БЕКІТІЛДІ
ҚОӘДСБ «Облыстық қан орталығы»
КМК директорының м.а.
2021 жылғы 31 желтоқсандағы
№139 бұйрығымен

Қостанай облысы әкімдігі денсаулық сақтау басқармасының «Облыстық қан орталығы» коммуналдық мемлекеттік кәсіпорнының ақпараттық қауіпсіздік САЯСАТЫ

ҚОӘДСБ «Облыстық қан орталығы» КМК
ақпараттық қауіпсіздік саясаты

Қостанай қ.- 2022 жыл

Мазмұны

ҚОӘДСБ «Облыстық қан орталығы» КМК
ақпараттық қауіпсіздік саясаты

1. Мақсаты

Осы ақпараттық қауіпсіздік саясаты (бұдан әрі - саясат) Қостанай облысы әкімдігі денсаулық сақтау басқармасының «Облыстық қан орталығы» коммуналдық мемлекеттік кәсіпорнында (бұдан әрі-ОҚО) қабылданатын ақпараттық қауіпсіздікті қамтамасыз ету саласындағы шаралар кешеніне қойылатын стратегиялық мақсаттарды, міндеттерді және негізгі талаптарды айқындау мақсатында әзірленді.

Ақпарат ОҚО-ның құнды активі болып табылады.

Ақпаратты іздеу, беру, сақтау, өңдеу және талдау үшін ақпараттық жүйелерді, ішкі жергілікті-есептеу желісін және ғаламдық Интернет желісін пайдалану ОҚО жұмысының тиімділігін арттыруға мүмкіндік береді.

Алайда, ақпараттық ресурстарды тиісінше пайдаланбау ОҚО-ны елеулі тәуекелге ұшыратуы, беделге нұқсан келтіруі, қаржылық, материалдық немесе материалдық емес залал келтіруі мүмкін.

ОҚО-ның ақпараттық ресурстарына жіберілген барлық қызметкерлер мен басқа да тұлғалар ақпаратты ұқыпты және ұтымды пайдалану және осы саясаттың талаптарын сақтау үшін жауапты болады.

ОҚО-ның ақпараттық ресурстарына қол жеткізу осы Саясатпен танысқаннан және ОҚО қызметкері қорғалатын ақпаратты құрайтын құжаттар мен мәліметтерді жария етпеу туралы міндеттемеге қол қойғаннан кейін ғана беріледі.

Ақпараттық қауіпсіздіктің барлық рәсімдері қол жеткізуге бағытталған негізгі мақсат ақпараттың қауіпсіздігіне қатер төндіретін оқиғалардан болатын залалды олардың алдын алу немесе олардың салдарын барынша азайту арқылы төмендету болып табылады.

Ақпараттық қауіпсіздікті қамтамасыз ету ОҚО-ның қолда бар ақпараттық ресурстарына барлық ықтимал қатерлермен байланысты тәуекелдер мен экономикалық ысыраптарды азайту үшін қажет.

2. Қолдану саласы

Осы Саясаттың күші ОҚО-ның барлық қызметкерлеріне қолданылады. Ақпараттық қауіпсіздік рәсімдері барлық мүдделі тараптардың үміттерін ескереді және ОҚО-ның барлық қызметкерлерінің орындауы үшін міндетті, сондай-ақ ОҚО-мен және оның қызметімен тікелей өзара байланысты бөлігінде ОҚО-ның ақпараттық жүйелері мен құжаттарына рұқсаты бар клиенттер мен өзге де үшінші тұлғалардың назарына жеткізіледі.

Осы Саясат ОҚО-ның кез келген қызметкеріне және оның ресурстарын пайдаланушыға қолжетімді құжат болып табылады және ОҚО басшылығы ресми түрде қабылдаған ақпараттық қауіпсіздікті қамтамасыз ету және мақсаттарды, процестер мен рәсімдерді жүйеленген баяндау негізінде оны басқару жүйесін білдіреді.

Осы Саясаттың ережелері ішкі нормативтік және әдістемелік құжаттарда, сондай-ақ шарттарда пайдалану үшін қолданылады.

3. Терминдер мен анықтамалар

Деректер базасы - кез-келген физикалық немесе виртуалды жүйенің сипаттамаларын сипаттайтын құрылымдалған, ұйымдастырылған мәліметтер жиынтығы.

Қорғалатын ақпарат - қолданыстағы заңнамаға және ОҚО-ның ішкі нормативтік құжаттарына сәйкес коммерциялық, қызметтік немесе заңмен қорғалатын өзге де құпияға жатқызылған мәліметтерді қамтитын ақпараттық ресурстар.

Ақпараттық ресурстар-ақпараттық жүйелердегі құжаттар мен құжаттар жиынтығы.

Ақпараттық жүйелер-ақпаратты сақтауға, іздеуге және өңдеуге арналған жүйелер және ақпаратты қамтамасыз ететін және таратын тиісті ұйымдастырушылық ресурстар.

ЖЕЖ (жергілікті-есептеу желісі) – пайдаланушыларға компьютер ресурстарын: бағдарламаларды, файлдарды, қалталарды, сондай-ақ перифериялық құрылғыларды: принтерлерді бірлесіп пайдалануға мүмкіндік беретін кабельдер (UTP, FTP, STP, коаксиалды кабель, телефон желілері, радиоарналар және т. б.) арқылы өзара байланысқан

дербес компьютерлердің белгілі бір санынан тұратын коммуникациялық жүйе, плоттерлер, дискілер, модемдер және т. б.

АТҚҚЕБ - ОҚО ақпараттық технологиялар мен қауіпсіздікті қамтамасыз ету бөлімі.

Пайдаланушы - өзінің лауазымдық міндеттерін орындау үшін жұмыс станциясын және ОҚО жергілікті-есептеу желісін пайдаланатын ОҚО қызметкері.

Бағдарламалық қамтылым - осы бағдарламаларды пайдалану үшін қажетті ақпаратты және бағдарламалық құжаттарды өңдеу жүйесінің бағдарламаларының жиынтығы.

БҚ - мыналарды қамтитын **стандартты БҚ:**

* операциялық жүйе (Microsoft Windows 8, 8.1, 10, 11 және барлық кейінгі нұсқалар);
* құрылғының өзекті драйверлерінің жиынтығы;
* Microsoft Windows операциялық жүйелеріне арналған өзекті жаңартулар жиынтығы;
* кеңсе бағдарламаларының жиынтығы (Microsoft Office 2010, 2013, 2016, 2019, 2021 және барлық кейінгі нұсқалар);
* PDF (Adobe Reader) форматындағы электрондық жарияланымдарды қарауға арналған бағдарлама;
* өзекті вирусқа қарсы базалар жиынтығы бар вирусқа қарсы БҚ;

Мультимедиаконтент – жұмыс станциясында түрлі медиа-элементтерді – барлық форматтағы әуендерді, реалтондарды, барлық форматтағы бейнероликтер мен толықметражды фильмдерді, түрлі-түсті және анимациялық суреттерді, экран сақтаушыларды (сағаттарды), ойындар мен java-қосымшаларды, сондай-ақ түрлі сипаттағы ойын-сауық ақпаратты алуға, қарауға немесе ойнатуға мүмкіндік беретін қызмет.

Жұмыс станциясы-бұл жергілікті есептеу желісі құрамына қосылған компьютер.

Резервтік көшірме жасау-бүлінген немесе бұзылған жағдайда деректерді бастапқы немесе жаңа жерде қалпына келтіруге арналған тасымалдағышта (қатты диск, деректерді сақтау жүйесі, ауыстырылатын медиа және т.б.) деректердің көшірмесін жасау процесі.

Бақылау қызметі – ОҚО сапаны басқару бөлімі және пациенттерді қолдау қызметі.

