Дәріс 2. Қауіп ұғымы. Қазақстанда жұмыс істеу жағдайындағы ақпараттық қауіпсіздік

Жоспары:

1 Қауіп ұғымы
2 Ақпараттық қауіпсіздік: негізгі ұғымдары
3 Қауіпсіздік саясаты және негізгі элементтері
4 Қорғаныш жоспарын құрастыру
5 Объектілерді қайтадан пайдаланудың қауіпсіздігі

Қымбат әдістерге қарамастан, компьютерлік ақпараттық жүйелердің жұмыс істеуі *ақпаратты қорғауда* әлсіз жақтардың болуын анықтады. Ақпараттың үнемі өсіп келе жатқан шығындары мен күш-жігері сөзсіз нәтиже болды. Алайда, қабылданған шаралар тиімді болуы үшін ақпараттың қауіпсіздігіне төнетін қатердің не екенін анықтау, ақпараттың ағып кетуі мүмкін арналарды және қорғалатын деректерге рұқсатсыз қол жеткізу жолдарын анықтау қажет.

"*Қауіп*" ұғымының өзі әртүрлі жағдайларда жиі әртүрлі түсіндірілетінін атап өтейік. Мысалы, құпиялылыққа қауіп төндіретін ашық ұйым үшін бұл мүмкін емес бар - барлық ақпарат жалпыға қол жетімді болып саналады (БАҚ); дегенмен, көп жағдайда заңсыз қол жетімділік үлкен қауіп болып көрінеді. Басқаша айтқанда, АҚ-дағы барлық қауіп-қатерлер ақпараттық қатынастар субъектілерінің мүдделеріне байланысты (және олар үшін қандай зиян қолайсыз).

Сонымен, ақпараттық қауіпсіздікке төнетін қатерлерді жүзеге асыру ақпараттың құпиялылығын, тұтастығын және қол жетімділігін бұзу болып табылады.

Шабуылдаушы құпия ақпаратпен таныса алады, оны өзгерте алады немесе тіпті жоя алады, сондай-ақ заңды пайдаланушының ақпаратқа қол жеткізуін шектей немесе бұғаттай алады. Бұл ретте ұйымның қызметкері де, бөгде адам да шабуылдаушы бола алады. Сонымен қатар, қызметкерлердің кездейсоқ, байқаусызда жіберген қателіктеріне, сондай-ақ кейде табиғаттың өзі ұсынған тосын сыйларға байланысты ақпараттың мәні төмендеуі мүмкін.

Ақпараттық қауіптердің жіктелуі 1,2-суретте көрсетілген.

1-сурет. Ақпараттық қауіптің түрлері

2-сурет. Ақпараттық қауіптердің пайда болу факторлары бойынша жіктелуі

Ақпараттық қауіпсіздік – мемлекеттік ақпараттық ресурстардың, сондай-ақ саласында жеке адамның құқықтары мен мүдделері қорғалуының жай-күйі.

Ақпаратты қорғау – ақпараттық қауіпсіздікті қамтамасыз етуге бағытталған шаралар кешені. Тәжірибе жүзінде ақпаратты қорғау деп деректерді енгізу, сақтау, өңдеу және тасымалдау үшін қолданылатын ақпарат пен қорлардың тұтастығын, қол жеткізулік оңтайлығын және керек болса жасырындылығын қолдауды түсінеді. Сонымен, ақпаратты қорғау – ақпараттың сыртқа кетуінің, оны ұрлаудың, жоғалтудың, рұқсатсыз жоюдың, өзгертудің, маңызына тимей түрлендірудің, рұқсатсыз көшірмесін алудың, бұғаттаудың алдын алу үшін жүргізілетін шаралар кешені. Қауіпсіздікті қамтамасыз ету кезі қойылатын шектеулерді қанағаттандыруға бағытталған ұйымдастырушылық, бағдарламалық және техникалық әдістер мен құралдардан тұрады.

Ақпараттық қауіпсіздік режімін қалыптастыру кешендік мәселе болып табылады. Оны шешу үшін заңнамалық, ұйымдастырушылық, бағдарламалық, техникалық шаралар қажет.

