ОӘЖ 004

АҚПАРАТТЫҚ ЖҮЙЕЛЕРДЕ ДЕРБЕС ДЕРЕКТЕРДІ ҚОРҒАУ

Ғалиханова Сымбат Төлегенқызы
galikhanovas@mail.ru
7М06111- «Ақпараттық қауіпсіздіктің әдістері мен технологиялары», 2-курс магистранті
Л.Н.Гумилев атындағы Еуразия ұлттық университеті, Нұр-Сұлтан қ., Қазақстан.
Ғылыми жетекші : Ташенова Жулдыз Мусагуловна - PhD, доцент м.а

Аннотация. Жеке ақпаратты қорғау соңғы бірнеше жылда жалпыға ортақ талқылау тақырыбы болып табылады. Бұл мәселе ерекше назар аударуға тұрарлық, өйткені ол бизнестің де, жеке өмірдің де көптеген аспектілеріне қатысты. Көптеген компаниялар үшін тұтынушылар туралы құпия мәліметтер мен қызметкерлер туралы ақпарат жинау бизнесті жүргізудің ажырамас бөлігі болып табылады. Компания қолданыстағы заңдар мен ережелерге сәйкес жеке ақпараттың жоғалуын, жойылуын, өзгеруін, ағып кетуін және рұқсатсыз кіруін болдырмау үшін қатаң қауіпсіздік шараларын жасауы керек. Мақала осы мәселеге арналған. Сонымен қатар, ол пайдалануға болатын негізгі бағдарламалық өнімдерді қарастырады.

Кілт сөздер. Ақпараттық технологиялар, дербес деректер, ақпараттық жүйелер.

Қазіргі уақытта дербес деректердің (ДД) қауіпсіздігін қамтамасыз ету қажеттілігі объективті шындық болып табылады. Адам туралы ақпарат әрқашан үлкен құндылыққа ие болды, бірақ бүгінде ол ең қымбат тауарға айналды. Алаяқтың қолындағы ақпарат қылмыс құралына, жұмыстан шығарылған қызметкердің қолында кек алу құралына, Инсайдердің қолында бәсекелеске сатылатын тауарға айналады... сондықтан жеке деректер ең маңызды қорғауды қажет етеді.

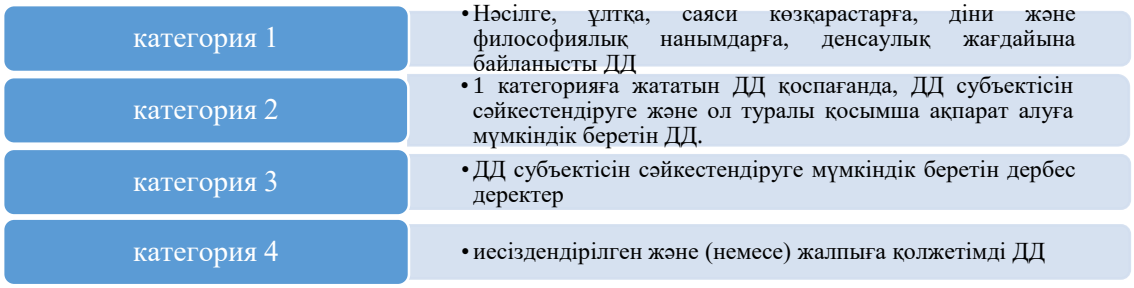
Бүгінгі таңда ұйымның қызметін адам туралы ақпаратты өңдеусіз елестету мүмкін емес. Қалай болғанда да, ұйым қызметкерлер, клиенттер, серіктестер, жеткізушілер және басқа жеке тұлғалар туралы деректерді сақтайды және өңдейді. Жеке деректердің ағуы, жоғалуы немесе рұқсатсыз өзгеруі орны толмас залалға, кейде ұйымның қызметін толығымен тоқтатуға әкеледі.

Жеке сипаттағы деректерді автоматтандырылған өңдеуге қатысты жеке тұлғаларды қорғау туралы Еуропа Кеңесінің Конвенциясын айқындау бойынша дербес деректер белгілі бір немесе айқындауға жататын жеке тұлға туралы кез келген ақпаратты білдіреді [1].