Әлеуметтік инженерия дегеніміз – қолданушылардың қаскүнем үшін қажет әрекеттерді орындау немесе пайдаланушылардан ақпарат немесе қызмет алу мақсатында пайдаланушыларды алдау немесе адастыру.

ЭМЖ- электрондық мұрағат жүйесі, электрондық құжаттарды құрылымдық сақтау жүйесі, қол жеткізу құқықтарын сақтау сенімділігін, құпиялылығын және аражігін ажыратуды, құжаттың пайдалану тарихын қадағалауды, жылдам және ыңғайлы іздестіруді қамтамасыз етеді.

ЭЦҚ - электрондық цифрлық қолтаңба, қолтаңбаның жабық кілтін пайдалана отырып, ақпаратты криптографиялық түрлендіру нәтижесінде алынған электрондық құжаттың деректемесі.

4. Жауапкершілік матрицасы

Ақпараттық қауіпсіздікті қамтамасыз ету процесін тиімді басқару үшін ОҚО-да процестер мен кіші процестер (процестің жекелеген элементтері) үшін жауапкершілік матрицасы қолданылады.

Жауапкершілік матрицасы процестің әр қатысушысының жеке кезеңдер мен тапсырмаларды орындау үшін жауапкершілік дәрежесін белгілейді. Жауапкершілік матрицасын құру кезінде RACI әдістемесі қолданылды.

RACI әдістемесі процестің әрбір кезеңінде тапсырмаларды орындау кезінде процеске қатысушылардың жауапкершілігін жоспарлаудың ыңғайлы және көрнекі құралы болып табылады.

RACI термині аббревиатура болып табылады:

- **Орындаушы** (Responsible) - тапсырманы орындайды, оны шешу тәсілін таңдауға жауап бермейді, бірақ іске асыру сапасы мен мерзіміне жауап береді. Әр тапсырмада кем дегенде бір орындаушы болуы керек.
- **Жауапты** (Accountable) – тапсырманың орындалуына толық жауап береді, іске асыру тәсілі бойынша шешім қабылдауға

құқылы. Тапсырмаға жауапты адам ретінде тек бір адам тағайындалуы мүмкін.

- **Кеңесші** (Consult before doing) - мәселелерді шешу барысында кеңес береді, іске асыру сапасын бақылайды.
- **Бақылаушы** (inform after doing) – процестің міндеттерін шешу барысында кеңес бере алады, жауап бермейді.

Кезеңдер мен міндеттер	**Орындаушылар**					
	Медициналық қызмет сапасын бақылау бойынша директордың орынбасары	**Бақылау қызметі**	**Заңгер**	**АТҚҚЕБ басшысы**	**АТҚҚЕБ маманы (жүйелік әкімші)**	**ОҚО-ның барлық қызметкерлері**
Ақпараттық қауіпсіздікті басқару процесі	**Ж*К**	**К**	**Б**			
№1 кіші процесс: Әкімшілік-құқықтық және ұйымдастыру шаралары				**ЖО**	**О**	**О**
№2 кіші процесс: Физикалық қауіпсіздік шаралары				**ЖО**	**О**	**О**
№3 кіші процесс: Бағдарламалық-техникалық шаралар				**ЖО**	**О**	**О**

Ж* - процеске жауапты;
К - кеңесші;
Б - бақылаушы;
Ж - кіші процеске жауапты;
О - орындаушы.

5. Процесс жұмысын қамтамасыз ету

5.1. Жалпы

Ақпараттық қауіпсіздікті басқару-бұл жеке процесс және ОҚО-ның жалпы басқару жүйесінің міндетті бөлігі.

ОҚО ақпараттық қауіпсіздікті қамтамасыз ету мәселелеріне ерекше назар аударады, ақпараттық қауіпсіздікті басқару жүйесін, ақпараттық қауіпсіздік қатерлерінен қорғаудың қолданылатын құралдары мен тәсілдерін үнемі жетілдіріп отырады, сондай-ақ ақпаратты қорғау саласындағы құзыреттілікті жоғары деңгейде ұстау үшін ОҚО қызметкерлерін үздіксіз оқытуды қамтамасыз етеді.

Ақпараттық қауіпсіздік саясаты иесі және пайдаланушысы ОҚОболып табылатын барлық ақпараттық жүйелер мен құжаттарды қамтиды. Ақпараттық қауіпсіздікті қамтамасыз ету ОҚО қызметін табысты жүзеге асыру үшін қажетті шарт болып табылады.

ОҚО ақпараттық қауіпсіздігінің негізінде ақпараттық қауіпсіздік оқиғаларын іске асыру ықтималдығын азайтуға бағытталған тәуекелге бағытталған тәсіл жатыр.

Ақпараттық қауіпсіздікті қамтамасыз ету ОҚО-ның қолда бар ақпараттық ресурстарына барлық ықтимал қатерлермен байланысты тәуекелдер мен экономикалық ысыраптарды азайту үшін қажет. Осы мақсатта ақпараттың негізгі қасиеттерін сақтау қажет, атап айтқанда:

1) қолжетімділік-осыған тиісті өкілеттіктері бар субъектілердің ақпаратына уақтылы кедергісіз қол жеткізу қабілетімен сипатталатын қасиет;

2) құпиялылық-осы ақпаратқа рұқсаты бар субъектілер тобына шектеулер енгізу қажеттілігін көрсететін және жүйенің (ортаның) оған қол жеткізуге өкілеттігі жоқ субъектілерден көрсетілген ақпаратты құпия сақтау қабілетімен қамтамасыз етілетін қасиет;

3) тұтастық – ақпараттың оның бұрмаланбаған түрде (оның қандай да бір тұрақты күйіне қатысты өзгермейтін) болуын құрайтын қасиеті.

ОҚО ақпараттық қауіпсіздігін қамтамасыз етудің негізгі объектілері болып мынадай элементтер танылады:

1) қолданыстағы заңнамаға және ОҚО ішкі нормативтік құжаттарына сәйкес коммерциялық, қызметтік немесе заңмен қорғалатын өзге де құпияға жатқызылған мәліметтерді қамтитын ақпараттық ресурстар;

2) қорғалатын ақпаратты өңдеу, беру және сақтау жүзеге асырылатын ақпараттандыру құралдары мен жүйелері (есептеу техникасы, ақпараттық-есептеу кешендері, желілер, жүйелер);

3) қорғалатын ақпаратты өңдеу жүргізілетін ОҚО автоматтандырылған жүйелерінің бағдарламалық құралдары (операциялық жүйелер, деректер базасын басқару жүйелері, басқа да жалпы жүйелік және қолданбалы БҚ);

4) ақпараттық ресурстарды басқарумен және пайдаланумен байланысты ОҚО процестері;

5) қорғалатын ақпаратты өңдеу құралдары орналасқан үй-жайлар;

6) жұмыс үй-жайлары мен қызметкерлердің кабинеттері, ОҚО-ның үй-жайлары;

7) қорғалатын ақпаратқа рұқсаты бар ОҚО жұмыскерлері;

8) ашық ақпаратты өңдейтін, бірақ қорғалатын ақпарат өңделетін үй-жайларда орналастырылған техникалық құралдар мен жүйелер.