Ақпараттық қауіпсіздіктің өте маңызды 3 жайын атап кетуге болады: қол жеткізерлік (оңтайлық), тұтастық және жасырындылық.

Қол жетерлік (оңтайлық) – саналы уақыт ішінде керекті ақпараттық қызмет алуға болатын мүмкіндік. Ақпараттың қол жеткізерлігі – ақпараттың, техникалық құралдардың және өңдеу технологияларының ақпаратқа кедергісіз қол жеткізуге тиісті өкілеттігі бар субъектілердің оған қол жеткізуін қамтамасыз ететін қабілетімен сипатталатын қасиеті.

Тұтастық – ақпарттың бұзудан және заңсыз өзгертуден қорғанылуы. Ақпарат тұтастығы деп ақпарат кездейсоқ немесе әдейі бұрмаланған кезде

есептеу техника құралдарының немесе автоматтандырылған жүйелердің осы ақпараттың өзгермейтіндігін қамтамасыз ететін қабілетін айтады.

Жасырындылық – заңсыз қол жеткізуден немесе оқудан қорғау.

Қауіпсіз жүйе – белгілі бір тұлғалар немесе олардың атынан әрекет жасайтын үрдістер ғана ақпаратты оқу, жазу құрастыру және жою құқығына ие бола алатындай етіп ақпаратқа қол жеткізуді тиісті құралдар арқылы басқаратын жүйе.

Сенімді жүйе - әр түрлі құпиялық дәрежелі ақпаратты қатынас құру құқығын бұзбай пайдаланушылар тобының бір уақытта өңдеуін қамтамасыз ету үшін жеткілікті аппаратық және бағдарламалық құралдарды қолданатын жүйе.

Жүйенің сенімділігі (немесе сенім дәрежесі) екі негізгі өлшеме бойынша бағаланады: қауіпсіздік саясаты және кепілділік.

Қауіпсіздік саясаты – мекеменің ақпаратты қалайша өңдейтінін, қорғайтынын және тарататынын анықтайтын заңдар, ережелер және тәртіп нормаларының жиыны. Бұл ережелер пайдаланушының қайсы кезде белгілі бір деректер жинағымен істей алатынын көрсетеді. Қауіпсіздік саясатын құрамына мүмкін болатын қауіптерге талдау жасайтын және оларға қарсы әрекет шаралар кіретін қорғаныштың белсенді сыңары деп санауға болады.

Қауіпсіздік саясатының құрамына ең кемінде мына элементтер кіруі керек: қатынас құруды ерікті басқару, объектілерді қайтадан пайдаланудың қауіпсіздігі, қауіпсіздік тамғасы және қатынас құруды мәжбүрлі басқару.

Кепілділік – жүйенің сәулетіне және жүзеге асырылуына көрсетілетін сенім өлшемі. Ол қауіпсіздік саясатын іске асыруға жауапты тетіктердің дұрыстығын көрсетеді. Оны қорғаныштың, қорғаушылар жұмысын қадағалауға арналған, белсенсіз сыңары деп сипаттауға болады. Кепілділіктің екі түрі болады: операциялық және технологиялық. Біріншісі жүйенің сәулеті және жүзеге асырылу жағына, ал екіншісі – құрастыру және сүйемелдеу әдістеріне қатысты.

Есепберушілік (немесе хаттамалау тетігі) қауіпсіздік қамтамасыз етудің маңызы құралы болып табылады. Сенімді жүйе қауіпсіздікке байланысты барлық оқиғаларды тіркеп отыруы керек, ал хаттаманы жазу – жүргізу тексерумен (аудитпен – тіркелу ақпаратына талдау жасаумен) толықтырылады.

Сенімді есептеу базасы (СЕБ) – компьютерлік жүйенің қауіпсіздік саясатты жүзеге асыруға жауапты қоршаған тетіктерінің жиынтығы. Компьтерлік жүйенің сенімділігіне баға беру үшін тек оның есептеу базасын қарастырып шықса жеткілікті болады. СЕБ негізгі міндеті – қатынасым мониторының міндетін орындау, яғни, объектілерімен белгілі бір операциялар орындау болатындығын бақылау.