«Дербес деректер туралы» заңға сәйкес дербес деректерге жеке тұлғаға (дербес деректер субъектісіне) қатысты, осындай мәліметтер негізінде анықталған немесе айқындалған кез келген мәліметтер, оның ішінде тегі, аты, әкесінің аты, туған жылы, айы, күні және туған жері, мекенжайы, отбасы, әлеуметтік, мүліктік жағдайы, білімі, кәсібі, табысы және өзге де мәліметтер жатады. Дербес деректерді қорғау - бұл дербес деректері бар ақпаратқа, тиісті өкілеттіктері жоқ тұлғаларға қолжетімділікті болдырмайтын, сондай-ақ осындай ақпаратты заңсыз пайдалану мүмкіндігін болдырмайтын ұйымдастырушылық және техникалық шаралар кешені [1].

Заңға сәйкес, қазір барлық деректер қорғалуы керек, бірақ бұл үшін әртүрлі қорғаныс деңгейлерін қолдануға болады. Қазақстан Республикасының техникалық және экспорттық бақылау жөніндегі қызметінің заңға тәуелді актілері дербес деректердің төрт санатын бөліп көрсетеді.

Зейнетақы қорына берілетін жоғары санаттағы деректер кез келген кәсіпорында бар (аты-жөні көрсетілген жалақы туралы үзінді көшірме, қызметкердің әлеуметтік жағдайы, мүгедектігі, отбасы жағдайы, балалардың саны және т.б. туралы мәліметтер) [2].



Сурет 1. Дербес деректердің санаттары

Жеке деректердің санаты неғұрлым жоғары болса, оларды қорғау тетіктері соғұрлым күрделі болады. Төменгі санат үшін – К4 – тек деректердің тұтастығын қамтамасыз ету жеткілікті, ал технологиялық шешімдерді таңдау компанияның ар-ожданында қалады. К1 санатындағы деректер визуалды және дыбыстық арналар арқылы ағып кетуден, сондай-ақ бүйірлік электромагниттік сәулеленуден қорғалуы керек, оны ұйымдастыру өте қиын, өйткені арнайы бөлмелер мен компьютерлік техника қажет, ал қорғаныс үшін қолданылатын шешімдер тиісті сертификаттарға ие болуы керек [3]. Соңғы бөлім криптографияны қолдануды бақылайды, бірақ осы деңгейдегі жүйеде шифрлаусыз жасау мүмкін емес. Сонымен қатар, сертификатталған крипто-кітапханаларды пайдалану кезінде оларды өнімге енгізудің дұрыстығы туралы қорытынды болуы керек.

Ақпараттың әртүрлі санаттары үшін жеке деректерді қорғауға қойылатын талаптардағы айтарлықтай айырмашылықтар қолданыстағы Ақпараттық технология жүйелерінің архитектураларына өзгерістер енгізу қажеттілігіне әкеледі, бірақ бұл бүкіл жүйе үшін емес, тек шағын дерекқорлар үшін оңай. Нәтижесінде, компаниялар жоғары деңгейдегі жеке деректермен жұмыс істеу үшін жауапты жеке жүйелерді бөлуге және шығындарды үнемдеу үшін басқа, салыстырмалы түрде арзан конфигурацияларда қалған ақпаратты қорғауға мәжбүр болады [4]. Нәтижесінде, контрагенттердің жеке деректерін қорғаудың жоғары деңгейі бар жеке дерекқорға көшіруді талап ететін CRM, call-орталықтар және т.б. сияқты жүйелердің архитектурасын өзгерту қажет болуы мүмкін.

Шешім архитектурасы жеке деректерді желінің жеке сегментіне ғана емес, сонымен бірге тұтастай сыртқы компанияға беруге мүмкіндік беруі керек, өйткені бұл мәліметтер базасын шифрлау қызметтерін әзірлеуге, сатуға және ұсынуға қажетті лицензиялар жиынтығы бар мамандандырылған компаниялар қорғайды. Мүмкін, ұйымдар заң мен заң актілерінің талаптарын өз бетінше орындағысы келмейді және өз деректерін қорғауды аутсорсингке жібереді [5].

ДД субъектісі өзінің ниетін құжаттай отырып, ДД-ны біреуге беруді дербес шешеді [6]. 152-бапқа сәйкес дербес деректерді өңдеу көрсетілген деректерді көрсете отырып, жазбаша келісіммен ғана жүзеге асырылады.