Қорғалатын ақпарат:

қағаз тасығыштарға салынған.;

электрондық нысанда бар (компьютерлік технологиялардың көмегімен өңделеді, беріледі және сақталады, техникалық құралдарды қолдану арқылы жазылады және көбейтіледі);

- телефон, телефакс, телекс және т.б. арқылы беріледі. электрлік сигналдар түрінде;

ОҚО ақпараттық қауіпсіздік жүйесін құру және оның жұмыс істеуі келесі принциптерге сәйкес жүзеге асырылады:

- заңдылық – ақпараттық қауіпсіздікті қамтамасыз ету бойынша қабылданған кез келген іс-әрекеттер қолданыстағы заңнама негізінде жүзеге асырылады;

- негізгі қызметке бағдарлану - ақпараттық қауіпсіздік ОҚО-ның негізгі қызметін қолдау процесі ретінде қарастырылады;

- үздіксіздік – ақпаратты қорғау жүйелерін басқару құралдарын қолдану, ОҚО-ның ақпараттық қорғалуын қамтамасыз ету жөніндегі кез келген іс-шараларды іске асыру ОҚО-ның ағымдағы бизнес-процестерін үзбей немесе тоқтатпай жүзеге асырылады;

- кешенділік дегеніміз – ақпараттық ресурстардың өмірлік циклі бойында, оларды қолданудың барлық технологиялық кезеңдерінде және барлық жұмыс режимдерінде қауіпсіздігін қамтамасыз ету;

- негізділік және экономикалық мақсаттылық-пайдаланылатын мүмкіндіктер мен қорғау құралдары ғылым мен техниканың тиісті даму деңгейінде іске асырылады, қауіпсіздіктің берілген деңгейі тұрғысынан негізделген және қойылатын талаптар мен нормаларға сәйкес келеді;

- басымдылық – ақпараттық қауіпсіздікке нақты, сондай-ақ ықтимал қатерлерді бағалаудағы маңыздылық дәрежесі бойынша ЦКБ-ның барлық ақпараттық ресурстарын санаттау (саралау);

- қажетті білім және артықшылықтардың ең төменгі деңгейі-пайдаланушы артықшылықтың ең төменгі деңгейін алады және өз өкілеттіктері шеңберіндегі қызметті орындау үшін қажетті деректерге ғана қол жеткізе алады;

- техникалық құралдарды пайдалану және ақпараттық қауіпсіздік шараларын іске асыру кәсіби дайындалған мамандармен жүзеге асырылады;

- хабардарлық және жеке жауапкершілік – барлық деңгейдегі басшылар мен орындаушылар ақпараттық қауіпсіздіктің барлық талаптарын біледі және осы талаптарды орындауға және ақпараттық қауіпсіздіктің белгіленген шараларын сақтауға дербес жауапты болады;

- өзара іс – қимыл және үйлестіру-ақпараттық қауіпсіздік шаралары ЦКБ-нің тиісті құрылымдық бөлімшелерінің өзара байланысы, қойылған мақсаттарға қол жеткізу үшін олардың күш-жігерін үйлестіру, сондай-ақ сыртқы ұйымдармен, кәсіптік қауымдастықтармен және қоғамдастықтармен, мемлекеттік органдармен, заңды және жеке тұлғалармен қажетті байланыстар орнату негізінде жүзеге асырылады;

- растау-маңызды құжаттама және барлық жазбалар-ақпараттық қауіпсіздік талаптарының орындалуын және оны ұйымдастыру

жүйесінің тиімділігін растайтын құжаттар Жедел қол жеткізу және қалпына келтіру мүмкіндігімен жасалады және сақталады.

5.2. Процесс кезеңдерінің сипаттамасы

5.2.1. Әкімшілік-құқықтық және ұйымдастыру шаралары

Әкімшілік-құқықтық және ұйымдастыру шаралары мыналарды қамтиды (бірақ олармен шектелмейді):

- Қазақстан Республикасының заңнамасы және ОҚО-ның ішкі құжаттары талаптарының орындалуын бақылау;
- ақпараттық қауіпсіздік рәсімдерін қолдайтын ережелерді, әдістемелер мен нұсқаулықтарды әзірлеу, енгізу және орындалуын бақылау;
- ОҚО бизнес-процестерінің ақпараттық қауіпсіздік рәсімдерінің талаптарына сәйкестігін бақылау;
- ОҚО қызметкерлерін ақпараттық жүйелермен жұмыс істеуге және ақпараттық қауіпсіздік талаптарына ақпараттандыру және оқыту;
- ақпараттың рұқсат етілмеген таралу арналарына, соған байланысты оқиғаларға ден қою, локализациялау және салдарын азайту;
- ақпараттық қауіпсіздіктің жаңа тәуекелдерін талдау;
- төтенше жағдайлар кезіндегі әрекеттерді анықтау;
- ОҚО қызметкерлерін жұмысқа қабылдау және жұмыстан босату кезінде алдын алу шараларын жүргізу;

Мына мақсаттар үшін шаралар кешенін, оның ішінде құқықтық, ұйымдастырушылық және техникалық шараларды қолдану арқылы жүзеге асырылатын қызметкерлер мен донорлардың жеке деректерін қорғау туралы ОҚО-ның кепілдігі:

1) жеке өмірге қол сұғылмаушылыққа, жеке және отбасылық құпияға құқықтарды жүзеге асыру;

2) олардың тұтастығы мен сақталуын қамтамасыз ету;

3) олардың құпиялылығын сақтау;

4) оларға қол жеткізу құқығын жүзеге асыру;

5) оларды заңсыз жинау мен өңдеуге жол бермеу.

5.2.1.1. Ақпараттық қауіпсіздік инциденттері туралы хабарлау

Пайдаланушылар ықтимал инциденттерді немесе ақпараттық қауіпсіздікті бұзу әрекеттерін тани білуі және олар туралы бақылау қызметіне және ақпараттық технологиялар мен қауіпсіздікті қамтамасыз ету бөліміне дереу хабарлай алуы тиіс. Инциденттерді немесе ақпараттық қауіпсіздікті бұзу әрекеттерін дербес зерттеуге тыйым салынады және ОҚО-ның ақпараттық қауіпсіздігіне шабуыл ретінде бағаланады.

Ақпараттық қауіпсіздік инциденттерінің белгілері мыналарды қамтиды (бірақ олармен шектелмейді):

- монитор экранынан ақпаратты суретке түсіру немесе ақпаратты алынбалы тасымалдағышқа көшіру мақсатымен пайдаланушының жұмыс орнының жанында рұқсат етілмеген адамның ұзақ уақыт болуы;
- есептік жазбаларды күтпеген жерден бұғаттау;
- ЖЕЖ-не немесе ақпараттық жүйеге кіру/тіркелудің ұзақ уақыты;
- ЖЕЖ-де белгісіз файлдардың пайда болуы;
- құпиялылықты бұзу;

деректердің күтпеген жерден бұрмалануы, ЖЕЖ-де немесе ақпараттық жүйелерде қате немесе толық емес деректердің пайда болуы;

- штаттан тыс мінез-құлық немесе жергілікті-есептеу желісі, оның жекелеген сегменттері немесе сервистерінің істен шығуы;
- штаттан тыс мінез-құлық немесе ақпараттық жүйенің істен шығуы.

АТҚҚЕБ басшысы ақпараттық қауіпсіздікті бұзу тәуекелінің иесі ретінде тәуекелді сәйкестендіргеннен және оның әсер ету дәрежесін анықтағаннан кейін «тәуекелдерді азайту және оларды және болдырмау жөніндегі ұсыныстарды тіркеу бланкісін» толтыруға, сондай-ақ болған инцидент туралы ОҚО-ның ішкі порталында жариялау үшін баспасөз хабарламасын дайындауға міндетті.

5.2.1.2. Авторлық құқықты қорғау

Көптеген бағдарламалар, фильмдер, электронды кітаптар, музыкалық және басқа да мультимедиялық файлдар авторлық құқық субъектілері болып табылады. Мұндай файлдарды көшіруге және таратуға тыйым салынуы мүмкін.

Авторлық құқықпен қорғалған бағдарламалар мен контенттерді ЖЕЖ-де және жұмыс станцияларында көшіруге, таратуға, көбейтуге және сақтауға тек құқық иесінің жазбаша рұқсатымен немесе «заңды пайдалану» болып саналатын басқа жағдайларда ғана рұқсат етіледі.