Қатынасым мониторы – пайдаланушынына бағдарламаларға немесе деректерге әрбір қатынасының мүмкін болатын іс-әрекеттер тізімімен келісімді екендігін тексеретін монитор. Қатынасым мониторынан үш қасиеттің орындалуы талап етіледі:

- оңашаланғандық . Монитор өзінің жұмысы кезінде аңдудан қорғалуға тиісті;

- толықтық. Монитор әрбір қатынасу кезінде шақырылады. Бұл кезде оны орай өтуге мүмкіндік болмау керек;

- иландырылатындық. Мониторды талдау және тестілеуге мүмкін болу үшін ол жинақы болуы керек.

Қауіпсіздік өзегі – қатынасым мониторының жүзеге асырылуы. Қауіпсіздік өзегі барлық қорғаныш тетіктерінің құрылу негізі болып табылады. Қатынасым мониторының аталған қасиеттерінен басқа қауіпсіздік өзегі өзінің өзгерместігіне кепілдік беруі керек.

Қауіпсіздік периметрі – сенімді есептеу базасының шекарасы. Оның ішіндегі сенімді, ал сыртындағы сенімсіз деп саналады. Сыртқы және ішкі әлемдер арасындағы байланыс ретқақпа (gateway) арқылы жүзеге асырылады. Бұл ретқақпа сенімсіз немесе дұшпандық қоршауға қарсы тұра алуға қабілеті бар деп саналады.

Объектінің ақпараттық қауіпсіздігін қамтамасыз етуге арналған жұмыстар бірнеше кезеңге бөлінеді: даярлық кезеңі, ақпараттық қорларды түгендеу, қатерлі талдау, қорғаныш жоспарын құрастыру және қорғаныш жоспарын жүзеге асыру. Осы аталған кезеңдер аяқталған соң эксплуатациялау кезеңі басталады.

Даярлық кезеңі. Бұл кезең барлық келесі шаралардың ұйымдастырушылық негізін құру, түпқазық құжаттарды әзірлеу және бекіту, сондай-ақ, үрдіске қатысушылардың өзара қарым – қатанастарын анықтау үшін қажет. Даярлық кезеңде ақпарат қорғау жүйесінің атқаратын міндеттері анықталады.

Ақпараттық қорларды түгендеу. Бұл кезеңде, әдетте, объект, ақпараттық ағындар, автоматтандырылған жүйелердің құрылымы, серверлер, хабар тасушылары, деректер өңдеу және сақтау тәсілдері жайында мәлімет жиналады. Түгендеу аяқталған соң олардың осалдылығына талдау жасалынады.

Қатерлі талдау. Келесі шаралардың нәтижелігі ақпараттық қорлардың қорғанылу күй-жағдайының қаншалықты толық және дұрыс талдануына тәуелді болады. Қатерлі талдау мыналардан тұрады: талданатын объектілерді және оларды қарастырудың нақтылану дәрежесін таңдау; қатерлі бағалау әдіснамасын таңдау; қауіптерді және олардың салдарын талдау; қатерлі бағалау; қорғаныш шараларын таңдау; таңдап алынған шараларды жүзеге асыру және тексеру; қалдық қатерді бағалау.

Қауіп бар жерде қатер пайда болады. Қауіптерді талдау кезеңі қатерді талдаудың орталық элементі болып табылады. Қауіптердің алдын алу үшін қорғаныш шаралары мен құралдары қажет. Қауіптерді талдау, біріншеден, мүмкін болатын қауіптерді анықтаудан (оларды идентификациялаудан) және екіншіден, келтірілетін болашақ зиянды болжау-бағалаудан тұрады.

Бұл кезеңнің орындалу нәтижесінде объектідегі қауіп-қатер тізбесі және олардың қауіптік дәрежесі бойынша жіктемесі құрастырылады. Бұлар бәрі

ақпарат қорғау жүйесіне қойылатын талаптарды айқындауға, қорғаныштың ең әсерлі шаралары мен құралдарын таңдап алуға, сондай-ақ, оларды жүзеге асыруға қажетті шығындарды анықтауға мүмкіндік береді.

Қорғаныш жоспарын құрастыру. Бұл кезеңде осының алдында жүргізілген талдаудың нәтижесінде анықталған қатерлерді бейтараптау үшін қорғаныштың тиісті ұйымдастырушылық және техникалық шаралары таңдап алынады.

