**Айкерім Қоңырбаева**

**(Қазақстан, Астана қ.)**

**КӘСІПОРЫНДАҒЫ АҚПАРАТТЫҚ ҚАУІПСІЗДІК**

Ақпараттық қауіпсіздік - ақпараттың қорғалғандығы және кездейсоқ немесе қасақана әсер ететін табиғи немесе жасанды сипаттағы - ақпарат иесіне, оның қолданушыларын зардап шегуден, сонымен қатар ақпараттық салада адам мен азаматтың, қоғамның және мемлекеттің құқықтары мен мүдделерін нақты және ықтимал қатерлерден қорғайтын инфрақұрылым. Бұл мақалада мекеме, кәсіпорындардағы ақпараттық қауіпсіздік жайлы, оның ішінде ақпаратқа келіп түсер қауіп-қатер жайлы сөз қозғаймыз.

Кәсіпорынның ақпараттық қауіпсіздігі - корпоративтік деректердің құпиялылығы, тұтастығы, дәлме-дәлдігі және қолжетімділігі қамтамасыз етілетінқорғалу деңгейі.

Кәсіпорынның ақпараттық қауіпсіздігі корпоративтік деректерді қорғауға бағытталған ұйымдық-техникалық шаралардың көмегімен жүзеге асырылады. Ұйымдастыру шаралары кәсіпорындағы ақпараттық технология сервистері мен қауіпсіздік құралдары бойынша жүргізілетін жұмыстардың құжаттандырылуын қамтиды. Техникалық шаралар қолжетімділікті бақылаудың аппараттық және бағдарламалық құралдарынан, вирусқа қарсы қорғаудан, желіаралық экрандаудан, электромагниттік сәулеленуден қорғау және т.б. шаралардан тұрады.

Кәсіпорынның ақпараттық қауіпсіздік жүйелерінің бірнеше міндеттері бар:

* ақпарат құралдарында ақпаратты қауіпсіз сақтауды қамтамасыз ету;
* байланыс арналары бойынша берілетін деректерді қорғау;
* әртүрлі құжаттарға қол жеткізуді бақылау;
* резервтік көшірмелеу, ақпараттық жүйелерді кейіннен қалпына келтіру және т.б.

Кәсіпорындар мен ұйымдардың толыққанды ақпараттық қауіпсіздігі - деректер қауіпсіздігіне әсер ететін барлық маңызды оқиғалар мен жағдайларға нақты уақыт режимінде мониторинг жүргізуді білдіреді. Қорғау тәулік, жыл бойы жүзеге асырылуы тиісті және де ақпараттың өмірлік циклін - ақпараттың келіп түсуінен, құрылуынан бастап өзектілігін жойғанға немесе өшірілуіне дейінгі кезеңді қамтуы тиіс.Кәсіпорынның ақпараттық қауіпсіздік жүйесі барлық компьютерлік қатерлер мен осалдықтарды ескеруі керек.Ақпараттық тәуекелдерді талдау қауіптер мен осалдықтардың түрлерін түсіну, қорғау жүйесін құру және іске асыруға қажетті инвестициялау үшін қажет.

Тәуекелдерге талдау жүргізу үшін ақпараттық жүйе туралы мынадай деректер қажет:

1. Критикалық деңгей көрсетілген ақпараттың тізбесі.

2. Ақпараттық жүйенің осалдықтары және оған әсер ететін қауіптер туралы мәліметтер.

Бұл тізім арқылы біздің мекемеміздегі «Рәсімдеу бюросы» ақпараттық жүйесіндегі жеке деректерге қолжетімділікті бұғаттау барысында жұмыстар атқарылып, соның ішінде мүмкін болар қауіп-қатерлер мен осалдықтардың тізіміжинақталды.

«Рәсімдеу бюросы» ақпараттық жүйесі – мекеменің қауіпсіздігін арттыруға, бақылау-өткізу жұмыстарын оңтайландыруға бағытталған жүйе. Жүйедегі құнды мәлімет – жеке тұлғалардың мемлекеттің деректер қоры.

Ақпараттық жүйеге мүмкін болар қауіп-қатерлер төмендегі 1-ші кестеде, осалдықтардың тізімі 2-ші кестеде көрсетілген.

Кесте 1. Мүмкін- болар қауіптердің тізбесі.

|  |  |
| --- | --- |
| **Қауіп** | **Қауіптіңжалпысипаттамасы** |
| Апат | Өрт |
| Апат | Су тасқыны |
| Апат | Жерсілкінісі |
| Апат | Күшті найзағай |
| Апат | Террористік акт |
| Апат | Қоғамдықтолқулар, жаппайтәртіпсіздіктер |
| Апат | Опырылунемесесырғу |
| Апат | Көшкін |
| Апат | Өндірістегіапат |
| Механикалық ақау | Қуат көзін өшіру |
| Механикалық ақау | Жабдықтыңістеншығуы |
| Механикалық ақау | Желіжұмысындағыіркіліс |
| Механикалық ақау | Қоршағанортаныбақылаужүйесіндегііркіліс |
| Механикалық ақау | Құрылыстағыапат |
| Қаскүнемемес | Хабардаремесқызметкер |
| Қаскүнемемес | Хабардаремеспайдаланушы |
| Қаскүнем | Хакер, бұзғыш |
| Қаскүнем | Компьютерлікқылмыскер |
| Қаскүнем | Өндірістік тыңшылық |
| Қаскүнем | Үкімет қаржыландыратын тыңшылық |
| Қаскүнем | Әлеуметтік инженерия |
| Қаскүнем | Ұсталған қызметкер |
| Қаскүнем | Бұрынғы қызметкер |
| Қаскүнем | Террорист |
| Қаскүнем | Атқарылған жұмысқа немқұрайлы қарайтын қызметкер |
| Қаскүнем | Адалемесқызметкер (сыбайласжемқорлықпен айналысатыннемесе бопсалауға қатысы бар қызметкер) |
| Қаскүнем | Зияндымобильді код |