Егер пайдаланушыда авторлық құқық туралы заңнаманың қолданылуына қатысты қандай да бір сұрақтар туындаса, олар ОҚО заңгеріне түсініктеме алу үшін жүгінуі тиіс.

Пайдаланушылар, егер керісінше сенімді ақпарат болмаса, барлық бағдарламалар мен басқа файлдар авторлық құқықпен қорғалған деп болжауы керек.

5.2.2. Физикалық қауіпсіздік шаралары

Физикалық қауіпсіздік шаралары мыналарды қамтиды (бірақ олармен шектелмейді):

- өткізу және объектішілік режимдерді ұйымдастыруды;
- қорғалатын объектілердің қауіпсіздік периметрін құруды;
- күзетілетін объектілерді тәулік бойы күзетуді, оның ішінде техникалық қауіпсіздік құралдарын пайдалана отырып ұйымдастыруды;;
- күзетілетін объектілердің өрт қауіпсіздігін ұйымдастыру;
- ОҚО қызметкерлерінің шектеу қойылған аймақтарға кіруін бақылау.

Шектеу қойылған үй-жайлар

ОҚО-да кіруіге шектеу қойылған үй-жайларға серверлік үй-жай және мұрағат жатады,

Серверлік үй-жайға кіруге рұқсаты барлар:

- коммуникациялық және серверлік жабдықтарға қызмет көрсету және пайдалану бойынша жұмыстарды орындау үшін АТҚҚЕБ қызметкерлері.

Архивке кіруге рұқсаты барлар:

- ОҚО басшылары;

- ОҚО-ның архив қызметін ұсынатын қызметкерлер;

Кіру шектеу қойылған үй-жайларға келушілерге үй-жайға қатысты шектеулердің себептері және орындалуы тиіс ескертулер туралы нұсқау берілуі тиіс.

Серверлік үй-жай мынадай талаптарға келуі тиіс:

- үй-жай бөгде адамдардың бақылаусыз кіру мүмкіндігін болдырмай, үнемі күзетіліп тұруы тиіс;

- бейнебақылау және оқиғаларды тіркеу жүйесінің болуы қажет. Оқиғаларды online режимінде де, кез келген мұрағаттық фрагменттерде де қарау мүмкіндігі қамтамасыз етілуі тиіс. Мұрағаттың ұзындығы кемінде 30 күнтізбелік күнді құрауы тиіс;

- стационарлық телефон болуы керек;

- автоматты газды өрт сөндіру жүйесі болуы қажет;

- өрт туралы ауызша хабарлау жүйесі болуы керек;

«қыс-жаз» типті ауаны салқындату және салқындату жүйесі болуы керек;

- әрбір розетка тобы үшін кіріс сөндіргіші және автоматты ажыратқыштары бар энергиядан тәуелсіз жүйе болуы керек;

- жылу бұру және дренаждың арнайы жүйесі болуы керек;

- қажетті жиһаз жинағымен және компьютерлік техникамен жабдықталған ЖЕЖ әкімшісінің жұмыс орны болуы керек;

- кіру тек блоктау, кіру картасы, кілт немесе үй-жайға жауапты адам берген басқа қауіпсіздік құралдары арқылы ғана мүмкін болады.

АТҚҚЕБ қызметкерлерінің серверлік үй-жайды жинауына алдын ала нұсқау берместен және ОҚО жауапты қызметкерінің міндетті түрде қатысуынсыз жүргізуге тыйым салынады.

Серверлік үй-жайға кіру тәртібі, кілттерді беруді тіркеу, бару мақсаттары және жүргізілген жұмыс түрлері жеке ішкі құжатпен (Серверлік үй-жайға бару журналы) реттеледі.

Техникалық құралдар кешенінің (проекторлар, аудиомикшерлер, күшейткіштер, бейнеконференцбайланыс жабдықтары, микрофондар, дыбысты шығаратын стерео құрылғылар) қалыпты жұмыс істеуін қамтамасыз ету АТҚҚЕБ-не жүктелген.

Бейне-материалдарды (фильмдер, бейне-роликтер) көрсету үшін АТҚҚЕБ қызметкерлерімен келесі шарттарды алдын ала келісу қажет:

- бейне материалдардың форматы;
- ұзақтығы (минут);
- ойнату режимі;
- бейне материал көзі;
- ойнату үшін жауапты пайдаланушы.

Пайдаланушыларға аудио - бейне ойнатқыштарды, сондай-ақ плагиндер мен оларға қосымшаларды өз бетінше орнатуға тыйым салынады.

5.2.3. Бағдарламалық-техникалық шаралар

- Бағдарламалық және аппараттық қамтамасыз ету шаралары мыналарды қамтиды (бірақ олармен шектелмейді):
- лицензияланған бағдарламалық қамтамасыз етуді және ақпаратты қорғаудың сертификатталған құралдарын пайдалануды;
- периметрді қорғау құралдарын пайдалану (Firewall, IPS және т. б.);
- кешенді антивирустық қорғауды қолдану;

- ақпараттық жүйелерге енгізілген ақпараттық қауіпсіздік құралдарын пайдалану;
- ақпараттың тұрақты резервтік көшірмесін қамтамасыз ету;
- бірінші кезекте артықшылықты пайдаланушылардың құқықтары мен әрекеттерін бақылау;
- нормативтік құқықтық актілерде белгіленген тәртіппен ақпаратты криптографиялық қорғау құралдарын қолдану;
- аппараттық құралдардың ақаусыз жұмысын қамтамасыз ету;
- ақпараттық жүйенің маңызды элементтерінің жағдайын бақылау.

5.2.3.1. Пайдаланушы тіркеулік жазбасы және оларға құпиясөздер

ОҚО ақпараттық ресурстарына қол жеткізу үшін әрбір пайдаланушыға бірегей (ОҚО ЖЕЖ шеңберінде) есептік жазба – дербес сәйкестендіргіш (логин) және құпиясөз беріледі.

Есептік жазбаны АТҚҚЕБ қызметкері пайдаланушыларға келесі құжаттардың көшірмелерін ұсынғаннан кейін ғана жасайды:

- ОҚО-ға жұмысқа қабылдау туралы бұйрық;
- жеке басын куәландыратын құжат.

Жаңа есептік жазбаны жасаған кезде немесе егер пайдаланушы өз құпиясөзін ұмытып қалса, оған уақытша құпиясөз беріледі, оны ОҚО-ның ЖЕЖ-не бірінші рет кірген кезде өзгерту керек.

Пайдаланушылар құпиясөздерін құпия сақтауға және құпиясөздердің күрделілігін қамтамасыз ету ережелерін сақтауға міндетті:

- құпиясөздің минималды ұзындығы-5 таңба;
- бұл құпиясөз оңай болжанатын реттілікте болмауы керек;
- құпия сөз бірдей сандардан немесе әріптерден тұрмауы керек.

Құпиясөзді үнемі өзгерту керек (60 күнде кемінде 1 рет).

Құпиясөзді әр 60 күн сайын немесе пайдаланушының құпиясөзі ашылған белгілер болған кезде алдыңғы беске сәйкес келмейтін жаңасына ауыстыру керек. Соңғы жағдайда құпиясөзді бір жұмыс күнінен кешіктірмей дереу өзгерту керек.

Өзінің логині мен құпиясөзін басқа пайдаланушыларға беруге және басқа пайдаланушылардың логинімен ақпараттық жүйелерге кіруге немесе ОҚО-ның ақпараттық жүйелерінде, басқа ақпараттық жүйелерде және Интернет желісінде басқа тұлға ретінде өзін кез келген тәсілмен танытуға тыйым салынады.