Қорғаныш жоспарын құру ақпарат қорғау жүйесінің функциональдық сұлбасын әзірлеуден басталады. Ол үшін қорғаныш жүйесінің атқаратын міндеттері анықталады және нақты объектінің ерекшіліктерін ескере отырып жүйеге қойылатын талаптар талқыланады. Жоспарға мынадай құжаттар қосылады: қауіпсіздік саясаты; ақпарат қорғау құралдарының объектіде орналасуы; қорғаныш жүйесін жұмысқа қосу үшін қажет шығындардың сметасы; ақпарат қорғаудың ұйымдастырушылық және техникалық шараларын жүзеге асырудың күнтізбелік жоспары.

2. Қауіпсіздік саясаты және негізгі элементтері

Қауіпсіздік саясаты (ұйымдастыру тұрғысынан қарағанда) есептеу және қатынас қорларын пайдалану тәсілін, сондай-ақ, қауіпсіздік режімін бұзудың алдын ала және мән беру (жауап қайтару) процедураларын дұрыс анықтайды. Қауіпсіздік саясатының қалыптастыру іс-әрекетін келесі кезеңдер түрінде қарастыруға болады:

• *Ұйымдастыру мәселелерін шешу*. бұл кезеңде ақпараттық қауіпсіздік қызметі (АҚҚ) құрылады, ақпараттық қауіпсіздік тұрғысынан қарағанда пайдаланушылардың санаттары, пайдаланушылардың барлық санаттарының жауаптылық деңгейлері, құқықты және міндеттері анықталады.

• *Қатерге талдау жасау*. Қатерді талдау үрдісі нені қорғау керек, неден қорғау керек және қалай қорғау (істеу) керек деген сияқты сұрақтардың жауабын анықтайды. Мүмкін болатын қатерлердің бәрін қарастырып шығу керек және оларды келтіретін зиянының ықтимал мөлшеріне байланысты жіктеу қажет. Қорғанышқа жұмсалатын қаржы қорғанылатын объектінің құнынан аспауға тиісті.

• *Жеңілдектерді анықтау*. Қорларды пайдалану құқықтары, қорларды қолдану ережелері, әкімшілік жеңілдіктер, пайдаланушылардың құқықтары мен міндеттері, жүйелік әкімшілердің құқықтар мен міндеттері, жасырын ақпаратпен жұмыс істеу тәртіптері және т.б. анықталады.

• *Қауіпсіздік саясатының бұзылуына жауап қайтару шараларын анықтау*. Қауіпсіздік режімі бұзушыларды табуға және жауапкершілікке тартуға бағытталған әрекеттер, сонымен қатар, ақпаратты бұрынғы қалпына келтіру және бұзулардың зардаптарын жою шаралары анықталады.

• *Ұйымдастыру -әкімгерлік құжаттарды дайындау*. Қауіпсіздік саясатының негізгі жайлары әр түрлі нұсқауларда, қағидаларда, ережелерде және өкімдерде келтіріледі.

Қауіпсіздік саясаты ақпарат қорғау жүйесінің қауіп-қатерлерге қарсы әрекет жасауға бағытталған құқықтық нормалардың, ұйымдастырушылқ шаралардың, бағдарламалық-техникалық құралдар және процедуралық шешімдер кешенінің жиынтығын анықтайды.

Ақпарат қауіпсіздігінің жоғарғы дәрежесіне қол жету тек тиісті ұйымдастыру шараларын қолдану негізінде ғана мүмкін болады. Ұйымдастырушылық шаралар кешенінің құрамына ақпараттық қауіпсіздік қызметін құру, жасақтау және оның іс-әрекеттерінің қолдану, ұйымдастыру-әкімгерлік құжаттар жүйесін дайындау жұмыстары, сондай-ақ, қорғаныш жүйесін құруға және оның жұмысын сүйемелдеуге арналған бірқатар ұйымдастырушылық және ұйымдастыру-техникалық шаралар кіреді.

