік субъектілері үшін — одан да жоғары мөлшер.[6]

Екі баптың да мақсаты – дербес деректерді қорғау және ақпараттық қауіпсіздікті қамтамасыз ету. Олар әсіресе қолжетімділігі шектелген деректерге қатысты деректермен заңсыз әрекет ету жағдайларын реттейді және азаматтардың жеке өмірге қол сұғылмау құқығын бұзудың алдын алуға бағытталған. ҚР ҚК-нің 211-бабы мен ҚР ӘҚБтК-нің 79-бабы да дербес деректерге рұқсатсыз қол жеткізу, оларды пайдалану, тарату немесе сақтау жағдайларын қарастырады. Сонымен қатар, бұл баптар дербес деректердің қауіпсіздігіне жауапты операторлар мен қызметкерлерге де қолданылуы мүмкін.

Бұл екі баптың негізгі айырмашылығы – қоғамға тигізетін қауіптілік дәрежесінде және жауапкершілік сипатына байланысты. ҚР Қылмыстық кодексінің 211-бабы – қылмыстық құқық бұзушылықтарға жатады. Ол құпия ақпаратты (оның ішінде дербес деректерді) тарату қасақана, зиян келтіру мақсатында жасалып, елеулі зардаптарға әкелген немесе зиян келтірген жағдайларда қолданылады. Мұндай әрекеттер үшін қатаң жазалар көзделген – бас бостандығынан айыру, айыппұлдар, түзету немесе шектеу шаралары. Ал ҚР Әкімшілік құқық бұзушылық туралы кодексінің 79-бабы қоғамға қауіптілігі төмен, қылмыстық сипатқа ие емес құқық бұзушылықтар жасалғанда қолданылады. Мысалы, дербес деректерді сақтау, өңдеу немесе жинау рәсімдерінің бұзылуы, ішкі саясаттың болмауы, ақпаратты жеткілікті дәрежеде қорғамау, рұқсатсыз қол жеткізу сияқты жағдайлар. Бұл жерде жауапкершілік әкімшілік сипатта және, көбіне, айыппұл түрінде қарастырылады. Сондай-ақ, 79-бап бойынша жауапкершілікке тек жеке тұлғалар ғана емес, сонымен қатар заңды тұлғалар – шағын, орта және ірі бизнес өкілдері де тартылады. Ал 211-бап тек жеке тұлғаларға қатысты қолданылады.

Мемлекет бұл саладағы реттеуді күшейтіп, заң бұзушылықтар үшін жауапкершілікті барған сайын қатаңдатып келеді. Бұған себеп те айқын: ақпараттық кеңістікте қазақстандықтарға қатысты дербес деректердің кең ауқымды таралуы туралы жаңалықтар жиі шығып отырады. Соның ішінде банктер тарапынан азаматтардың деректерін сату фактілері мен олардың Қытайға таралуы қоғамда үлкен резонанс тудырған болатын.

Цифрлық даму, инновациялар және аэроғарыш өнеркәсібі министрлігі (ЦДИАӨМ) қазақстандықтардың деректері Қытай үкіметінің құжаттарындағы деректердің таралуына байланысты пайда болды деген ақпаратқа пікір білдірді. Сол кезде ведомство бұл мәселеге қатысты Ұлттық қауіпсіздік комитетімен бірлесіп алынған материалдарға талдау жүргізіп жатқанын хабарлаған еді. Кибершабуылдарды талдау және зерттеу орталығы (ЦАРКА) орын алған оқиғаға қатысты жантүршігерлік мәліметтерді жариялады. Олардың мәліметінше, қытайлық хакерлер Windows, Mac, iOS және Android жүйелеріне арналған зиянды бағдарламаларды, трояндарды, DDoS шабуылдарына арналған сервистерді, әлеуметтік желі қолданушыларын деанонимизациялау жүйелерін, Wi-Fi желілерін бұзатын құрылғыларды және басқа да құралдарды қолданған. Жүргізілген талдаудың нәтижесінде хакерлердің мақсаты дерекқорларға ғана емес, сонымен қатар жекелеген тұлғаларға бағытталған нақты ақпаратты жинау болғаны анықталды: хат алмасу, қоңыраулар, орналасқан жері туралы деректерге бақылау жүргізілген.

Ішкі істер министрлігі Ұлттық қауіпсіздік комитетімен бірлесіп дербес деректердің заңсыз таралуына қарсы ауқымды операция жүргізді. Қылмыстық топ мемлекеттік базалардан ақпарат алып, оны Telegram-арналар арқылы таратып, сонымен бірге коллекторлық компанияларға да жеткізген. Ішкі істер министрлігінің мәліметінше, 140-тан

астам адам ұсталды. Олардың арасында компаниялардың иелері мен арналардың әкімшілері бар. Бес күдікті қамауға алынып, коллекторлық компаниялардан 400-ден астам техника құралдары тәркіленді. Ішкі істер министрлігі мұндай әрекеттердің заңды бұзумен қатар, миллиондаған қазақстандықтардың цифрлық қауіпсіздігіне қауіп төндіретінін баса айтты. Мұндай оқиғалар назардан тыс қалмады, енді мемлекет жаңа ережелерді енгізіп, дербес деректерді қорғау саясатына басымдық беріп отыр.[7]

