БЕКІТЕМІН
«СҚО әкімдігінің денсаулық сақтау басқармасы» КММ
«Облыстық қан орталығы» ШЖҚ КМК
директоры_____ С. А.Таукелов

«Солтүстік Қазақстан облысы әкімдігінің денсаулық сақтау басқармасы» КММ «Облыстық қан орталығы» ШЖҚ КМК ақпараттық қауіпсіздік саясаты

Петропавл қ., 2024 жыл

Мазмұны

1. Мақсаты

Осы Ақпараттық қауіпсіздік саясаты (бұдан әрі - Саясат) «Солтүстік Қазақстан облысы әкімдігінің денсаулық сақтау басқармасы» КММ «Облыстық қан орталығы» ШЖҚ КМК (бұдан әрі - Кәсіпорын) қабылданатын ақпараттық қауіпсіздікті қамтамасыз ету саласындағы шаралар кешеніне қойылатын стратегиялық мақсаттарды, міндеттерді және негізгі талаптарды айқындау мақсатында әзірленді.

Ақпарат Кәсіпорынның бағалы активі болып табылады.

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

Алайда, ақпараттық ресурстарды тиісінше пайдаланбау Кәсіпорынды елеулі тәуекелдерге ұшыратуы, беделіне нұқсан келтіруі, қаржылық, материалдық немесе материалдық емес нұқсан келтіруі мүмкін.

Кәсіпорынның ақпараттық ресурстарына жіберілген барлық қызметкерлер мен басқа да адамдар ақпаратты ұқыпты және ұтымды пайдалану және осы Саясат талаптарының сақталуы үшін жауап береді.

Кәсіпорынның ақпараттық ресурстарына қол жеткізу осы Саясатпен танысқаннан және Кәсіпорын 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 ақпарат қауіпсіздігіне қатер төндіретін оқиғалардан олардың алдын алу немесе олардың зардаптарын барынша азайту арқылы залалды барынша азайту болып табылады.

Ақпараттық қауіпсіздікті қамтамасыз ету Кәсіпорынның қолда бар ақпараттық ресурстарына төнген барлық ықтимал қатерлерге байланысты тәуекелдер мен экономикалық шығындарды азайту үшін қажет.

2. Қолдану саласы

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

Осы Саясат Кәсіпорынның кез келген қызметкері мен оның ресурстарын пайдаланушыға қол жетімді құжат болып табылады және Кәсіпорын басшылығы ресми қабылдаған ақпараттық қауіпсіздікті қамтамасыз ету және мақсаттарды, процестер мен рәсімдерді жүйелендірілген 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 - қандай да бір физикалық немесе виртуалдық жүйенің сипаттамаларын сипаттайтын деректердің құрылымдалған ұйымдасқан жинағы.

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

Ақпараттық ресурстар - ақпараттық жүйелердегі құжаттар мен құжаттар массивтері.

Ақпараттық жүйелер - ақпаратты сақтауға, іздестіруге және өңдеуге арналған жүйелер және ақпаратты қамтамасыз ететін және тарататын тиісті ұйымдық ресурстар.

Жергілікті есептеу желісі (ЖЕЖ) - пайдаланушыларға компьютердің ресурстарын: бағдарламаларды, файлдарды, папкаларды, сондай-ақ шеткері құрылғыларды бірлесіп

пайдалануға мүмкіндік беретін, бір-бірімен кабельдер (UTP, FTP, STP, коаксиалды кабель, телефон желілері, радиоарналар және т.б.) арқылы қосылған дербес компьютерлердің белгілі бір санынан тұратын коммуникациялық жүйе : принтерлер, плоттерлер, дискілер, модемдер және т.б

IT мамандарының бөлімшесі - ақпараттандыру объектілерін құру, сүйемелдеу және дамыту мәселелерімен айналысатын басқа құрылымдық бөлімшелерден оқшауланған құрылымдық бөлімше немесе ақпараттық қауіпсіздікті қамтамасыз етуге жауапты белгілі бір лауазымды адам.

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

БҚ - бағдарламалық қамтамасыз ету, ақпаратты өңдеу жүйесі бағдарламаларының және осы бағдарламаларды пайдалану үшін қажетті бағдарламалық құжаттардың жиынтығы.

Стандартты БҚ - мыналарды қамтитын БҚ:

• операциялық жүйе (Microsoft Windows 8, 8.1, 10, 11 және т.б.)

кейінгі нұсқалары);

• құрылғылардың өзекті драйверлерінің жиынтығы;

• Microsoft Windows операциялық жүйелері үшін өзекті жаңартулар жиынтығы;

• кеңсе бағдарламаларының жиынтығы (Microsoft Office 2010, 2013, 2016, 2019, 2021 және одан кейінгі барлық нұсқалар);

• PDF (Adobe Reader) форматындағы электрондық жарияланымдарды қарауға арналған бағдарлама;

• өзекті антивирустық базалар жиынтығы бар антивирустық бағдарламалық қамтамасыз ету.

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

Жұмыс станциясы - бұл жергілікті есептеу желісінің құрамына қосылған компьютер.

Резервтік көшірме - деректерді зақымдалған немесе бүлінген жағдайда олардың түпнұсқалық немесе жаңа орналасқан жерінде қалпына келтіруге арналған жеткізгіште (қатты дискіде, деректерді сақтау жүйесінде, ауыспалы жеткізгіште және т.б.) деректердің көшірмесін жасау процесі.

Әлеуметтік инженерия - бұл пайдаланушылардың жәбірленушіге қажет әрекеттерді орындауы немесе пайдаланушылардан ақпарат немесе қызмет алу мақсатында пайдаланушыларды алдау немесе жаңылыстыру.

ЭМЖ - электрондық мұрағат жүйесі, электрондық құжаттарды сақтаудың сенімділігін, құпиялылығын және қол жеткізу құқықтарының аражігін ажыратуды, құжатты пайдалану тарихын қадағалауды, жылдам және ыңғайлы іздестіруді қамтамасыз ететін электрондық құжаттарды құрылымдық сақтау жүйесі.