Логиндер мен құпиясөздерді оңай қол жетімді жерлерде жазбаша түрде сақтауға болмайды.

Пайдаланушы өзінің есептік жазбасы атынан жасалған барлық әрекеттер үшін жауапты болады.

Жұмыс станциясына немесе ОҚО-ның ақпараттық жүйелеріне кірген кезде парольдерді автоматты түрде енгізуді баптауға тыйым салынады.

Қызметкер жұмыстан босатылған және соңында қол қойылған кету парағын АТҚҚЕБ -ға ұсынған кезде, АТҚҚЕБ қызметкерлері жұмыстан босатылған қызметкердің есептік жазбасымен келесі әрекеттерді орындайды:

- пайдаланушы есептік жазбасы дереу өшіріледі;
- жергілікті профиль туралы ақпарат өшірілгеннен кейін 90 күннен кейін жойылады.

5.2.3.2. Пайдаланушылардың жұмыс станцияларының қауіпсіздігі

ОҚО қызметкерлерге өздерінің лауазымдық міндеттерін орындау үшін жұмыс станцияларын ұсынады.

Жұмыс станцияларын баптауды және оларға стандартты БҚ орнатуды АТҚҚЕБ қызметкерлері жүргізеді. Қосымша БҚ немесе жабдықты орнату, стандартты баптауларды өзгерту немесе жұмыс станцияларын жөндеу қажет болған жағдайда пайдаланушы АТҚҚЕБ-не жүгінеді. Пайдаланушылардың өз бетінше жөндеуіне, жұмыс станцияларының конфигурациясына өзгерістер енгізуіне, жабдықты орнатуына немесе алып тастауына тыйым салынады.

БҚ және АТҚҚЕБ қызметкерлері орнатқан басқа бағдарламаларды өздігінен орнатуға немесе іске қосуға тыйым салынады.

Пайдаланушыларға, егер пайдаланушының тікелей басшысының өкімі болмаса, басқа тұлғаларға (АТҚҚЕБ қызметкерлерінен басқа) өздерінің жұмыс станцияларына кіруге рұқсат беруге тыйым салынады.

Пайдаланушылар жұмыс күні ішінде жұмыс орнынан кететін болса жұмыс станциясын бұғаттауы керек («Ctrl + Alt + Del» пернетақтасындағы пернелер тіркесімі), жұмыс күні аяқталғаннан кейін оны өшіріу керек.

Құпиясөзді енгізген кезде және құпия ақпаратпен жұмыс істеген кезде, пайдаланушылар бөгде адамдардың монитор экранынан ақпаратты немесе енгізілетін құпиясөзді қарап отыра алмайтындығына көз жеткізуі тиіс.

Пайдаланушылар 5 минут әрекетсіздіктен кейін автоматты түрде қосылатын экран сақтағыштарын пайдалануға міндетті, олардан шығу үшін құпиясөз қажет.

5.2.3.3. Вирустар мен зиянды бағдарламалық қамтылымнан қорғау

ОҚО ЖЕЖ вирусқа қарсы қорғау бойынша жұмыстардың барлық кешенін АТҚҚЕБ жүзеге асырады.

Пайдаланушының серверін немесе жұмыс станциясын жаңартылған вирусқа қарсы бағдарламалық қамтылыммен қорғаусыз ОҚО ЖЕЖ-не қосуға тыйым салынады.

Өзінің дербес компьютерін немесе жұмыс станциясын ОҚО-ның ЖЕЖ-не қосу қажет мердігер ұйымдар АТҚҚЕБ қызметкерлерінің алдын ала рұқсатын алады.

ОҚО-ның барлық жұмыс станцияларында желілік басқарылатын жүйе пайдаланылады, онда вирусқа қарсы дерекқорларды жаңарту автоматты режимде жүргізіледі. Егер мұндай мүмкіндік болмаса, әрбір жұмыс станциясына АТҚҚЕБ қызметкерлері вирусқа қарсы дерекқорды автоматты түрде жаңарта отырып, дербес вирусқа қарсы БҚ орнатады.

Пайдаланушыларға жұмыс станцияларында орнатылған вирусқа қарсы бағдарламаларды жоюға немесе олардың жұмысын тоқтатуға тыйым салынады.

Егер вирус немесе зиянды бағдарлама анықталса немесе күдіктенсе, пайдаланушы жұмыс станциясындағы жұмысын дереу тоқтатып, бұл туралы АТҚҚЕБ-не хабарлауы керек.

Вирустар мен зиянды бағдарламаларды жою әдетте автоматты түрде жүреді. Пайдаланушыларға вирустардан немесе зиянды бағдарламалардан өз бетінше құтылуға тырысуға тыйым салынады.

Егер болжамды вирус немесе зиянды бағдарлама пайдаланушының БҚ немесе ақпаратын зақымдай/жоя бастады деген

күдік болса, жұмыс станциясын дереу өшіріп, ол туралы АТҚҚЕБ-не хабарлау қажет.

Пайдаланушыларға ОҚО ішінде және одан тыс қандай да бір нысанда зиянды немесе өзін-өзі көбейтетін кодтарды сақтауға, зерттеуге, жасауға, енгізуге және/немесе таратуға тыйым салынады.

5.2.3.4. «Таза үстел» саясаты

«Таза үстел» саясатын қамтамасыз ету пайдаланушылардың өздеріне жүктелген.

Пайдаланушылар ақпараттың құпиялылық санатына сәйкес кез келген түрін (баспа көшірмелері, дискілер, USB-флэш-тасымалдағыштар және т.б.) қорғауды қамтамасыз етеді.

Пайдаланылмайтын құжаттар, алмалы-салмалы тасымалдағыштар және компьютерлік құралдар (әсіресе, жұмыстан тыс уақытта) осы мақсаттарға қолайлы, мүмкіндігінше кілтке жабылатын шкафта және (немесе) тиісті сақталуын қамтамасыз ететін қандай да бір басқа құрылғыларда сақталады.

Кіріс және шығыс хат-хабарлар, сондай-ақ факсимильдік аппараттар жалпыға қолжетімді орындарда болмауы тиіс.

Пайдаланылмайтын құпия ақпарат, әсіресе кеңседе ешкім болмаған кезде сейфтерде, құлыпталатын шкафтарда сақталады.

Входящая и исходящая корреспонденция, а также факсимильные аппараты, не должны находиться в общедоступных местах.

Құпия құжаттарды басып шығару, сканерлеу, көшіру немесе факс арқылы жіберу кезінде қараусыз қалдыруға тыйым салынады.

5.2.3.5. Физикалық қауіпсіздік

Әрбір жұмыс станциясына немесе компьютерлік жабдықтар жиынтығына жауапты адам бекітіледі. Жабдықты қабылдау және/немесе оны басқа жауапты тұлғаға тапсыру жабдыққа материалдық жауапты тұлға тиісті құжаттарды ресімдегеннен кейін ғана жүзеге асырылады.

Жұмыстан босатылған кезде пайдаланушы АТҚҚЕБ-не кету парағына қол қоюға міндетті.

Қызметкерлерге ОҚО ЖЕЖ-ға өз компьютерлерін (ноутбуктер, планшеттік компьютерлер) немесе басқа жабдықтарды әкелуге және қосуға тыйым салынады.

Ноутбуктерді немесе басқа да компьютерлік жабдықтарды, сондай-ақ оргтехниканы ОҚО үй-жайларынан материалдық рұқсатнама болған кезде ғана шығаруға болады. Мүлікке берілетін материалдық рұқсаттамада жабдықтың маркасы (өндірушісі) туралы ақпарат, қысқаша техникалық сипаттамасы, сериялық, сондай-ақ түгендеу нөмірі болуға тиіс.

