ӘОЖ 004.9

АҚПАРАТТЫҚ РЕСУРСТАРДЫ ҚОРҒАУ ТӘСІЛДЕРІ МЕН ӘДІСТЕРІ

Турсынбекова Г.Ж., 4-курс, инженерлік-техникалық институты, информатика мамандығы, А.Байтұрсынов атындағы Қостанай өңірлік университеті
Калакова Г.Қ., инженерлік-техникалық институты, информатика кафедрасының аға оқытушысы, А.Байтұрсынов атындағы Қостанай өңірлік университеті

Адамдар өз құпияларын қорғауға бейім. Ақпараттық технологиялардың дамуы, олардың адам қызметінің барлық салаларына енуі ақпараттық қауіпсіздік проблемалары жыл сайын өзекті болып, сонымен бірге күрделене түседі. Ақпаратты өңдеу технологиялары үнемі жетілдіріліп отырады, сонымен бірге ақпараттық қауіпсіздікті қамтамасыз етудің практикалық әдістері де өзгереді.

Бүгінгі таңда ақпараттық сала-халықаралық ынтымақтастықтың маңызды салаларының бірі ғана емес, сонымен бірге бәсекелестіктің объектісі. Технологиялық стандарттарды белгілей отырып және тұтынушыларға өз ресурстарын ұсына отырып, ақпараттық инфрақұрылымы неғұрлым дамыған елдер басқа елдердегі ақпараттық инфрақұрылымдарды қалыптастыру және олардың қызметін жүзеге асыру шарттарын айқындайды, олардың ақпараттық саласының дамуына әсер етеді. Сондықтан өнеркәсібі дамыған елдерде ұлттық саясатты қалыптастыру кезінде ақпараттық саланы қорғау құралдарын дамыту және оның қауіпсіздігін қамтамасыз ету басымдыққа ие болады.

Компьютерлік жүйелердегі ақпараттың шоғырлануы оны қорғауға күш салуға мәжбүр етеді. Ұлттық қауіпсіздік, мемлекеттік құпия, коммерциялық құпия – осы заңды аспектілердің барлығы коммерциялық және мемлекеттік ұйымдардағы ақпаратқа бақылауды күшейтуді талап етеді. Осы бағытта жүргізіліп жатқан жұмыстар «Ақпараттық қауіпсіздік» деген жаңа пәннің пайда болуына алып келді.

Ақпараттық қауіпсіздік саласындағы маман ұйымда айналымдағы ақпараттың тұтастығын, қол жетімділігін және құпиялылығын қамтамасыз етуге арналған жүйені әзірлеуге, құруға және пайдалануға жауап береді. Оның функциялары физикалық қорғауды (аппараттық құралдар, компьютерлік желілер), сондай-ақ деректерді қорғау және бағдарламалық қамтамасыз етуді қамтиды.

Ақпараттық қауіпсіздікті қамтамасыз ету – бұл өте қымбат іс қана емес (техникалық және бағдарламалық қамтамасыз етуді сатып алу және орнату шығындары компьютерлік техниканың жартысынан көбін құрауы мүмкін), сонымен қатар өте күрделі: ақпараттық қауіпсіздік жүйесін құру кезінде ақпараттық жүйені жұмыс күйінде ұстау үшін қажет ықтимал қауіптер мен қажетті қорғаныс деңгейін анықтау қиын.

Қазіргі ақпараттық қоғам заңнама нормаларын сөзсіз қолдануға негізделген құқықтық мемлекет жағдайында ғана қалыптасып, тиімді дами алады. Ақпараттық қоғам өміріндегі құқықтың рөлі айқындаушы болады, оның барлық мүшелері заң нормаларын орындауға және туындаған дауларды заңнама негізінде өркениетті түрде шешуге тиіс.

Ақпаратты қорғау және ақпараттық қауіпсіздіктің негізгі ұғымдары. Ақпаратты өңдеудің, берудің және жинақтаудың заманауи әдістері деректерді жоғалту, бұрмалау және ашу мүмкіндігімен байланысты қауіптердің пайда болуына ықпал етті. Сондықтан ақпараттық қауіпсіздікті қамтамасыз ету ақпараттық технологияларды дамытудың жетекші бағыттарының бірі болып табылады.