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

4. Процестің жұмысын қамтамасыз ету

4.1. Жалпы

Ақпараттық қауіпсіздікті басқару жеке процесс және Кәсіпорынды басқарудың жалпы жүйесінің міндетті бөлігі болып табылады.

Кәсіпорын ақпараттық қауіпсіздікті қамтамасыз ету мәселелеріне ерекше назар аударады, ақпараттық қауіпсіздікті басқару жүйесін, ақпараттық қауіпсіздікке қатерлерден қорғаудың қолданылатын құралдары мен тәсілдерін үнемі жетілдіреді, сондай-ақ Кәсіпорын

қызметкерлерін ақпаратты қорғау саласындағы құзыретті жоғары деңгейде ұстап тұру үшін үздіксіз оқытуды қамтамасыз етеді.

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

Кәсіпорынның ақпараттық қауіпсіздігінің негізінде ақпараттық қауіпсіздік оқиғаларын іске асыру ықтималдығын төмендетуге бағытталған тәуекелге бағдарланған тәсіл жатыр.

Ақпараттық қауіпсіздікті қамтамасыз ету Кәсіпорынның қолда бар ақпараттық ресурстарына төнген барлық ықтимал қатерлерге байланысты тәуекелдер мен экономикалық шығындарды азайту үшін қажет. Осы мақсатта ақпараттың басты қасиеттерін қолдау қажет, атап айтқанда:

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

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

3) тұтастық - ақпараттың бұрмаланбаған түрде (оның кейбір тіркелген жай-күйіне қатысты өзгеріссіз) болуынан тұратын қасиет.

Кәсіпорында ақпараттық қауіпсіздікті қамтамасыз етудің негізгі объектілері болып мынадай элементтер танылады:

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

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

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

4) ақпараттық ресурстарды басқаруға және пайдалануға байланысты Кәсіпорынның процестері;

5) қорғалатын ақпаратты өңдеу құралдары орналасқан үй-жайлар;

6) Кәсіпорын қызметкерлерінің жұмыс үй-жайлары мен кабинеттері;

7) қорғалатын ақпаратқа рұқсаты бар Кәсіпорын қызметкерлері;

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

Қорғауға жататын ақпарат:

- қағаз тасығыштарда орналастырылады;

- электрондық түрде бар (есептеу техникасы құралдарымен өңделеді, беріледі және сақталады, техникалық құралдардың көмегімен жазылады);

- телефон, телефакс, телекс және т.б. арқылы электр сигналдары түрінде беріледі;

Кәсіпорынның ақпараттық қауіпсіздігін қамтамасыз ету жүйесін құру және оның жұмыс істеуі мынадай қағидаттарға сәйкес жүзеге асырылады:

- заңдылық - ақпараттық қауіпсіздікті қамтамасыз ету үшін қолданылатын кез келген іс-қимыл қолданыстағы заңнама негізінде жүзеге асырылады;

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

- үздіксіздік - ақпаратты қорғау жүйелерін басқару құралдарын қолдану, Кәсіпорынды ақпараттық қорғауды қамтамасыз ету жөніндегі кез келген іс-шараларды іске асыру Кәсіпорынның ағымдағы бизнес-процестерін тоқтатпай немесе тоқтатпай жүзеге асырылады;

- кешенділік - ақпараттық ресурстардың бүкіл өмірлік циклі ішінде, оларды пайдаланудың барлық технологиялық кезеңдерінде және жұмыс істеудің барлық режимдерінде қауіпсіздігін қамтамасыз ету;

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

- басымдық - ақпараттық қауіпсіздіктің нақты, сондай-ақ әлеуетті қатерлерін бағалау кезінде маңыздылық дәрежесі бойынша Кәсіпорынның барлық ақпараттық ресурстарын санаттау (ранжирлеу);

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

- техникалық құралдарды пайдалануды және ақпараттық қауіпсіздік шараларын іске асыруды кәсіби даярланған мамандар жүзеге асырады;

- хабардар болу және дербес жауапкершілік - барлық деңгейдегі басшылар мен орындаушылар ақпараттық қауіпсіздіктің барлық талаптары туралы хабардар және осы талаптардың орындалуына және ақпараттық қауіпсіздіктің белгіленген шараларының сақталуына дербес жауапты болады;

- өзара іс-қимыл және үйлестіру - ақпараттық қауіпсіздік шаралары Кәсіпорынның 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;

- расталуы - маңызды құжаттама және барлық жазбалар - ақпараттық қауіпсіздік жөніндегі талаптардың орындалуын және оны ұйымдастыру жүйесінің тиімділігін растайтын құжаттар жедел қол жеткізу және қалпына келтіру мүмкіндігімен жасалады және сақталады.

4.2. Процесс кезеңдерінің сипаттамасы

4.2.1. Әкімшілік-құқықтық және ұйымдастырушылық шаралар

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

- Қазақстан Республикасы заңнамасы талаптарының және Кәсіпорынның ішкі құжаттарының орындалуын бақылау;
- ақпараттық қауіпсіздік рәсімдерін қолдайтын қағидаларды, әдістемелер мен нұсқаулықтарды әзірлеу, енгізу және олардың орындалуын бақылау;
- Кәсіпорынның бизнес-процестерінің ақпараттық қауіпсіздік рәсімдерінің талаптарына сәйкестігін бақылау;
- Кәсіпорын қызметкерлерін ақпараттық жүйелермен және ақпараттық қауіпсіздік талаптарымен жұмыс істеуге ақпараттандыру және оқыту;
- ақпараттың рұқсатсыз таралу арналарына, осыған байланысты инциденттерге, салдарды оқшаулауға және азайтуға ден қою;
- ақпараттық қауіпсіздіктің жаңа тәуекелдерін талдау;
- төтенше жағдайлар туындаған кездегі іс-қимылдарды айқындау;
- Кәсіпорын қызметкерлерін жұмысқа қабылдау және жұмыстан шығару кезінде алдын алу шараларын жүргізу;
- Кәсіпорынның қызметкерлер мен донорлардың дербес деректерін қорғау туралы кепілдігі, ол шаралар кешенін, оның ішінде құқықтық, ұйымдастырушылық және техникалық шараларды қолдану жолымен:

1) жеке өмірге, жеке және отбасылық құпияға қол сұғылмаушылық құқықтарын іске асыру;
2) олардың тұтастығы мен сақталуын қамтамасыз ету;
3) олардың құпиялылығын сақтау;
4) оларға қол жеткізу құқығын іске асыру;
5) оларды заңсыз жинау мен өңдеуді болдырмау.