Іссапарларда, сондай-ақ ұшулар мен орын ауыстырулар кезінде ноутбуктерді портфельде немесе ноутбуктерге арналған арнайы сөмкеде қол жүгі ретінде алып жүру қажет.

Компьютерлік жабдықты қатты ыстықта немесе қатты суықта қалдыруға болмайды.

5.2.3.6. Жергілікті-есептеу желісін қолдану

Ішкі және сыртқы ақпараттық ресурстармен өзара іс-қимылды және жұмысты ұйымдастыру үшін барлық жұмыс станциялары мен ОҚО ақпараттық жүйелері ЖЕЖ-ге қосылған, оны басқаруды АТҚҚЕБ жүзеге асырады.

Пайдаланушыларға жұмыс станцияларының папкалары мен дискілеріне желіге кіруге тыйым салынады.

Ортақ пайдаланылатын ресурстар мен ортақ папкаларды АТҚҚЕБ қызметкерлері ОҚО серверлерінде ғана жасайды.

Кіру рұқсат етілген жағдайларды қоспағанда, барлық пайдаланушыларға ортақ ресурсқа кіруге тыйым салынады.

Пайдаланушыларға ішкі және сыртқы желілерді сканерлеуді, желілік трафикті тыңдау және талдауды жүзеге асыратын бағдарламаларды пайдалануға тыйым салынады.

5.2.3.7. Электронды пошта және Интернет ресурстары

ОҚО-дағы электрондық пошта коммуникация, ақпаратты тарату және өндірістік мақсаттарда процестерді басқару құралы болып

табылады: ОҚО қызметкерлері еңбегінің тиімділігін арттыру және оның ресурстарын үнемдеу.

ОҚО-дағы электрондық пошта тек қана қызметтік мақсаттарда пайдалануға арналған.

Электрондық поштаны пайдалану және интернет ресурстарына кіру кезінде пайдаланушылар анық (жұмыс орны мен лауазымын көрсету арқылы) немесе анық емес (мысалы, электрондық пошта мекенжайы арқылы немесе ОҚО-ның ішкі ЖЕЖ-нен Интернетке шығу кезінде) ОҚО-мен қауымдаса алады, сондықтан осы қаражатты пайдалана отырып, олар мынадай талаптарды орындау арқылы ОҚО-ның имиджін ұстап тұруға міндетті:

- ОҚО имиджін саналы түрде құруға және қолдауға;

- электрондық хабарламаны жазуға кез келген ОҚО құжатын әзірлеу сияқты мұқият және байыптылықпен қарауға;

- электрондық пошта хабарламаларында немесе Интернетте өз пікірлерін білдіру кезінде пайдаланушылар олар білдірген пікірлер олардың жеке пікірлері екенін анық көрсетуі керек, бұл ОҚО пікірімен сәйкес келмеуі мүмкін.

- ОҚО-ның электрондық поштасын пайдаланушылардың өз лауазымдық міндеттерін орындауымен байланысты емес жеке және өзге де хат жазысу үшін пайдалануға;

- тексерілмеген көздерден электрондық пошта хабарламаларында тіркемелерді немесе сілтемелерді ашуға;

- ОҚО қаржыландырмайтын саяси қызметті немесе қайырымдылық қызметті жүзеге асыру үшін электрондық поштаны пайдалануға;

- электрондық пошта арқылы алынған бағдарламаларды ашуға немесе іске қосуға;

- шифрлау құралдарын қолданбай құпия деректерді жіберуге;

- мөлшері 30 мегабайттан асатын тіркемелері бар хабарламаларды жіберуге;

- басқа қызметкерлердің шоттарын пайдалану немесе біреудің атынан хабарлама жіберуге;

- басқа адресаттарға жіберу туралы өтініші бар «бақыт хаттарын» жіберуге тыйым салынады.

ОҚО ЖЕЖ-нен тыс жерлерде ОҚО-ға тиесілі жұмыс станцияларынан электрондық поштаға және интернет желісіне қол жеткізу ОҚО ЖЕЖ-нің ішінде электрондық пошта мен интернетті пайдалану кезінде қолданылатын ережелерді сақтай отырып жүзеге асырылады.

Қызметкерлер өз отбасы мүшелеріне немесе ОҚО қызметкері болып табылмайтын басқа да адамдарға ОҚО-ның электрондық поштасына және ақпараттық жүйелеріне рұқсат бермеуі тиіс.

ОҚО-ның электрондық поштасын пайдалана отырып берілген немесе қабылданған барлық пошта хабарламалары ОҚО-ға тиесілі және оның өндірістік процесінің ажырамас бөлігі болып табылады.

ОҚО Интернет желісіне шығудың бірыңғай қорғалған нүктесіне ие. Ақпараттық қауіпсіздік жүйелері интернет желісіндегі шабуылдардан қорғауды қамтамасыз ету, трафикті тұтынуды және байланыс арналарын пайдалануды есепке алу мен оңтайландыру, сондай-ақ пайдаланушылардың интернеттің зиянды және қауіпті ресурстарына шығуын болдырмау мақсатында ОҚО-ның ішкі ЖЕЖ-нен Интернетке қол жеткізуді бақылайды.

Пайдаланушылардың ОҚО ішкі ЖЕЖ-нен Интернетке қосымша қосылуларды ұйымдастыруына немесе интернет-трафикті бақылау жүйесін айналып өтуге және басқа да талпыныстарға тыйым салынады.

Қызметтік қажеттілік жағдайларын қоспағанда, Интернет желісінде жұмыс істеген кезде пайдаланушыларға тыйым салынады:

- нақты уақыт режимінде үлкен көлемдегі деректерді (бейнелер, музыка, суреттер) жүктеуге, сақтауға және таратуға, қарауға және тыңдауға;

- бағдарламаларды жүктеуге және іске қосуға;

- ақпаратты ашуға және қарауға, сондай-ақ ойын-сауық, діни, жала жабу, кемсітушілік, экстремистік, нәсілшіл, әдепсіз және қылмыстық сипаттағы ақпаратты сақтауға және таратуға;

- мазмұны қызметкердің лауазымдық міндеттеріне жатпайтын сайттарға кіруге;

- түрлі ойындар ойнауға және интернет-казинолар мен тотализаторларға баруға;

- интернетте ақша табу үшін бағдарламаларды пайдалануға.

Белгілі бір сайтқа кірудің техникалық мүмкіндігінің болуы пайдаланушыларға осы сайтқа кіруге рұқсат етілгенін білдірмейді.

5.2.3.8. Алып-салмалы тасымалдағыштар

ОҚО-да жұмыс станцияларында ауыстырмалы тасымалдағыштарды (USB-флэш-жинақтағыш) пайдалануға тыйым салынады.

Оларды пайдалану кезінде келесідей ақпараттық қауіпсіздік тәуекелдері бар:

- өнеркәсіптік тыңшылық қаупі;

- қорғалған ақпараты бар тасымалдағыштың кездейсоқ жоғалуы;

- тасымалдағыш вирус жұқтырған кезде ақпараттың бұрмалануы немесе жоғалуы (ішінара немесе толық);

- тасымалдағыштың істен шығуы.

Ауыстырылатын ақпарат тасымалдағыштарды пайдалану қатаң түрде АТҚҚЕБ қызметкері арқылы мынадай тәртіппен жүзеге асырылады: жұмыс станциясына қосылған кезде АТҚҚЕБ қызметкері вирусқа қарсы БҚ тасымалдаушысының ішіндегісін вирустар мен зиянды БҚ-ның бар-жоғына тексеру жүргізуге міндетті. АТҚҚЕБ қызметкерлеріне ауыстырмалы тасымалдағышты вирусқа қарсы БҚ-мен сканерлеу процесін үзуге тыйым салынады.