Ұйымдастырушылық және ұйымдастыру-техникалық шаралар жүргізу ақпараттың сыртқа кететін жаңа арналарын дер кезінде табуға, оларды бейтараптандыру шараларын қолдануға, қорғаныш жүйелерін толық жетілдіруге және қауіпсіздік режімін бұзу әрекеттеріне жедел қарсы шара қолдануға мүмкіндік береді. Қатерге талдау жүргізу қауіпсіздік саясатын қалыптастырудың негізгі кезеңі болып табылады.

Ұйымдастыру мәселері шешілгеннен кейін бағдарламалық-техникалық проблемалардың кезегі келеді – таңдалған қауіпсіздік саясатын іске асыру үшін не істеу керек? Қазіргі уақытта құны, атқаратын міндеті және сапасы жағынан әртүрлі болатын ақпарат қорғау құралдарының көптеген түрі бар. Олардың ішінен нақты объектінің ерекшелігіне сай келетінін таңдап алу күрделі мәселелердің бірі болып саналады.

Қауіпсіздік саясаты мынадай элементтерден тұрады: қатынас құруды ерікті басқару, объектілерді қайтадан пайдаланудың қауіпсіздігі, қауіпсіздік тамғасы және қатынас құруды мәжбүрлі басқару.

Қатынас құруды ерікті басқару – жеке субъект немесе құрамына осы субъект кіретін топтың тұлғасын ескеру негізінде жасалған объектілерге қатынас құруды шектеу. Ерікті басқару – белгілі бір тұлға (әдетте, объектінің иесі) өзінің қарауынша басқа субъектілерге өзінің шешімі бойынша объектіге қатынас құру құқығын бере алады (немесе алып тастайды).

Қатынас құрудың ағымдағы жағдайы ерікті басқару кезінде матрица түрінде көрсетілді. Қатарларында – субъектілер, бағандарында – объектілер, ал матрицаның түйіндерінде қатынас құру құқығының құру (оқу, жазу, орындау және т.б.) кодасы көрсетіледі.

Операциялық жүйелердің және дерекқор жүйелерінің көпшілігі осы ерікті басқаруды жүзеге асырады. Оның негізгі жағымдағы – икемділігі, ал негізгі кемшіліктері – басқарудың бытыраңқылығы және орталықтандырылған тексерудің күрделігі, сондай-ақ, қатынас құру құқығының деректерден бөлек қарастырылуы (қаскүнемдер осыны пайдалана отырып құпия ақпараттарды жалпы қол жеткізерлік файлдарға көшіріп алуы мүмкін).

Объектілерді қайтадан пайдаланудың қауіпсіздігі. Бұл элемент құпия ақпаратты кездейсоқ немесе әдейі шығарып алудан сақтайтын қатынас құруды басқаратын құралдардың маңызды қосымшасы болып табылады.Объектілерді қайтадан пайдаланудың мүмкін болатын 3 қаупі мыналар: жедел жадыны қолдану. сыртқы сақтау құрылғыларын қайтадан пайдалану және ақпарат енгізу/шығару құрылғыларын қайтадан пайдалану.

Қорғаныш тәсілдерінің бірі – құпия ақпаратпен жұмыс істегеннен кейін жедел жадыны немесе аралық жадыны тазалау. Жақсы әдіс деп тегерішті (дискіні) нығыздау программаларын қолдануды да санауға болады.

Мәселен, принтердің аралық жадында (арашықта) құжаттың бірнеше беті сақталып қалуы мүмкін. Олар басу үрдісі аяқталған соң да жадыда қалып қояды. Сондықтан оларды арашықтан шығарып тастау үшін арнаулы шаралар қолдану қажет. Әдетте кездейсоқ биттер тізбегін үш дүркін қайталап жазу жеткілікті болады.

“Субъектілерді қайтадан пайдаланудың қауіпсіздігі” жайында да қамдану керек. Пайдаланушы ұйымнан кеткен кезде оны жүйеге кіру мүмкіншіліктерінен айыру және барлық объектілерге оның қатынас құруына тиым салу керек.

Қауіпсіздік тамғасы. Қатынас құрудың мәжбүрлі басқаруы кезінде субъектілер және объектілер қауіпсіздік тамғасы арқылы байланысады. Субъектінің тамғасы оның шүбәсіздігін сипаттайды. Объектінің тамғасы оның ішіндегі сақталатын ақпараттың жабықтық деңгейін көрсетеді.