4.2.1.1. Ақпараттық қауіпсіздік инциденттері туралы хабарлау

Пайдаланушылар ықтимал инциденттерді немесе ақпараттық қауіпсіздікті бұзу әрекеттерін танып, олар туралы IT мамандарына дереу хабарлауы тиіс. Инциденттерді немесе ақпараттық қауіпсіздікті бұзу әрекеттерін дербес зерттеуге тыйым салынады және Кәсіпорынның ақпараттық қауіпсіздігіне жасалған шабуыл ретінде бағаланады.

Ақпараттық қауіпсіздік инциденттерінің белгілеріне мыналар жатады (бірақ олармен шектелмейді):

- пайдаланушының жұмыс станциясының жанында ақпаратты монитор экранынан түсіріп алу немесе ақпаратты алмалы-салмалы тасымалдағышқа көшіру ниетімен бөгде адамның ұзақ уақыт бойы болуы;
- есептік жазбаларды күтпеген жерден бұғаттау;
- тіркелгілерді күтпеген жерден бұғаттау;
- ЖЕЖ немесе ақпараттық жүйеге кіру/тіркеудің ұзақ уақыты;
- ЖЕЖ белгісіз файлдардың пайда болуы;
- құпиялылықты бұзу;
- деректердің күтілмеген бұрмалануы, ЖЕЖ немесе ақпараттық жүйелерде дұрыс емес немесе толық емес деректердің пайда болуы;
- штаттан тыс мінез-құлық немесе ЖЕЖ, оның жекелеген сегменттерінің немесе сервистерінің істен шығуы;
- штаттан тыс мінез-құлық немесе ақпараттық жүйенің істен шығуы.

4.2.1.2. Авторлық құқықтарды қорғау

Көптеген бағдарламалар, фильмдер, электрондық кітаптар, музыкалық және өзге де мультимедиялық файлдар авторлық құқық субъектілері болып табылады. Мұндай файлдарды көшіруге және таратуға тыйым салынуы мүмкін.

Авторлық құқықпен қорғалған бағдарламалар мен контентті ЖЕЖ және Жұмыс станцияларында көшіруге, таратуға, жаңғыртуға және сақтауға құқық иесінің жазбаша рұқсатымен ғана немесе бұл «заңды пайдалану» деп есептелетін басқа да жағдайларда рұқсат етіледі.

Егер пайдаланушының авторлық құқық туралы заңнаманың қолданылуына қатысты қандай да бір сұрақтары болса, олар түсіндіру үшін Кәсіпорынның заң кеңесшісіне жүгінуге тиіс.

Пайдаланушылар, егер керісінше дұрыс ақпарат болмаса, барлық бағдарламалар мен басқа да файлдар авторлық құқықтармен қорғалған деп пайымдауға тиіс.

4.2.2. Физикалық қауіпсіздік шаралары

Физикалық қауіпсіздік шаралары мыналарды қамтиды (бірақ олармен шектелмейді):

- өткізу және объекті ішіндегі режимдерді ұйымдастыру;
- қорғалатын объектілердің қауіпсіздік периметрін құру;
- күзетілетін объектілерді тәулік бойы күзетуді, оның ішінде техникалық қауіпсіздік құралдарын пайдалана отырып ұйымдастыруды;
- күзетілетін объектілердің өртке қарсы қауіпсіздігін ұйымдастыру;
- Кәсіпорын қызметкерлерінің кіруі шектеулі үй-жайларға кіруін бақылау.

ОҚО кіру шектелген үй-жайларға серверлік үй-жай және мұрағат жатады.

Серверлік үй-жайға:

- Коммуникациялық және серверлік жабдықтарға қызмет көрсету және пайдалану жөніндегі жұмыстарды орындауға арналған IT-мамандар.

Мұрағатқа:

- Кәсіпорын басшысы;
- Кәсіпорынның мұрағат қызметін білдіретін қызметкерлер.

Кіру шектелген үй-жайларға келушілерге үй-жайға қатысты шектеулердің себептері және орындалуы тиіс алдын ала ескертулер туралы нұсқау берілуі тиіс.
Серверлік үй-жай мынадай талаптарға жауап беруі тиіс:
- үй-жай бөгде адамдардың бақылаусыз кіру мүмкіндігін толық болдырмай, үнемі күзетілуі тиіс;
- оқиғаларды бейнебақылау және тіркеу жүйесінің болуы. Оқиғаларды online режимінде де, сондай-ақ кез келген мұрағаттық фрагментте де көру мүмкіндігі қамтамасыз етілуі тиіс. Мұрағаттың ұзындығы кемінде күнтізбелік 30 күнді құрауы тиіс;
- стационарлық телефонның болуы;
- автоматты газбен өрт сөндіру жүйесінің болуы;
- өрт туралы сөйлеу арқылы хабарлау жүйесінің болуы;
- «қыс-жаз» түріндегі ауаны салқындату және баптау жүйесінің болуы;
- әрбір розетка тобына кірме автоматты ажыратқышы және автоматты ажыратқышы бар энергияға тәуелсіз жүйенің болуы;
- жылу бөлу мен дренаждың арнайы жүйесінің болуы;
- қажетті жиһаз және компьютерлік техника жиынтығымен жабдықталған ЛВС әкімшісінің жұмыс орнын қолма-қол;
- кіру тек бұғаттаудың, кіру картасының, кілттің немесе үй-жайға жауапты адам беретін басқа да қауіпсіздік құралдарының көмегімен ғана мүмкін болады.

Кәсіпорын қызметкерлерінің серверлік үй-жайды алдын ала нұсқаулықсыз және Кәсіпорынның жауапты қызметкерінің міндетті түрде қатысуынсыз жинауға тыйым салынады.