Ауыстырмалы тасымалдағышты жұмыс станциясына қосу алдында тасымалдағышты ондағы жарықтар мен физикалық зақымданулардың жоқтығына көзбен қарап тексеру қажет, бұл одан әрі жұмыс станциясының USB-портының істен шығуына әкелуі мүмкін.

Пайдаланушылар қорғалған ақпараты бар ауыстырмалы тасымалдағыштарды кәдеге жарату кезінде ақпараттық қауіпсіздік шараларын сақтауы қажет. Ауыстырылатын медиа физикалық түрде жойылады (жад чипі бұзылады).

Қызметкерлердің дербес деректерін беру үшін ауыстырмалы тасымалдағыштарды пайдаланған жағдайда, оларды жою үшін пайдаланушының қатысуымен тасымалдағышты жою жүргізілетін және

қажет болған жағдайда жою процесі бейнеге жазылатын АТҚҚЕБ -ға жүгіну қажет.

5.2.3.9. Әлеуметтік инженерия әдісімен шабуылдардан қорғау

Әлеуметтік инженерияның құрбаны болмау үшін келесі шараларды қабылдау қажет:

- сіз кіммен сөйлесіп жатқаныңызды білуіңіз керек. Егер сіз қоңырау шалушыны жеке білмесеңіз немесе қоңырау шалушы сенімді емес деп күдіктенсеңіз, қоңырау шалушының нөмірін анықтаңыз және оған қоңырау шалмас бұрын оның заңдылығын тексеріңіз;

- әлеуметтік инженерлік шабуылдарды электрондық пошта, веб-сайттар және жедел хабар алмасу жүйелері арқылы жүргізілуі де мүмкін. Электрондық пошта хабарында көрсетілген атау мен мекен-жай жалған болуы мүмкін. Сіз білмейтін немесе тексере алмайтын электрондық мекенжайларға ішкі немесе басқа құпия ақпаратты жібермеңіз;

- қоңырау шалушы адам сұратқан ақпараттың оған өндірістік қажеттіліктер үшін талап етілетініне көз жеткізу қажет. Қоңырау шалушыға қажет екенін анықтағанша ешқашан ішкі ақпаратты бермеңіз;

- белгісіз немесе тексерілмеген көздерден алынған сілтемелерді, файлдарды және тіркемелерді ашуға тыйым салынады;

- әлеуметтік инженерия әдісімен шабуылға күдік туындаған немесе анықталған жағдайда, инцидент туралы бақылау қызметі мен АТҚҚЕБ-не шұғыл хабарлау қажет.

5.2.3.10. Ақпараттық жүйелердің қауіпсіздігі

Қолданбалы ақпараттық жүйелер-белгілі бір қызмет саласында деректерді өңдеумен байланысты міндеттерді немесе міндеттер класын шешуге арналған бағдарламалар.

ОҚО-де пайдаланылатын қолданбалы ақпараттық жүйелер мақсатына, архитектурасына және әзірлемесіне қарамастан (бөгде ұйымдар, АТҚҚЕБ қызметкерлерінің өз күшімен) деректер базасы болып табылады.

ОҚО деректер базасын қорғау бүгінгі таңда өзекті мәселе болып табылады, өйткені ақпаратты құпияландыру мүмкіндігі дерекқордағы ақпаратты белгілі бір адамдар белгілі бір мақсаттар үшін ғана пайдаланатынына сенімді болуға мүмкіндік береді.

ОҚО – ның деректер базасын әкімшілендіру АТҚҚЕБ-ға, ал олардың ақпараттық қауіпсіздігін қамтамасыз ету АТҚҚЕБ-ға және ОҚО-ның деректер базасына қол жеткізе алатын қызметкерлерге жүктелген.

ОҚО-ның деректер базасын пайдалану кезінде ақпараттық қорғаудың негізгі тәсілдері мыналар болып табылады:

- деректер қорын пайдалану кезінде ақпараттық қауіпсіздік бойынша ішкі нормативтік құжаттарды пайдаланушылардың қатаң сақтауы;
- ОҚО қорғайтын ақпаратты ұсынатын дербес деректер мен деректерді бүркемелеу;
- домендік саясат деңгейінде қорғау;
- дерекқордың өзінде есептік жазба саясаты, құпясөздер, құқықтар мен рұқсаттар деңгейінде қорғау;
- серверге терминалды қатынау арқылы қорғау;
- файл кеңейтімдерін өзгерту;
- деректер базасының нұсқаларын өзгерту;
- кесте мәндерін шифрлау.

АТҚҚЕБ қызметкерлеріне ақпараттық жүйелердің өнімді дерекқорларына тұрақты (бақыланбайтын) қол жеткізуді орнату арқылы әзірлеушілерге мерзімсіз тұрақты авторизация параметрлерін ұсынуға тыйым салынады.

Қаржы ұйымдары мен мемлекеттік органдар (клиенттер-банк, мемлекеттік органдарға есептілікті жіберу/алу жүйелері) тегін негізде ұсынатын қолданбалы ақпараттық жүйелердің ақпараттық қауіпсіздік саясаты ақпараттық жүйелер иелерінің өздерінің ішкі құжаттарымен регламенттеледі және пайдаланушылар оны орындауға міндетті.

5.2.3.11. Ақпараттардың резервтік көшірмелері

Осы мақсаттарда ОҚО-да көшірудің екі түрі қолданылады: серверлік операциялық жүйелердің меншікті құралдарымен және арнайы БҚ құралдарымен (оның ішінде көлеңкелі көшіру үшін де).

ОҚО-ның маңызды аймақтарының резервтік көшірмесін жасау үшін Synology RS818 + NAS сервері қолданылады.

Ақпаратты резервтік көшіру құралдары мынадай талаптарға жауап береді:

- ақпаратты сақтаудың сенімділігі – сақтау жүйелерінің ақауға төзімді жабдығын пайдалану, ақпаратты қайталау және көшірмелердің біреуі жойылған жағдайда (оның ішінде ақауларға төзімділік бөлігі ретінде) жоғалған көшірмені басқасына ауыстыру арқылы қамтамасыз етіледі;

көп платформалы – гетерогенді желіде резервтік көшіру жүйесінің толық жұмыс істеуі оның серверлік бөлігінің әртүрлі операциялық орталарда жұмыс істейтінін және әртүрлі аппараттық және бағдарламалық платформалардағы клиенттерге қолдау көрсететінін болжайды;

- пайдаланудың қарапайымдылығы – автоматтандыру (мүмкіндігінше адамның қатысуын барынша азайту: пайдаланушының да, жергілікті желі әкімшісінің де);

- жылдам енгізу – бағдарламаларды оңай орнату және баптау, пайдаланушыны жылдам оқыту.

Ақпаратты резервтік көшіру жөніндегі жұмысты жүзеге асыратын АТҚҚЕБ қызметкерлеріне резервтік көшіру үшін лицензияланбаған БҚ пайдалануға тыйым салынады.

Резервтік көшіру кестесі мен тәртібі, көшірмелердің өмірлік циклі, резервтік ақпаратты сақтау орындары мен объектілері, резервтік көшіру түрлері, бақылау іс – қимылдары, резервтік көшіруге жауапты АТҚҚЕБ қызметкерлері және олардың ақпараттың толықтығы мен өзектілігі үшін жауапкершілігі жеке ішкі құжатпен-ОҚО резервтік көшіру жүйесі туралы ережесімен регламенттеледі.