Жеке деректерді қорғауды шабуылдаушы оның негізгі элементтерінің – желілік құрылғылардың, операциялық жүйелердің, қосымшалардың және ДҚБЖ жұмысына араласа алмайтын ақпараттық жүйеде ғана қамтамасыз етуге болады [7].

Вирустан қорғау - құпия ақпараттың, соның ішінде жеке мәліметтердің ағып кетуіне жол бермейтін құралдардың бірі - вирустар, құрттар және басқа да зиянды бағдарламалар ақпаратты жиі ұрлайды және жасырын ағып кету арналарын ұйымдастырады [8]. Қазіргі заманғы антивирустық шешімдерге тек қолтаңбаны қорғау ғана емес, сонымен қатар бағдарламалардың мінез-құлқын талдау, қолданбалы деңгейдегі экрандар, операциялық жүйе үшін маңызды деректердің тұтастығын бақылау және жұмыс станциялары мен серверлерді қорғаудың басқа әдістері сияқты заманауи құралдар кіреді.

Кейбір Internet Security антивирустық шешімдерінде (мысалы, Касперский зертханасы, Symantec, Eset, McAfee және Trend Micro) жеке брандмауэрлер желілік протоколдардағы шабуылдарды және желілік құрттардың қорғалған машинаға ену

әрекеттерін анықтауға арналған. Сонымен қатар, сыртқы веб-қосымшалар мен пошта жүйелері үшін демилитаризацияланған аймақты (DMZ) құратын брандмауэрлер шлюз маршрутизаторында іске қосылуы керек (бұл функция әдетте желілік құрылғыларда қол жетімді). Шын мәнінде, қол жеткізу үшін брандмауэрде қатаң ережелерді қолданатын DMZ-де сырттан қол жетімді желілік ресурстар және олар үшін қорғаныс механизмдері орналастырылған [9].

Интрузияның алдын алу жүйелері (Intrusion Prevention System, IPS) желінің үзілуіне орнатылады және трафиктің ішінде шабуыл белгілерін анықтауға және ең танымал шабуылды бұғаттауға қызмет етеді. Шлюз антивирустарынан айырмашылығы, IPS тек IP пакеттерінің мазмұнын ғана емес, сонымен қатар пайдаланылған протоколдар мен оларды қолданудың дұрыстығын талдайды. Шабуылдардың алдын алу жүйелері қорғайтын шабуылдар спектрі шлюз антивирустарына қарағанда біршама кең [10]. IPS жүйелерін Check Point және McAfee (Network Security Platform өнімі) сияқты желіні қорғауға мамандандырылған компаниялар да, желілік жабдықты өндірушілер – Juniper және Cisco шығарады.

Көрсетілген қауіпсіздік шаралары бүкіл желі үшін ортақ болып табылады және дербес деректерді қорғаумен тікелей байланысты емес, бірақ олардың болуы талаптарда арнайы ескерілген, сондықтан әрбір дербес деректер операторында қауіпсіздік шараларын таңдау оператордың өзінде қалатын К4 ең төменгі деңгейі үшін де осы негізгі құралдар болуы тиіс [11].

Қазіргі уақытта құпия деректерді ағып кетуден қорғау құралдарының кешені әзірленуде. Мұндай өнімдердің үш класы бар: перифериялық басқару жүйелері, деректердің ағып кетуіне жол бермеу жүйелері (DLP) және шифрлау құралдары, және өндірушілердің әрқайсысы олардың ағып кетуінен қорғайтын өнім деп санайды. Сірә, толық қауіпсіздік үшін өнімнің барлық үш түрін біріктірген жөн, бірақ әзірге нарықта мұндай күрделі шешімдер жоқ. Құпия ақпараттың ағып кетуіне жол бермейтін өнімдерді тек жеке деректерді қорғау үшін ғана емес, сонымен қатар кәсіпорынның жұмыс істеуі үшін маңызды кез-келген ақпараттың ашылуына жол бермеу үшін де қолдануға болады [12]. Осы құралдарды пайдалана отырып, компания дербес деректерді қорғау жөніндегі талаптарына формальды түрде сәйкес келіп қана қоймай, сонымен қатар құпия ақпараттың басқа да түрлерін қорғау міндеттерін шеше алады.