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

Техникалық құралдар кешенінің (проекторлар, аудиомикшерлер, күшейткіштер, бейнеконференцбайланыс жабдықтары, микрофондар, дыбыс шығарудың стереофониялық құрылғылары) қалыпты жұмыс істеуін қамтамасыз ету IT мамандарына жүктелген.
Бейне-материалдарды (фильмдер, бейне-роликтер) көрсету үшін cIT мамандарының мынадай шарттарды алдын ала келісуі қажет:
- бейне-материалдардың форматы;
- ұзақтығы (минут);
- жаңғырту режимі;
- бейне-материал көзі;
- шығаруға жауапты пайдаланушы.

Пайдаланушыларға аудио-бейне ойнатқыштарды, сондай-ақ плагиндер мен оларға толықтыруларды өздігінен орнатуға тыйым салынады.

4.2.3. Бағдарламалық-техникалық шаралар

Бағдарламалық-техникалық шаралар мыналарды қамтиды (бірақ олармен шектелмейді):
- лицензиялық БҚ және ақпаратты қорғаудың сертификатталған құралдарын пайдалану;
- периметрді қорғау құралдарын пайдалану (Firewall, IPS және т.б.);
- вирусқа қарсы кешенді қорғауды қолдану;
- ақпараттық жүйелерге орнатылған ақпараттық қауіпсіздік құралдарын пайдалану;
- ақпаратты тұрақты резервтік көшіруді қамтамасыз ету;
- бірінші кезекте артықшылықты пайдаланушылардың құқықтары мен әрекеттерін бақылау;
- нормативтік құқықтық актілерде белгіленген тәртіппен ақпаратты криптографиялық қорғау құралдарын қолдану;
- аппараттық құралдардың тоқтаусыз жұмыс істеуін қамтамасыз ету;
- ақпараттық жүйенің сындарлы элементтерінің жай-күйіне мониторинг жүргізу.

4.2.3.1. Пайдаланушы тіркелгілері және олардың құпия сөздері

Кәсіпорынның ақпараттық ресурстарына қол жеткізу үшін әрбір пайдаланушыға бірегей (Кәсіпорынның ЖЕЖ шеңберінде) есептік жазба - дербес сәйкестендіргіш (логин) және пароль беріледі.

Есептік жазбаны IT маманы пайдаланушы мынадай құжаттардың көшірмелерін ұсынғаннан кейін ғана жасайды:

- Кәсіпорынға жұмысқа қабылдау туралы бұйрық;
- жеке басын куәландыратын құжат.

Жаңа есеп жазбасын жасаған кезде немесе егер пайдаланушы өзінің құпия сөзін ұмытып қалған жағдайда, оған уақытша құпия сөз беріледі, ол Кәсіпорынның ЖЕЖ бірінші кірген кезде ауыстырылуы тиіс.

Пайдаланушылар өз парольдерін құпия сақтауға және парольдердің күрделілігін қамтамасыз ету жөніндегі ережелерді сақтауға міндетті:

- парольдің ең аз ұзындығы - 5 символ;
- пароль оңай анықталатын бірізділікті білдірмеуі тиіс;
- пароль бірдей сандардан немесе әріптерден тұрмауы тиіс.

Құпия сөзді тұрақты түрде (60 күнде кемінде 1 рет) ауыстыру қажет.

Құпия сөзді әрбір 60 күн сайын немесе пайдаланушының құпия сөзі ашылған кезде алдыңғы бесеуімен сәйкес келмейтін жаңа құпия сөзге ауыстыру керек. Соңғы жағдайда құпия сөзді бір жұмыс күнінен кешіктірмей дереу өзгерту қажет.

Өз логині мен паролін басқа пайдаланушыларға беруге және басқа пайдаланушылардың логинімен ақпараттық жүйелерге кіруге немесе кез келген тәсілмен Кәсіпорынның ақпараттық жүйелерінде басқа тұлға ретінде көрінуге тыйым салынады.

ақпараттық жүйелерде және Интернет желісінде.

Логиндер мен парольдерді жазылған күйде оңай қол жетімді жерлерде сақтауға болмайды.

Пайдаланушы өзінің есеп жазбасының атынан жасалған барлық әрекеттер үшін жауапты болады.

Жұмыс станциясына немесе Кәсіпорынның ақпараттық жүйелеріне кірген кезде парольдерді автоматты түрде енгізуді реттеуге тыйым салынады.

Қызметкер жұмыстан босатылған және соңғысы IT мамандарына қол қойған айналым парағын ұсынған кезде, IT мамандары жұмыстан босатылған қызметкердің есептік жазбасымен мынадай іс-қимылдарды орындайды:

- пайдаланушының тіркелгісі дереу өшіріледі;
- жергілікті профильдегі ақпарат 90 күннен кейін өшіріледі.

4.2.3.2. Пайдаланушылардың жұмыс станцияларының қауіпсіздігі

Кәсіпорын қызметкерлерге өздерінің лауазымдық міндеттерін орындау үшін жұмыс станцияларын береді.

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

БҚ өз бетінше орнатуға немесе бағдарламаларды іске қосуға тыйым салынады.

Егер пайдаланушының тікелей басшысының өкімі болмаса, пайдаланушыларға басқа адамдарға (IT мамандарынан басқа) өздерінің жұмыс станцияларына кіруге рұқсат беруге тыйым салынады.

Пайдаланушылар жұмыс күнінің ішінде өз жұмыс орнынан шығып, жұмыс күнінің соңында оны өшіргенде («Ctrl + Alt + Del» пернетақтасындағы перне комбинациясы немесе Win + L) жұмыс станциясын бұғаттауы тиіс.

Құпия сөзді енгізу кезінде және құпия ақпаратпен жұмыс істеу кезінде пайдаланушылар бөтен адамдардың монитордың экранынан ақпаратты немесе енгізілетін құпия сөзді көре алмайтынына көз жеткізуі тиіс.

Пайдаланушылар әрекетсіздіктің 5 минуттан кейін автоматты түрде қосылатын экрандық сақтағыштарды пайдалануға міндетті, олардан шығу үшін пароль талап етіледі.