Кесте 2. Мүмкін- болар осалдықтардың тізбесі.

|  |  |
| --- | --- |
| **Осалдықкласы** | **Осалдық** |
| *Осалдықтаркласыныңжалпысипаттамасы* | *Осалдықтыңқысқашасипаттамасы* |
| Физикалықпараметрлері | Бекітілмегенесіктер |
| Физикалықпараметрлері | Компьютерлікжабдыққабақыланбайтынқолжетімділік |
| Физикалықпараметрлері | Өртсөндіружүйелерініңжеткіліксізтиімділігі |
| Физикалықпараметрлері | Ғимараттардыңсәтсізжобалары |
| Физикалықпараметрлері | Ғимараттар салу кезіндегіқателіктер |
| Физикалықпараметрлері | Құрылыскезінде тез тұтанатынматериалдардыпайдалану |
| Физикалықпараметрлері | Өңдеукезінде тез тұтанатынматериалдардыпайдалану |
| Физикалықпараметрлері | Бекітілмегентерезелер |
| Физикалықпараметрлері | Жеткіліксізсенімдіқабырғалар |
| Физикалықпараметрлері | Ішкіқабырғаларыбөлменіжоғарғы және төменгі жағынан толық қоршамайды |
| Табиғи | Жабдықшығаружелісіндеорналасқан |
| Табиғи | Жабдық су басу аймағында орналасқан |
| Табиғи | Жабдықтар көшкін түсу аймағында орналасқан |
| Құрал-жабдықтар | Түзетулердіңболмауы |
| Құрал-жабдықтар | Ескіргенмикробағдарлама |
| Құрал-жабдықтар | Қатежүйеконфигурациясы |
| Құрал-жабдықтар | Жүйелердің физикалыққауіпсіздігіқамтамасызетілмеген |
| Құрал-жабдықтар | Жалпықолжетімдіинтерфейстердебасқарухаттамаларырұқсатетілген |
| Бағдарламалыққамтамасызету | Ескіргенантивирустықбағдарламалыққамтамасызету |
| Бағдарламалыққамтамасызету | Түзетулердіңболмауы |
| Бағдарламалыққамтамасызету | Қосымшалардыәзірлеукезіндегікемшіліктер |
| Бағдарламалыққамтамасызету | Қасақанабұрмалаужасау |
| Бағдарламалыққамтамасызету | Әлсізорындардықасақанажасау |
| Бағдарламалыққамтамасызету | Қасақанақұрукемшіліктері |
| Бағдарламалыққамтамасызету | Конфигурация қателері |
| Орта | Электрліккедергілер |
| Байланыс | Шифрланбайтынжелілікхаттамалар |
| Байланыс | Бірнешежелілергеқосылу |
| Байланыс | Қажетсізхаттамаларөшірілмеген |
| Байланыс | Желісегменттеріарасындафильтрлеу жоқ |
| Адами фактор | Дұрыс анықталған рәсімдер |
| Адами фактор | Ұрланғанесептікдеректер |

Қауіп-қатердің орын алу себептерін анықтағаннан кейін, келесі ретте мекемеде қауіп-қатерді азайту және алдын алу бойынша келесі шаралар жүргізілу міндетті.

Кесте 3. Қауіп-қатерді азайту бойынша шаралар тізбесі

|  |
| --- |
| **Қауіп-қатерді азайту бойынша шаралар** |
| Жиналыстарды өткізукезіндешумогенератордыпайдалану |
| Қолжеткізудібақылаудықамтамасызету |
| Кабель коммуникацияларынэкрандау |
| Терезелергеторлардыорнату |
| Қолжетімділікті бақылау жүйесін ұйымдастыру, БӨП |
| Қызметкерлердің құпияақпаратқақолжеткізуінесепкеалудықамтамасызету |
| **DDoS-шабуылдардан (атака) қорғалу. Distributed-Denial-of-Service** |
| Вирустардың бағдарламалық қамтамаға енуін болдырмау, антивирустық БҚ қолдану |
| Деректердің резервті көшірмеленуі |
| Деректердің қайта қалпына келтіру жұмыстарының жоспарын дайындау |
| Ақпаратты электрондық форматта жіберу кезінде деректерді шифрлау (end-to-end protection). |

**Пайдаланылған әдебиеттер тізімі:**

1. [Ю. Родичев «Нормативная база и стандарты в области информационной безопасности» (2017)](https://www.ozon.ru/context/detail/id/137707095/)
2. [Е. Баранова, А. Бабаш «Информационная безопасность и защита информации» 3-шішығарылым. (2016)](https://www.ozon.ru/context/detail/id/136470734/)

**Ғылыми жетекшісі:**

Муканова Асель Сериковна

PhD доктор, Л.Н.Гумилев атындағы Еуразия Ұлттық Университетінің аға оқытушысы, Қазақстан, Астана қ.