Ағып кетуден қорғау жүйелері құпия деректерді деректер ағынынан оқшаулау және олардың рұқсатсыз берілуіне жол бермеу үшін арнайы алгоритмдерді қолданады. DLP жүйелері ақпаратты берудің әртүрлі арналарын басқару тетіктерін қамтамасыз етеді: электрондық пошта, лездік хабар алмасу, веб-пошта, принтерде басып шығару, алынбалы дискіде сақтау және т.б. сонымен қатар, DLP модульдері құпия деректердің ағып кетуіне жол бермейді, өйткені оларда ақпараттың қаншалықты құпия екенін анықтайтын механизмдер бар. Бұл ретте үш технология қолданылады: кілт сөздер және тұрақты тіркестер бойынша, анықтамалық құпия құжаттардың іздері бойынша немесе қауіпсіздік тегтері бойынша [13]. Соңғы уақытқа дейін әртүрлі өндірушілердің өнімдері осы әдістердің бірін қолданды, бірақ жақында осы әдістердің бірнешеуін қолданатын құпиялылықты бақылаудың кешенді механизмі жасалды.

Шын мәнінде, «Дербес деректер туралы» заң ақпараттық қауіпсіздік нарығына қатысушы компаниялардан дербес деректерді сақтау үшін ғана емес, сондай-ақ бүкіл ақпараттық жүйені толық бақылау, құпия ақпараттың немесе құпиялардың өзге де түрлерінің ағып кетуін болдырмау, сондай-ақ ақпараттық жүйенің аса маңызды бөліктерінің істен шығуын болдырмау үшін пайдалы болуы мүмкін қазіргі заманғы қауіпсіздік жүйесін құруды талап етеді [13]. Барлық компаниялардың қандай-да бір түрдегі жеке деректері болғандықтан, бұл заң кез-келген қызмет түріндегі ақпаратты қорғауға қойылатын мемлекеттік талаптар ретінде түсіндірілуі мүмкін және осы заңның талаптары еленбеуі керек. Сонымен қатар, көптеген компаниялар жеке деректерді қорғау бойынша біраз жұмыс жасады, өйткені желіні антивирус пен брандмауэр орнатпай пайдалану мүмкін емес.

Осы негізде ақпаратты қорғаудың корпоративтік жүйесін тез құра алатын және тексеруші органдар үшін қажетті құжаттар пакетін дайындауға қабілетті кәсіпорындар үшін үлкен қызмет саласы ашылады. «Дербес деректер туралы» заңға сәйкестік мәселесін шешудің тағы бір нұсқасы дербес деректерді қорғау функциясын бөгде ұйымдарға беру болып табылады және мұндай аутсорсингтік компаниялар Қазақстанда пайда бола бастайды. Алайда, бұл опция IT архитектурасының өзгеруімен байланысты болуы мүмкін және уақыт пен қосымша шығындарды қажет етеді.

Қолданылған әдебиеттер

1. Волчинская Е. К. Защита персональных данных.Опыт правового регулирования // № 6, 2010, 5-7 б.
2. Fersko-Weis H. Projekt management software// 2008, 178-226 б.
3. Марков А.П. “Проблемы и решения по защите персональных данных в информационных системах персональных данных // № 5, 20-27 б.
4. Баймакова и.А. Обеспечение защиты персональных данных // № 2, 2011,155-164 б.
5. Йошида Х. Будущее систем хранения // №5, 2010,34 б.
6. Федотов Н. К. Обременительная защита // № 18, 2010, 28-30 б.
7. Черняк Л. С. Барьеры на пути утечек данных // № 9, 2010, 12-14 б.
8. Круглова Н.И. Информационные технологии и вычислительные системы // № 5, 2010, 4 б.
9. Коржов В.В. Защита персональных данных: проблемы и пути решения // № 10, 2010, 11 б.
10. Долакова Е. П. Средства массовой информации и соблюдение конфиденциальности // № 7, 2010, 6-7 б.
11. Астахов А. В. Защита информации. Инсайдер [Электрондық ресурс] - қол жеткізу режимі: http://www.osp.ru/.
12. Сергеев Р. П. Защищая свои права. [Электрондық ресурс] - қол жеткізу режимі: http://www.osp.ru/.
13. Лушников А.К. Мера и средства защиты персональных данных. [Электрондық ресурс] - қол жеткізу режимі: http://www.osp.ru/.