4.2.3.3. Вирустардан және зиянды БҚ қорғау

Кәсіпорынның ЖЕЖ вирусқа қарсы қорғау жөніндегі барлық жұмыс кешенін IT мамандары жүзеге асырады.

Жаңартылған вирусқа қарсы бағдарламалық қамтамасыз етумен қорғаусыз пайдаланушының серверін немесе жұмыс станциясын Кәсіпорынның ЖЕЖ қосуға тыйым салынады.

Өзінің дербес компьютерін немесе жұмыс станциясын Кәсіпорынның ЖЕЖ қосу қажет мердігер ұйымдар Кәсіпорын басшысының келісімімен IT мамандарының алдын ала рұқсатын алады.

Кәсіпорынның барлық жұмыс станцияларында желілік басқарылатын жүйе пайдаланылады, онда вирусқа қарсы дерекқорды жаңарту автоматты режимде жүргізіледі. Егер мұндай мүмкіндік болмаса, IT мамандары әрбір жұмыс станциясына вирусқа қарсы дерекқорды автоматты түрде жаңарта отырып, дербес вирусқа қарсы БҚ орнатады.

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

Вирус немесе зиянды бағдарлама анықталған немесе оған күдік туған жағдайда пайдаланушы жұмыс станциясындағы жұмысын дереу тоқтатуы және бұл туралы IT мамандарына хабарлауы тиіс.

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

Егер болжамды вирус немесе зиянды бағдарлама бағдарламалық қамтамасыз етуді немесе пайдаланушының ақпаратын бүлдіре/жоя бастады деген күдік болса, жұмыс станциясын дереу өшіріп, бұл туралы IT мамандарына хабарлау қажет. Пайдаланушыларға Кәсіпорынның ішінде және одан тысқары жерлерде қандай да бір нысанда зиянды немесе өзін-өзі көбейтетін кодтарды сақтауға, зерттеуге, жасауға, енгізуге және/немесе таратуға тырысуға тыйым салынады.

4.2.3.4. «Таза үстел» саясаты

«Таза үстел» саясатын қамтамасыз ету пайдаланушылардың өздеріне жүктелген.

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

Пайдаланылмайтын құжаттар, алмалы-салмалы тасығыштар және компьютерлік құралдар (әсіресе жұмыстан тыс уақытта) осы мақсаттарға сай келетін, кілтпен жабылатын шкафта және (немесе) тиісті сақталуын қамтамасыз ететін қандай да бір басқа құрылғыларда сақталады.

Кіріс және шығыс хат-хабарлары, сондай-ақ факсимильді аппараттар жалпыға бірдей қолжетімді орындарда болмауы тиіс.

Пайдаланылмайтын құпия ақпарат кілтпен жабылатын сейфтерде, атап айтқанда офисте ешкім болмаған кезде болады.

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

4.2.3.5. Физикалық қауіпсіздік

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

Жұмыстан босаған кезде пайдаланушы IT маманының тексеру парағына қол қоюға міндетті.

Қызметкерлерге өз компьютерлерін (ноутбуктер, планшетті ПК) немесе өзге де жабдықтарды Кәсіпорынның ЖЕЖ әкелуге және қосуға тыйым салынады.

Ноутбуктерді немесе басқа да ұтқыр құрылғыларды, сондай-ақ ақпарат тасығыштарды Кәсіпорынның үй-жайларынан ұтқыр құрылғылар мен ақпарат тасығыштарды беру журналында жазба болған кезде ғана шығаруға болады.

Іссапарда болған кезде, сондай-ақ ұшу және өту кезінде ноутбуктерді портфельде немесе ноутбуктерге арналған арнайы сөмкеде қол жүгі ретінде алып жүру қажет.

Компьютерлік жабдықты қатты ыстықта немесе қатты суықта қалдыруға болмайды.

4.2.3.6. ЖЕЖ пайдалану

Ішкі және сыртқы ақпараттық ресурстармен өзара іс-қимылды және жұмысты ұйымдастыру үшін Кәсіпорынның барлық жұмыс станциялары мен ақпараттық жүйелері IT маманы әкімшілендіретін ЖЕЖ қосылған.

Пайдаланушыларға жұмыс станцияларының қалталары мен дискілеріне желілік қатынауды ашуға тыйым салынады.

Ортақ пайдаланылатын ресурстар мен ортақ қалталарды тек ITмамандар Кәсіпорынның серверлерінде жасайды.

Әдепкі пайдаланушылардың барлығына ортақ ресурсқа қатынау рұқсат етілмеген.

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

4.2.3.7. Электрондық пошта және интернет ресурстары

Кәсіпорынның электрондық поштасы коммуникация, ақпаратты бөлу және өндірістік мақсаттарда процестерді басқару құралы болып табылады: Кәсіпорын қызметкерлерінің еңбек тиімділігін арттыру және оның ресурстарын үнемдеу.

Кәсіпорынның электрондық поштасы тек қана қызметтік мақсаттарда пайдалануға арналған.

Электрондық поштаны пайдалану және Интернет ресурстарына бару кезінде пайдаланушылар Кәсіпорынмен анық (жұмыс орны мен лауазымын көрсету арқылы) немесе анық емес (мысалы, электрондық поштаның мекенжайы арқылы немесе Кәсіпорынның ішкі ЛВС-нан Интернетке шығу кезінде) байланыс жасай алады, сондықтан осы құралдарды пайдалана отырып, олар мынадай талаптарды орындау жолымен Кәсіпорынның имиджін қолдауға міндетті:

- Кәсіпорынның имиджін саналы түрде құру және қолдау;
- Кәсіпорынның кез келген құжатын әзірлеудегідей мұқияттылықпен және салмақтылықпен электрондық хабарлама жазуға қатысты;
- электрондық пошта хабарламаларында немесе Интернет желісінде өз пікірін білдірген жағдайда пайдаланушылар өздері айтқан пікірлер Кәсіпорынның пікірімен сәйкес келмеуі мүмкін олардың жеке пікірлері болып табылатынын нақты көрсетуі тиіс.