Қауіпсіздік таңбасы екі бөліктен тұрады: құпиялық деңгейі (дәрежесі) және категориялар (санаттар).

Құпиялылық деңгейі реттелген жиынтық құрайды және әр түрлі жүйелерде құпиялық деңгейлер жиынтығы әр түрлі болуы мүмкін. Қазақстан Республикасының заңнамасында мемлекеттік құпия құрайтын мәліметтердің үш құпиялылық дәрежесі тағайындалған және осы дәрежелерге сәйкес аталған мәліметтердің тасуыштарына мынадай құпиялық белгілері берілген: “ аса маңызды”, “өте құпия” және “құпия”, ал қызметтік құпия құрайтын мәліметтерге “құпия” деген құпиялық белгісі беріледі.

Санаттар реттелмеген жиынтық құрайды. Олардың міндеті – деректер жататын аймақтың тақырыбын сипаттау.

Қауіпсіздік таңбалардың тұтастығын қамтамасыз ету оларға байланысты негізгі проблемалардың біреуі болып табылады. Біріншіден, тамғаланбаған субъектілер мен объектілер болмау керек. Әйтпесе тамғалық қауіпсіздікте саңылаулар пайда болады және қаскүнем осы жағдайды пайдаланып қорғанылатын ақпаратқа заңсыз қол жеткізуі мүмкін. Екіншіден, қорғанылатын деректермен қандай да болмасын операция орындалмасын, қаупсіздік тамғалары өзгермей қалуы керек.

Қауіпсіздік тамғаларының тұтастығын қамтамасыз етуші құралдардың біреуі – құрылғыларды көпдеңгейлік және бір деңгейлік деп бөлу. Көпдеңгейлік

құрылғыларда әр түрлі құпиялық деңгейлі ақпарат, ал бірдеңгейлік құрылғыларда тек бір құпиялық деңгейі бар ақпарат сақталады.

Қатынас құруды мәжбүрлі басқару. Қатынас құруды мәжбүрлі басқару деп атаудың себебі – қатынас құру мүмкіндігі субъектінің ерігіне тәуелді емес. Мұндай басқару субъектінің және объектінің қауіпсіздік тамғаларын салыстыру негізінде жүргізіледі.

Егер субъектінің құпиялық деңгейі объектінің құпиялық деңгейінен кем болмаса, ал объектінің қауіпсіздік тамғасында көрсетілген барлық санаттар субъектінің тамғасында болса, (яғни, осындай екі шарт орындалған болса), онда субъект объектіден кез келген ақпаратты оқи алады. Мысалы, “өте құпия” субъект “өте құпия” және “құпия” файлдарды оқи алады. Бұл жағдайда “субъектінің қауіпсіздік тамғасы объектінің қауіпсіздік тамғасынан басым” деп айтады.

Ұсынылған әдебиеттер:

Негізгі әдебиеттер:

1. Нестеров, С. А. Основы информационной безопасности: учебник для вузов/ С. А. Нестеров. - Санкт-Петербург : Лань, 2021., 324 с. — ISBN 978-5-8114-6738-9.
2. Зенков, А. В. Информационная безопасность и защита информации: учебное пособие для вузов / А. В. Зенков. — 2-е изд., перераб. и доп. — Москва: Издательство Юрайт, 2023. — 107 с. — (Высшее образование). — ISBN 978-5-534-16388-9
3. Суворова, Г. М. Информационная безопасность : учебное пособие для вузов / Г. М. Суворова. — 2-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. — 277 с. — (Высшее образование). — ISBN 978-5-534-16450-3

Қосымша әдебиеттер:

1. Внуков, А. А. Защита информации : учебное пособие для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2023. — 161 с. — (Высшее образование). — ISBN 978-5-534- 07248-8
2. Казарин, О. В. Надежность и безопасность программного обеспечения : учебное пособие для вузов / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2023. — 342 с. — (Высшее образование). — ISBN 978-5-534-05142-1
3. Корабельников, С. М. Преступления в сфере информационной безопасности : учебное пособие для вузов / С. М. Корабельников. — Москва : Издательство Юрайт, 2023. — 111 с. — (Высшее образование). — ISBN 978-5-534-12769-0