Қорытындылай келе, дербес деректер мен қаржылық қызметтерді пайдалану кезінде негізгі қауіпсіздік ережелерін сақтаудың маңыздылығын ерекше атап өткіміз келеді. Цифрлық даму, инновациялар және аэрогарыш өнеркәсібі министрлігі барлық пайдаланушыларға «Электрондық үкімет» веб-порталы немесе EgovMobile қосымшасы сияқты ыңғайлы әрі сенімді қызметтерді пайдаланып, қажетсіз несиелерден бас тартуды және өз қаржылық операцияларын бақылауды ұсынады. Егер сізге «банк қызметкерлері» деп телефон шалған жағдайда, сөйлесуді дереу тоқтатып, банкпен ресми байланыс арналары арқылы өз бетіңізше хабарласқаныңыз дұрыс. Операцияларды растауға арналған SMS кодтарын, интернет-банкинг парольдерін немесе картаңыздың CVV/CVC кодтарын ешқашан бермеңіз. Арнайы емес, әсіресе қашықтан қол жеткізуге мүмкіндік беретін үшінші тарап қосымшаларын орнатпаңыз және қаржылық есепшоттарыңыз үшін бірегей әрі күрделі парольдерді қолданыңыз. Екі факторлы аутентификацияны қосуға ерекше назар аударыңыз — бұл бұзылудан сенімді қорғаныс болып табылады. Белгісіз адамдардан келген электрондық хаттағы қосымшаларға сақ болыңыз және күмәнді сайттардан аулақ болыңыз. Жеке мәліметтеріңізді сенімсіз ресурстарға бермеңіз және қаржылық операцияларыңызды жүйелі түрде тексеріп отырыңыз.

Осы қарапайым, бірақ тиімді ережелерді сақтау дербес деректеріңізді қорғауға және цифрлық ортадағы қаржылық қауіпсіздігіңізді сақтауға көмектеседі.

Пайдаланылған әдебиеттер тізімі

1. «Персональные данные как объект правового регулирования: понятие и способы защиты» / CyberLeninka. – Электрондық ресурс. – Қолжетімді: https://cyberleninka.ru/article/n/personalnye-dannye-kak-obekt-pravovogo-regulirovaniya-ponyatie-i-sposoby-zaschity/viewer – Қол жеткізу күні: 2025 ж. 1 қыркүйек.

2. Дауысты қолдан жасау және алдамшы лендингтер: қазақстандықтар фишинг туралы не біледі // Profit.kz. – 2025 ж. 27 маусым. – Электрондық ресурс. – Қол жеткізу күні: 2025 ж. 1 қыркүйек. – Қолжетімді: https://profit.kz/articles/14957/Poddelka-golosov-i-lendingi-lovushki-chto-kazahstanci-znaut-o-fishinge/

3. Дербес деректер және оларды қорғау туралы : Қазақстан Республикасының Заңы № 94-V от 21 мамыр 2013 ж. // Егемен Қазақстан. – 2013. – 25 мамыр. – № 134 (28073); Казахстанская правда. – 2013. – 25 мая. – № 178–179 (27452–27453); Қазақстан Республикасы Парламентінің Жаршысы. – 2013. – № 7. – 35-құжат.

4. «11 мыңнан астам киберқылмыс Қазақстанда тіркелді» / Profit.kz. – 2025 ж. 10 шілде. – Электрондық ресурс. – Қолжетімді: https://profit.kz/news/71020/Bolee-11-tisyach-kiberprestuplenij-zaregistrirovano-v-Kazahstane/ – Қол жеткізу күні: 2025 ж. 11 қыркүйек.

5. Қазақстан Республикасының Қылмыстық кодексі : Қазақстан Республикасының Кодексі № 226-V ҚРЗ, 2014 жылғы 3 шілде // Қазақстан Республикасының Парламентінің Жаршысы. – 2014. – № 9. – 40-құжат.

6. Әкімшілік құқық бұзушылық туралы Қазақстан Республикасының Кодексі : Қазақстан Республикасының Кодексі № 235-V ҚРЗ, 2014 жылғы 5 шілде [Электрондық ресурс]. – Қолжетімді: https://adilet.zan.kz/kaz/docs/K1400000235

7. Қазақстандықтардың деректерін сату: 140-тан астам адам ұсталды / BizMedia.kz. – 2025 ж. 9 маусым. – Электрондық ресурс. – Қолжетімді: https://bizmedia.kz/2025-06-09-prodazha-dannyh-kazahstanczev-zaderzhany-bolee-140-chelovek/?utm_source=chatgpt.com – Қол жеткізу күні: 2025 ж. 1 қыркүйек.

УДК 376. 3

МЕХАНИЗМЫ ОПРЕДЕЛЕНИЯ УРОВНЕЙ ПОДГОТОВКИ БУДУЩИХ СПЕЦИАЛЬНЫХ ПЕДАГОГОВ К РАБОТЕ ПО МЕТОДИКЕ ИНДИВИДУАЛЬНОГО СОПРОВОЖДЕНИЯ ДЕТЕЙ С ОСОБЫМИ ОБРАЗОВАТЕЛЬНЫМИ ПОТРЕБНОСТЯМИ В ИНКЛЮЗИВНОМ ОБРАЗОВАНИИ

Тохтиярова Ш. Е., Национальный педагогический университет Узбекистана, Ташкент, Узбекистан
Алшинбаева С. Ж., Карагандинский университет имени Е.А. Букетова, Караганды, Казахстан

Аннотация. В области инклюзивного образования особое внимание уделяется подготовке специальных педагогов. Целью данной статьи является определение особенностей подготовки будущих специальных педагогов к работе по методике индивидуального сопровождения детей с особыми образовательными потребностями. В процессе исследования использовались следующие методы: сравнительное изучение и анализ научной, методической, педагогической литературы, источников, государственных образовательных стандартов, квалификационных требований, учебных планов, программ и учебников, а также национального и зарубежного опыта; наблюдение, беседа, интервью, анкетирование, анализ констатирующего эксперимента. Авторы в результате исследования предлагают эффективную и качественную подготовить будущих специальных педагогов к работе по методике индивидуального сопровождения детей с особыми образовательными потребностями.