Тыйым салынады:

- сервері Қазақстан Республикасының аумағынан тыс орналасқан жеке немесе өзге де поштаны пайдалану;
- пайдаланушылардың лауазымдық міндеттерін орындауына байланысты емес жеке және өзге де хат алмасу үшін кәсіпорынның электрондық поштасын пайдалану;
- тексерілмеген көздерден электрондық пошта хабарламаларында тіркемелерді немесе сілтемелерді ашыңыз;

- Кәсіпорын қаржыландырмайтын саяси қызметті немесе қайырымдылық қызметті жүзеге асыру үшін электрондық поштаны пайдалану;

- электрондық пошта арқылы алынған бағдарламаларды ашу немесе іске қосу;

- шифрлау құралдарын қолданбай құпия деректерді жіберу;

- көлемі 30 Мегабайттан асатын тіркемелері бар хабарламаларды жіберу;

- басқа қызметкерлердің есептік жазбаларын пайдалану немесе басқаның атынан хабарлама жіберу;

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

Кәсіпорынға тиесілі ЖЕЖ шегінен тыс жұмыс станцияларынан электрондық поштаға және Интернет желісіне қол жеткізу Кәсіпорынның ішкі ЖЕЖ электрондық поштаны және Интернетті пайдалану кезінде қолданылатын ережелерді сақтай отырып жүзеге асырылады.

Қызметкерлер өз отбасы мүшелеріне немесе Кәсіпорынның қызметкерлері болып табылмайтын басқа адамдарға Кәсіпорынның электрондық поштасы мен ақпараттық жүйелеріне қол жеткізуге рұқсат бермеуі тиіс.

Кәсіпорынның электрондық поштасын пайдалана отырып берілген немесе қабылданған барлық пошта хабарламалары Кәсіпорынға тиесілі және оның өндірістік процесінің ажырамас бөлігі болып табылады.

Кәсіпорынның Интернет желісіне шығудың бірыңғай қорғалған нүктесі бар. Ақпараттық қауіпсіздік жүйелері Интернет желісінен 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 Кәсіпорынның ішкі ЖЕЖ Интернетке қол жеткізуді бақылайды.

Пайдаланушылардың Кәсіпорынның ішкі ЖЕЖ Интернетке қосымша қосылулар ұйымдастыруына немесе интернет-трафикті бақылау жүйесін айналып өтуге басқа да әрекеттеріне тыйым салынады.

Қызметтік қажеттілік жағдайларын қоспағанда, Интернет желісінде жұмыс істеу кезінде пайдаланушыларға:

- деректердің үлкен көлемін (бейне, музыка, бейнелер) нақты уақыт режимінде көшіріп алу, сақтау және тарату, қарау және тыңдау;

- бағдарламаларды жүктеп алып, іске қосу;

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

- мазмұны қызметкердің лауазымдық міндеттеріне жатпайтын сайттарға кіруге;

- түрлі ойындар ойнау және интернет-казино мен тотализаторларға бару;

- Интернет желісінде ақша табу үшін бағдарламаларды пайдалану.

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

4.2.3.8. ЭЦҚ құру және пайдалану

Электрондық цифрлық қолтаңба (ЭЦҚ) – электрондық цифрлық қолтаңба құралдарымен жасалған және электрондық құжаттың дұрыстығын, оның тиесілігін және мазмұнының өзгермейтіндігін растайтын, Қазақстан Республикасының Ұлттық куәландырушы орталығы берген және электрондық құжаттың заңдылығын растайтын электрондық цифрлық нышандар жиынтығы.

Кәсіпорын өз қызметі барысында ЭЦҚ пайдаланады. ЭЦҚ қол қоюшының өз қолымен қойған қолына тең және мынадай шарттарды орындау кезінде бірдей заңдық салдарға әкеп соғады:

1) тіркеу куәлігі бар ашық кілттің көмегімен ЭЦҚ түпнұсқалығы куәландырылған;

2) электрондық құжатқа қол қойған адам ЭЦҚ-ның жабық кілтін заңды түрде иеленеді;

3) ЭЦҚ тіркеу куәлігінде көрсетілген мәліметтерге сәйкес пайдаланылады;

4) ЭЦҚ құрылды және тіркеу куәлігін Қазақстан Республикасының аккредиттелген куәландырушы орталығы немесе Қазақстан Республикасының сенім білдірілген үшінші тарапында тіркелген шетелдік куәландырушы орталық берді.

ЭЦҚ жабық кілттері оларды заңды түрде иеленетін кәсіпорын қызметкерлерінің меншігі болып табылады.

Қажет болған жағдайда кәсіпорын қызметкері өзінің лауазымдық міндеттерін орындау үшін ЭЦҚ жабық кілттерін ала алады.

Кәсіпорында ЭЦҚ құру IT мамандарына жүктелген. ЭЦҚ құрмас бұрын, IT маманы қызметкерді «Заңды тұлғаның ЭЦҚ алатын қызметкерінің міндеттемесімен» таныстыруға міндетті.

Танысқаннан кейін қызметкер келіскен кезде өз тегін, атын, әкесінің атын міндеттемеге өз қолымен енгізуге, қолын және ЭЦҚ құрылған күнін қоюға міндетті. ЭЦҚ жасалатын қызметкер жеке басын куәландыратын құжатты (паспортты немесе жеке куәлікті) ұсынуға, сондай-ақ өзімен бірге мобильді азаматтар базасында тіркелген қолданыстағы нөмірі бар ұялы телефонды алып жүруге тиіс.

ЭЦҚ жабық кілттерін басқа қызметкерлерге және/немесе үшінші тұлғаларға беруге тыйым салынады. ЭЦҚ беру кәсіпорынға материалдық та, беделді де елеулі залал келтіруі мүмкін.

ЭЦҚ үшінші тұлғаларға беру кезінде мынадай тәуекелдер бар:

1. Заңсыз тіркеу әрекеттерін жасау;
2. Кәсіпорынның ресми құжаттарын жалғау;
3. Құпия ақпаратты үшінші тұлғаларға алу және беру;
4. Қате немесе дұрыс жасалмаған құжаттарға қол қою (мысалы, салық есептілігі).
5. Жалған мәмілелер жасаңыз;
6. Сыйлықақыларды есептеңіз немесе кәсіпорын шоттарынан материалдық қаражат алыңыз.