Ақпаратты қорғау және ақпараттық қауіпсіздіктің негізгі ұғымдарын қарастырыңыз:

Ақпаратты қорғау – қорғалған ақпараттың ағып кетуіне, қорғалған ақпаратқа рұқсатсыз және абайсызда әсер етуге жол бермеу қызметі.

Қорғау объектісі – ақпаратты қорғаудың қойылған мақсатына сәйкес қорғауды жүзеге асыру қажет ақпараттың өзі, ақпарат тасымалдаушысы немесе ақпараттық процесс.

Ақпаратты қорғаудың мақсаты – ақпаратты қорғаудың қажетті нәтижесі. Ақпаратты қорғаудың мақсаты ақпараттың ықтималдығы жоғалуы (кемуі) немесе ақпаратқа кері әсер жасағанда және абайсызда әсер ету нәтижесінде ақпараттың меншік иесіне, иеленушісіне, пайдаланушысына залалдың алдын алу болып табылуы мүмкін.

Ақпаратты қорғаудың тиімділігі – қойылған мақсатқа қатысты ақпаратты қорғау нәтижелерінің сәйкестік дәрежесі.

Ақпаратты жария етуден қорғау – қорғалатын ақпараттың таралуын (оны жария етуді), қорғалатын ақпаратқа санкцияланбаған қол жеткізуді және зиянкестердің қорғалатын ақпаратты алуын болдырмау жөніндегі қызмет. Ақпаратты жария етуден қорғау – қорғалатын ақпаратты ақпарат алушылардың бақыланбайтын санына рұқсатсыз жеткізудің алдын алу.

Ақпаратты рұқсатсыз қол жеткізуден қорғау – мүдделі субъектінің қорғалатын ақпаратқа қол жеткізу ережелерін құқықтық құжаттарда, ақпараттың меншік иесінде немесе иесінде белгіленген бұза отырып, қорғалатын ақпаратты алуына жол бермеу. Заңды тұлға, жеке тұлғалар тобы, қоғамдық ұйым, жеке тұлға және тіпті мемлекет мүдделі субъект бола алады.

Ақпаратты қорғау жүйесі – органдар мен орындаушылардың жиынтығы, олар пайдаланатын ақпаратты қорғау техникасы, сондай-ақ белгіленген қағидалар бойынша ұйымдастырылған және жұмыс істейтін, ақпаратты қорғау жөніндегі құқықтық, ұйымдастырушылық-өкімдік және нормативтік құжаттарға сәйкес келетін қорғау объектілері.

Ақпараттық қауіпсіздік дегеніміз ақпараттың заңсыз танысудан, қайта құрудан және жойылудан қорғалуын, сондай-ақ ақпараттық ресурстардың олардың жұмыс қабілеттілігін бұзуға бағытталған әсерлерден қорғалуын білдіреді. Бұл әсерлердің табиғаты әр түрлі болуы мүмкін (шабуылдаушылардың кіру әрекеттері, қызметкерлердің қателіктері, аппараттық және бағдарламалық құралдардың істен шығуы, табиғи апаттар (дауыл, жер сілкінісі, өрт) және т. б.

Ақпараттың ықтимал қауіптерін жіктеу және мазмұны. Ақпаратты өңдеудің қазіргі заманғы жүйелеріндегі ақпарат қауіпсіздігіне төнетін қатерлер сыртқы ортаның әсерін бұзатын және бұрмалайтын қасақана (әдейі жасалған қауіптер) және табиғи (әдейі жасалмаған қауіптер), ақпаратты өңдеу құралдарының жұмыс істеу сенімділігімен, сондай-ақ мақсаттары өңделетін ақпаратты ұрлау, жою, қирату, санкцияланбаған түрлендіру және пайдалану болып табылатын санкцияланбаған пайдаланушылардың қасақана пайдакүнемдік әсерімен айқындалады. Бұл ретте қасақана немесе қасақана деп адамдардың қаскүнемдік әрекеттерінен туындайтын қауіптер түсініледі.