5.2.3.12. Әлеуметтік желілер және мультимедиа-контент

ОҚО әлеуметтік желілерді еңбек құралы ретінде қарастырмайды және оларды қорғалған ақпаратты ықтимал қауіпті тарату құралына теңейді. Сондықтан оларға, сондай-ақ барлық интернет-алаңдарына, оларда тіркелген қолданушыларға өздері туралы ақпаратты орналастыруға және әлеуметтік байланыс орнату арқылы бір-бірімен

байланысуға мүмкіндік беретін сайттарға кіру бұғатталған. ОҚО әлеуметтік желілерін донорлықты насихаттау үшін жауапты қызметкер жүргізетін жұмыс станциясын оған қоспай ақ қоюға болады.

Мультимедиялық контент пайдаланушылардың өздерінің қызметтік міндеттерін орындауына байланысты емес, сондықтан ОҚО жергілікті-есптеу желісі барлық жұмыс станцияларында бұғатталуы керек.

6. Процестің нәтижелілігі

6.1. Процесс нәтижелілігінің критерийлері

Процесс нәтижелілігінің объективті критерийі инфрақұрылымды басқару процесінің нәтижелілік көрсеткіштеріне сәйкес дербес компьютерлердің, серверлік жабдықтардың және ОҚО-ның корпоративтік жергілікті-есептеу желісінің бүкіл паркінің үздіксіз жұмыс істеуін қамтамасыз ету, сондай-ақ ақпараттық қауіпсіздік тәуекелдерін іске асыру ықтималдығын қолайлыға дейін төмендету болып табылады.

6.2. Процесті бақылау және талдау

Ақпараттық қауіпсіздікті басқару процесі ешқашан аяқталмайды. Ақпараттық қауіпсіздіктің жеткілікті сенімді жүйесін қамтамасыз ету үшін оның параметрлерін үнемі қайта бағалау, сыртқы және ішкі ортадан туындайтын жаңа қауіптерді көрсету үшін бейімделу қажет.

Құжатталған стандартты операциялық рәсімдер жүйелі түрде, 3 (үш) жылда кемінде 1 (бір) рет, қажет болған жағдайда - жиі қайта қаралады. Осыған байланысты ақпараттық қауіпсіздікті басқару циклі келесі кезеңдерге бөлінеді:

- жоспарлау (әзірлеу) – ОҚО-ның жалпы стратегиясы мен мақсаттарына сәйкес нәтижелер алу үшін тәуекелдерді басқаруға және ақпараттық қауіпсіздікті жетілдіруге қатысты тәуекелдерді талдау, мақсаттарды, міндеттерді, процестерді, рәсімдерді, бағдарламалық-аппараттық құралдарды айқындау;

- іске асыру (енгізу және пайдалану) - бақылау тетіктерін, процестерді, рәсімдерді, бағдарламалық-аппараттық құралдарды енгізу және пайдалану;

- тексеру (мониторинг және талдау) – рәсімдерге, мақсаттарға және практикалық тәжірибеге сәйкес үдерістердің орындалу сипаттамаларын өлшеу, ақпараттық ресурстардың қорғалуына әсер ететін сыртқы және ішкі факторлардың өзгеруін талдау, талдау үшін басшылыққа есеп беру;

- түзету (сүйемелдеу және жетілдіру) - ақпараттық қауіпсіздік жүйесін үздіксіз жетілдіруді қамтамасыз ету мақсатында ақпараттық қауіпсіздіктің жай-күйін, басшылық тарапынан қойылатын талаптарды, өзге де факторларды ішкі және сыртқы тексеру нәтижелеріне негізделген түзету және алдын алу шараларын қабылдау.

6.3. Процесті жақсарту

ОҚО-да нормативтік құқықтық актілер талаптарының сақталуын, зияткерлік меншік құқықтарының сақталуын, заңмен қорғалатын дербес ақпаратты қорғауды, криптографиялық құралдарды пайдалану бойынша шектеулердің сақталуын қамтамасыз ету үшін тиісті процестер енгізілген.

Ақпараттық қауіпсіздік құралдары мен әдістерін әзірлеу және қолдану кезінде ОҚО үшінші тараптармен жасасқан шарттық міндеттемелер мен келісімшарттардың талаптары ескеріледі.

Үшінші тараптың ОҚО-ның ақпараттық ресурстарына қол жеткізуі осындай қол жеткізуді ұсыну кезінде туындауы мүмкін тәуекелдерді талдағаннан және барабар қорғау шараларын қабылдағаннан кейін ғана жүзеге асырылады. Қажет болған жағдайда (атап айтқанда, нормативтік құқықтық актілердің немесе халықаралық стандарттардың талаптары болған кезде) ОҚО контрагенттердің (тауарлар мен көрсетілетін қызметтерді ұсынушылардың) белгілі бір талаптарға сәйкестігіне тексеру жүргізеді.

Үшінші тараптар мемлекеттік құпияларға және таратылуы шектелген ақпаратқа қолданылып жүрген заңдарда белгіленген тәртіппен жіберіледі.

Осы саясаттың негізінде ақпараттық қауіпсіздікті қамтамасыз етудің нақты ережелері мен әдістерін, стандарттардың қолданылу саласындағы жеке рәсімдерді және т.б. регламенттейтін бірқатар бағыныста ішкі нормативтік құжаттар әзірленеді. Мұндай құжаттар

саясаттың талаптарын толықтыра және кеңейте алады, бірақ оған қайшы келмейді.

7. Қолданылу кезеңі, өзгерістер енгізу тәртібі және жариялау

Осы саясат ОҚО директорының бұйрығымен қолданысқа енгізіледі.

ОҚО директорының бұйрығы негізінде саясат күші жойылды деп танылады.

Саясатқа өзгерістер ОҚО директорының бұйрығымен енгізіледі.

Саясатқа өзгерістер енгізудің бастамашылары:

- ОҚО директоры;
- ОҚО директорының орынбасарлары;
- Бақылау қызметі;
- АТҚЕБ басшысы.

Осы саясатты өзектендіру бастамашылардың талап етуі, ОҚО-ға залал келтірген ақпараттық қауіпсіздікті бұзу бойынша оқиға және инцидент (инциденттер) анықталған кезде ОҚО-ның ақпараттық қауіпсіздігіне қатысты ішкі нормативтік құжаттарды (нұсқаулықтарды, СОП-тарды, ережелерді, басшылықтарды) өзгерту бойынша жүргізіледі және саясатта айқындалған қорғау шараларын ақпаратты қорғауға қойылатын нақты шарттар мен ағымдағы талаптарға сәйкес келтіру мақсаты бар.

Саясатты өзектендіруге АТҚҚЕБ басшысы жауапты болып табылады.

Саясат жалпыға қолжетімді құжат болып табылады және Саясатты бекіту және оны қолданысқа енгізу туралы бұйрық шығарылған күннен бастап бір тәулік ішінде ОҚО-ның www.ockkostanay.kz корпоративтік сайтында жарияланады.

8. Саясат талаптарының сақталуы үшін жауапкершілік

ОҚО-ның барлық қызметкерлері ақпаратты және оны өңдеу құралдарын қорғау жөніндегі саясат пен процестердің талаптарын бұзғаны және/немесе орындамағаны үшін дербес жауапты болады және барлық анықталған бұзушылықтар мен инциденттер туралы бақылау қызметіне және АТҚҚЕБ -ға дереу хабарлауға міндетті.

ҚОӘДСБ «Облыстық қан орталығы» КМК
ақпараттық қауіпсіздік саясаты

Ақпараттық ресурстармен жұмыс істеудің белгіленген қағидалары бұзылған жағдайда, ОҚО қызметкері осындай ресурстарға қол жеткізу құқығымен шектеледі, сондай-ақ Қазақстан Республикасының қолданыстағы заңнамасына сәйкес жауапкершілікке тартылады.

ОҚО-ның барлық жұмыскерлерінің лауазымдық нұсқаулықтарында ақпараттық қауіпсіздікті қамтамасыз ету және сақтау жөніндегі талаптар болуға тиіс.