Қызметкер жұмыстан шығарылған кезде IT маманы айналып өту парағына қол қоймас бұрын осы қызметкерде ЭЦҚ бар-жоғын тексеруге және қажет болған жағдайда ЭЦҚ кері қайтарып алу процесін бастауға міндетті.

4.2.3.9. Алынбалы тасымалдағыштар

Кәсіпорында жұмыс станцияларында алынбалы тасымалдағыштарды (USB-флэш-жинақтағышты) пайдалануға тыйым салынады.

Оларды пайдалану кезіндегі ақпараттық қауіпсіздік тәуекелдері мыналарды білдіреді:

- өнеркәсіптік тыңшылық қаупі;
- қорғалатын ақпаратты қамтитын тасығыштың кездейсоқ жоғалуы;
- вирус тасымалдағышты жұқтыру кезінде ақпараттың бұрмалануы не жоғалуы (ішінара немесе толық);
- тасымалдағыштың істен шығуы.

Алынбалы ақпарат тасымалдағыштарды пайдалану қатаң түрде IT маманы арқылы мынадай тәртіппен жүзеге асырылады: IT жұмыс станциясына қосылған кезде маман вирусқа қарсы бағдарламалық қамтамасыз етудің (БҚ) мазмұнын вирустардың және зиянды бағдарламалық қамтамасыз етудің (БҚ) болуы тұрғысынан тексеруге міндетті. IT мамандарына вирусқа қарсы бағдарламалық қамтамасыз етуді (БҚ) алынбалы тасымалдағышты сканерлеу процесін тоқтатуға тыйым салынады.

Алынбалы тасымалдағышты жұмыс станциясына қосар алдында тасымалдағышта жарықтардың және физикалық зақымданулардың болмауын көзбен шолып қарау қажет, бұл жұмыс станциясының USB-портының одан әрі істен шығуын тудыруы мүмкін.

4.2.3.10. Әлеуметтік инженерия әдісімен шабуылдардан қорғау

Әлеуметтік инженерияның құрбаны болмау үшін мынадай шаралар қабылдау қажет:

- сіз кіммен сөйлесіп отырғаныңызды білу. Егер сіз қоңырау шалушыны жеке танымасаңыз немесе қоңырау шалушы сенімді емес деп күдіктенсеңіз, қоңырау шалушының нөмірін анықтаңыз және оған қайта қоңырау шалудан бұрын оның заңдылығын тексеріңіз;
- әлеуметтік инженерия әдісімен жасалған шабуылдар электрондық пошта, веб-тораптар және жедел хабарламалар жүйесі арқылы жүргізілуі мүмкін. Электрондық пошта хабарында көрсетілген атау мен мекенжай қолдан жасалуы мүмкін. Ішкі немесе басқа құпия ақпаратты сіз білмейтін немесе тексере алмайтын электрондық мекенжайларға жібермеңіз;
- қоңырау шалушы адам сұратқан ақпараттың оған өндірістік қажеттіліктер үшін талап етілетініне көз жеткізу қажет. Қоңырау шалушы адамға қажет екенін анықтағанша, ішкі ақпаратты ешқашан бермеңіз;
- белгісіз немесе тексерілмеген көздерден алынған сілтемелерді, файлдар мен тіркемелерді ашуға тыйым салынады;
- әлеуметтік инженерия әдісімен шабуыл жасалғаны анықталған немесе күдікті жағдайда IT мамандарына оқиға туралы шұғыл хабарлау қажет.

4.2.3.11. Ақпараттық жүйелердің қауіпсіздігі

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

Кәсіпорында пайдаланылатын қолданбалы ақпараттық жүйелер мақсатына, архитектурасына және әзірлемесіне қарамастан (бөгде ұйымдар, IT мамандарының өз күштері) деректер базасы болып табылады.

Кәсіпорынның дерекқорын қорғау бүгінгі күні өзекті проблема болып табылады, өйткені ақпаратты құпияландыру қабілеті дерекқордағы ақпаратты белгілі бір мақсаттар үшін белгілі бір адамдар ғана пайдаланатынына сенімді болуға мүмкіндік береді.

Кәсіпорынның дерекқорын әкімшілендіру IT мамандарына, ал олардың ақпараттық қауіпсіздігін қамтамасыз ету Кәсіпорынның дерекқорына қолжетімділігі бар IT мамандары мен қызметкерлеріне жүктелген.

IT мамандарына ақпараттық жүйелердің өнімді дерекқорына тұрақты (бақыланбайтын) қол жеткізуді теңшеу арқылы әзірлеушілер үшін авторландырудың мерзімсіз тұрақты параметрлерін ұсынуға тыйым салынады.

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

4.2.3.12. Ақпараттың сақтық көшірмесі

Кәсіпорынның аса маңызды салаларын резервтік көшіру процесін қамтамасыз ету үшін NAS-сервер пайдаланылады.

Ақпаратты резервтік көшіру құралдары мынадай талаптарға жауап береді:

- ақпаратты сақтаудың сенімділігі - сақтау жүйелерінің істен шығуға төзімді жабдықтарын қолданумен, ақпаратты қайталаумен және көшірмелердің біреуі жойылған жағдайда жоғалған көшірмені басқасымен ауыстырумен (оның ішінде істен шығуға төзімділіктің бір бөлігі ретінде) қамтамасыз етіледі;
- пайдаланудың қарапайымдылығы - автоматтандыру (мүмкіндігінше адамның: пайдаланушының да, ЖЕЖ әкімшісінің де қатысуын барынша азайту);
- жылдам енгізу - бағдарламаларды қарапайым орнату және баптау, пайдаланушыларды жылдам оқыту.

Ақпаратты резервтік көшіру бойынша жұмыстарды жүзеге асыратын IT мамандарына резервтік көшіру үшін лицензиялық емес БҚ пайдалануға тыйым салынады.

Резервтік көшіру кестесі мен тәртібі, көшірмелердің өмірлік циклі, резервтік ақпаратты сақтау орындары мен объектілері, резервтік көшіру түрлері, бақылау іс-қимылдары, IT резервтік көшіруге жауапты мамандар және олардың ақпараттың толықтығы мен өзектілігі

үшін жауапкершілігі жеке ішкі құжатпен - Кәсіпорынның резервтік көшіру жүйесі туралы ережемен регламенттеледі.