Шынында да, кез келген қорғаныс құралын ашуға болады, себебі оның коды процессор арқылы қойылады. Бұзушы бағдарламаны жан-жақты виртуалды жүйеде зерттей алады, онда процессор, жады, сыртқы құрылғылар, операциялық орта эмулирленеді. Бұл жағдайда көптеген қарсы тұру тәсілдері тиімсіз болып саналады. Қандай да ортаның эмуляциясы сапалы болғанымен соңғысы болмыстан ерекше болады. Мысалы, аппаратураның мерзімдік сипаттамасының дәл эмуляциясының болмауынан және қорғалған бағдарлама осыдан шығатын барлық ақпаратты тани білетіндей.

Кездейсоқ немесе табиғи – бұл адамдардың еркіне тәуелді емес қауіптер. Қазіргі уақытта ақпараттың сақталуына (тұтастығына) төнетін қауіптердің мынадай жіктемесі қарасырылады.

Қауіп-қатер көзі дегеніміз-ақпаратқа теріс әсер ету тұрғысынан қатерді тікелей орындаушы.

Қауіп көздерді келесі топтарға бөлуге болады: адамдар; техникалық құрылғылар; модельдер, алгоритмдер, бағдарламалар; технологиялық өңдеу схемалары; сыртқы орта.

Қауіптердің пайда болуының мынадай алғышарттары немесе себептері бар:

- объективті (жүйе элементтерінің сандық немесе сапалық жеткіліксіздігі) – адамдардың іс-әрекетімен тікелей байланысты емес және пайда болу сипаты бойынша кездейсоқ қауіп тудыратын;

- субъективті-адамның іс-әрекетімен тікелей байланысты және қасақана (шет мемлекеттердің барлау қызметі, өнеркәсіптік тыңшылық, қылмыстық элементтер мен жосықсыз қызметкерлердің қызметі), сондай-ақ абайсызда (психофизиологиялық жағдайы нашар, жеткіліксіз дайындық, білім деңгейі төмен) ақпарат қаупін тудырады.

Ақпараттық ресурстарды қорғаудың әдістері мен әдістері ақпаратты түрлендіру және беру әдістері мен әдістерін дамытумен қатар, оның қауіпсіздігін қамтамасыз ету әдістері үнемі дамып келеді. Бұл проблеманы дамытудың қазіргі кезеңі оны дәстүрлі түрде ұсынудан ақпаратты қорғау проблемасы ретінде кеңірек түсінуге – екі негізгі бағыт бойынша кешенді шешуден тұратын ақпараттық қауіпсіздік проблемасына көшумен сипатталады.

Компьютерлердің көбіне және желіге қатынауды пұрсатты пайдаланушы, яғни әртүрлі жеңілдікпен пайдаланушы, немесе суперпайдаланушы немесе жүйелік администратор (жиі сисадмин деп қысқартылып қолданылатын) қадағалап бақылайды (тексереді). Жүйелік администратор деп отырғанымыз – пайдаланушылардың есепке алу жазбаларын құратын, өзгертетін және жоятын, сонымен қатар жүйенің және желінің дұрыс жұмыс істеуіне жауапты болатын адам. Осындай пұрсатты пайдаланушының әдеттегі міндеті қауіпсіздік параметрлерін орнату және өзгерту болып табылады. Біреу паролін ұмытып қалды делік.

Біріншісіне мемлекеттік құпияны және құпия ақпаратты қорғауды жатқызуға болады, бұл негізінен оларға рұқсатсыз кірудің мүмкін еместігін қамтамасыз етеді. Бұл ретте құпия мәліметтер деп қоғамдық сипаттағы қолжетімділігі шектеулі мәліметтер (коммерциялық құпия, партиялық құпия және т.б.) түсініледі.

Екінші бағытқа соңғы уақытта халықаралық ауқым мен стратегиялық сипатқа ие болатын ақпараттан қорғау жатады. Сонымен қатар, ақпараттық қарудан (әсерден) қорғаудың үш негізгі бағыты бар: техникалық жүйелер мен құралдарға; қоғам; адам психикасы. Осы тәсілге сәйкес ақпараттың көптеген қауіптері, ақпаратты қорғау міндеттерінің функциялары мен сыныптары нақтыланды және толықтырылды.

Ақпараттандыру процесі қоғам өмірінің барлық салаларына әсер етті. Ақпараттандыру – қазіргі қоғамның өміріне тән қасиет. Ол адам қызметінің барлық бағыттарын сіңіреді. Жаңа ақпараттық технологиялардың пайда болуымен ақпарат мемлекеттердің, заңды тұлғалардың, қоғамдық бірлестіктер мен азаматтардың қызметін қамтамасыз етудің қажетті атрибуты болады.

Ақпараттың сапасы мен сенімділігіне, оны алудың жеделдігіне әр түрлі деңгейде – мемлекет басшыларынан бастап қарапайым азаматқа дейін қабылданатын көптеген шешімдер тәуелді.

Ақпараттық қауіпсіздікті қамтамасыз ету күрделі міндет болып табылады, өйткені ақпараттық ортаның өзі күрделі және көп қырлы механизм болып табылады, онда персонал, электронды жабдық, бағдарламалық жасақтама және т.б. сияқты компоненттер болуы мүмкін. Бұл мәселенің кем дегенде бір аспектісін елемеу қазіргі қоғам өмірінде маңызды рөл атқаратын және маңызды рөл атқаратын ақпараттың жоғалуына (ағып кетуіне) әкелуі мүмкін.

Пайдаланған әдебиеттер тізімі

1. В.Л. Цирлов «Автоматтандырылған жүйелердің ақпараттық қауіпсіздік негіздері. Қысқаша курс», 2008
2. «Есептеу жүйелеріндегі ақпаратты қорғау. Білім», 1982
3. Н.Н. Безруков «Компьютерлік вирусология» / Киев, 1991
4. Ю.В. Романец, П.А. Тимофеев, В.Ф. Шаньгин «Компьютерлік жүйелер мен желілердегі ақпаратты қорғау», 2001

УДК 371.39

ИНКЛЮЗИВНОЕ ОБРАЗОВАНИЕ НА УРОКАХ ФИЗИКИ

Тайрбергенова Д.Б., 4 курс, кафедра физики, Костанайский региональный университет им. А.Байтурсынова

Демина Н.Ф., кандидат педагогических наук, профессор кафедры физики Костанайского регионального университета им. А.Байтурсынова

В данной статье рассматривается тема инклюзивного образования на уроках физики. Целью статьи является выявление основных направлений работы с детьми с ОВЗ, анализ проблемы инклюзивного образования школьников с ОВЗ, изучение проблемы развития инклюзивного образования, исследовать проявляют ли учащиеся с ОВЗ, интерес к физике при выполнении заданий.

Инклюзивное образование – это образовательный процесс, направленный на устранение барьеров и включение всех лиц с особыми образовательными потребностями в общеобразовательный процесс и их социальную адаптацию с целью обеспечения равного доступа к качественному образованию.

В настоящее времядетей, имеющих ограниченные возможности здоровья, включают, в образовательный процесс обычной школы. Такой подход к обучениюдетей с ограниченными возможностями здоровья называется инклюзивнымобразованием. Инклюзивное образование предполагает, что дети с различнымиособенностями должны быть включены в образовательный процесс, а учрежденияобразования – создать им для этого соответствующие условия.

Важными коррекционными задачами курса физики для детей с ЗПР являются развитие у обучающихся основных мыслительных операций (анализ, синтез,сравнение, обобщение), нормализация взаимосвязи их деятельности с речью,формирование приемов умственной работы: анализ исходных данных,планирование материала, осуществление поэтапного и итогового самоконтроля. Обучающимся с задержкой психического развития в первую очередь необходимо развивать образное мышление, использовать образные представления и предлагать выполнять те виды умственной деятельности, которые детям наиболее близки ипонятны. Для этого необходимыразвивающиезадания.

Работоспособность детей спецкоррекции ЗПР зависит от характера выполняемых заданий. Они не могут долго сосредотачиваться на выполнении мыслительных задач, чем активнее они включаются в работу, тем скорее утомляются. Главным источником развития положительной мотивации является способность читать информацию, предоставленную нам окружающим миром. В широком смысле слово читать понимается, как умение объяснять, истолковывать физические явления или процессы, наблюдаемые в природе или в повседневной жизни. Для тогочтобы обеспечить усвоение обучающимисяспецкоррекции ЗПР необхо-