4.2.3.13. Әлеуметтік желілер және мультимедиа-контент

Кәсіпорында әлеуметтік желілерді еңбек құралы ретінде қарамайды және оларды қорғалатын ақпаратты ықтимал қауіпті тарату құралына теңестіреді. Сондықтан оларға, сондай-ақ барлық интернет-алаңдарға, сайттарға кіруге тыйым салынған, олар тіркелген пайдаланушыларға өздері туралы ақпаратты орналастыруға және әлеуметтік байланыстар орнатып, өзара байланысуға мүмкіндік береді. Кәсіпорынның әлеуметтік желілері донорлықты танымал ету үшін жауапты қызметкермен жүргізілетін жұмыс станциясы бұған жатпайды.

Мультимедиа-контент пайдаланушылардың лауазымдық міндеттерін орындауымен байланысты емес, сондықтан Кәсіпорынның барлық ЖЕЖ жұмыс станцияларында бұғатталуы тиіс.

5. Процестің нәтижелілігі

5.1. Процестің нәтижелілік критерийлері

Инфрақұрылымды басқару процесінің нәтижелілік көрсеткіштеріне сәйкес Кәсіпорынның барлық дербес компьютерлер паркінің, серверлік жабдығының және корпоративтік жергілікті есептеу желісінің үздіксіз жұмыс істеуін қамтамасыз ету, сондай-ақ ақпараттық қауіпсіздік тәуекелдерін іске асыру ықтималдығын қолайлы деңгейге дейін төмендету процестің нәтижелілігінің объективті өлшемі болып табылады.

5.2. Процесті мониторингілеу және талдау

Ақпараттық қауіпсіздікті басқару процесі ешқашан аяқталмайды. Ақпараттық қауіпсіздіктің жеткілікті сенімді жүйесін қамтамасыз ету мақсатында оның параметрлерін ұдайы қайта бағалау, сыртқы және ішкі ортадан шығатын жаңа қауіптерді көрсету үшін бейімдеу 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 циклінің мынадай кезеңдері айқындалады:

- жоспарлау (әзірлеу) - тәуекелдерді талдау, Кәсіпорынның жалпы стратегиясы мен мақсаттарына сәйкес нәтижелер алу үшін тәуекелдерді басқаруға және ақпараттық қауіпсіздікті жетілдіруге қатысты 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) - рәсімге, мақсаттарға және практикалық тәжірибеге сәйкес процестердің орындалу сипаттамаларын өлшеу, ақпараттық ресурстардың қорғалуына әсер ететін сыртқы және ішкі факторлардың өзгеруін талдау, талдау үшін басшылыққа есептер ұсыну;
- түзету (сүйемелдеу және жетілдіру) - ақпараттық қауіпсіздік жүйесін үздіксіз жетілдіруді қамтамасыз ету мақсатында ақпараттық қауіпсіздіктің жай-күйін, басшылық тарапынан талаптарды, өзге де факторларды ішкі және сыртқы тексерулердің нәтижелеріне негізделген түзету және алдын алу шараларын қабылдау.

5.3. Процесті жақсарту

Кәсіпорында нормативтік құқықтық актілердің талаптарын сақтауды қамтамасыз ету, зияткерлік меншік құқықтарын сақтау, заңмен қорғалатын дербес ақпаратты қорғау, криптографиялық құралдарды пайдалану бойынша шектеулерді сақтау үшін тиісті процестер енгізілді.

Ақпараттық қауіпсіздік құралдары мен әдістерін әзірлеу және қолдану кезінде Кәсіпорынның үшінші тараптармен жасасқан шарттық міндеттемелері мен келісім-шарттарының талаптары ескеріледі.

Үшінші тараптың Кәсіпорынның ақпараттық ресурстарына қолжетімділігі осындай қолжетімділікті 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) Кәсіпорын контрагенттердің (тауарлар мен көрсетілетін қызметтерді берушілердің) белгілі бір талаптарға сәйкестігіне тексеру жүргізеді.

Таратылуы шектелген ақпарат пен мемлекеттік құпияларға үшінші тараптар қолданылып жүрген заңдарда белгіленген тәртіппен жіберіледі.

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

Мұндай құжаттар Саясат талаптарын толықтыруы және кеңейтуі мүмкін, бірақ онымен қайшы келе алмайды.

6. Қолданылу кезеңі, өзгерістер енгізу және жариялау тәртібі

Осы саясат Кәсіпорын басшысы бекіткеннен кейін қолданысқа енгізіледі.

Осы Саясатты өзектендіру бастамашылардың талап етуі бойынша, Кәсіпорынның ақпараттық қауіпсіздігіне қатысты ішкі нормативтік құжаттарды (нұсқаулықтарды, СОП-тарды, ережелерді, басшылықтарды) өзгерту, Кәсіпорынға залал келтірген ақпараттық қауіпсіздіктің бұзылуы бойынша оқиға болған және тосын оқиғалар (тосын оқиғалар) анықталған кезде жүргізіледі және Саясатта айқындалған қорғау шараларын нақты жағдайларға және ағымдағы ақпаратты қорғауға қойылатын талаптар.

Саясатты өзектендіруге IT мамандары жауапты болып табылады.

Саясат жалпыға қол жетімді құжат болып табылады және Кәсіпорынның корпоративтік сайтында жарияланады.

7. Саясат талаптарын сақтау үшін жауапкершілік

Кәсіпорынның барлық қызметкерлері ақпаратты және оны өңдеу құралдарын қорғау жөніндегі саясат пен процестердің талаптарын бұзғаны және/немесе орындамағаны үшін дербес жауап береді және барлық анықталған бұзушылықтар мен оқиғалар туралы IT мамандарына дереу хабарлауға міндетті.

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

Кәсіпорынның барлық қызметкерлерінің лауазымдық нұсқаулықтары ақпараттық қауіпсіздікті қамтамасыз ету және сақтау талаптарын қамтуы керек.