БЕКІТЕМІН
Қостанай облысы әкімдігінің білім басқармасының «Қостанай қаласы білім бөлімінің Абай атындағы жалпы орта мектебі» КММ директорының м.а. _____
Ж.К.Бекентаев

«31» қазан 2023 ж

13 парақта

«Қостанай қаласы білім бөлімінің Абай атындағы жалпы білім беретін мектебі» КММ ақпараттық қауіпсіздік саясаты

ӘЗІРЛЕГЕН
Қостанай облысы әкімдігінің білім басқармасының «Қостанай қаласы білім бөлімінің Абай атындағы жалпы білім беретін мектебі» КММ директордың АКТ жөніндегі орынбасары И.С. Храмей

«31» қазан 2023 ж

Қостанай қ., 2023 жыл

1. Интернет пен электрондық поштаны пайдалану ережелері

Терминдер мен анықтамалар

Бұл Ережелерде келесі негізгі ұғымдар мен терминдер пайдаланылады:

1) Электрондық ақпараттық ресурстар – ақпараттық жүйелерде қамтылған электрондық түрде сақталатын ақпарат (ақпараттық дерекқорлар);

2) Ақпараттық жүйе (бұдан әрі – АЖ) – аппараттық-бағдарламалық кешеннің көмегімен ақпаратты сақтауға, өңдеуге, іздеуге, таратуға, беруге және беруге арналған жүйе.

3) Интернет-ресурс – электрондық ақпараттық ресурс, оны жүргізу және (немесе) пайдалану технологиясы, жұмыс істейтін және ашық ақпараттық-коммуникациялық желі, сондай-ақ ақпараттық өзара іс-қимылды қамтамасыз ететін ұйымдық құрылым;

4) Интернет-провайдер - Интернетке қол жеткізу қызметтерін және Интернетке қатысты басқа қызметтерді ұсынатын ұйым;

5) Жұмыс станциясы – белгілі бір міндеттерді шешуге арналған аппараттық және бағдарламалық құралдар кешені;

6) Құпия ақпарат-Қазақстан Республикасының заңдарына немесе олардың меншік иесіне немесе иеленушісіне сәйкес Қазақстан Республикасының заңнамасында көзделген жағдайларда қолжетімділігі шектелген мемлекеттік құпияларды қамтымайтын ақпарат;

7) Электрондық пошта мониторингі – спамның алдын алу, электрондық құралдар арқылы берілуі мүмкін зиянды кодтың болуы және одан қорғау мақсатында электрондық пошта хабарламаларын (қайдан, қайдан, өлшемі) қадағалау;

8) Интернет-ресурстардың мониторингі-пайдаланушылар кіретін сайттардың тақырыбын анықтау, Интернетке кіру орнын анықтау, бұл ретте зиянды сайттарды бұғаттау мақсатында Интернет-ресурстың атауын (сайт мекенжайын) қарау ғана жүзеге асырылады;

9) Ақпараттық жүйенің мониторингі – қабылданған бақылау құралдарының тиімділігін тексеру және қол жеткізу саясаты үлгісіне сәйкестігін тексеру үшін қолданылады;

10) Электрондық поштаны тарату – бұқаралық коммуникация, топтық байланыс және жарнама құралы;

11) IT мамандары мектептің ақпараттық жүйелеріндегі күрделі ақауларды дамыту мен жоюды қамтамасыз етуге, сондай-ақ ақпараттық ресурстар мен жүйелерді техникалық қамтамасыз етуге жауапты.

Құжаттың мақсаты

1. Мектептің жұмыс станцияларында электрондық поштаны және Интернет қызметтерін пайдаланудың осы Ережелері электрондық пошта және Интернет қызметтерімен жұмыс істеу ережелерін реттейді.

2. Интернетке қол жеткізуді басқару тиімділігін, Интернет-ресурстарды

пайдалану кезінде ақпараттық қауіпсіздікті ұйымдастыру талаптарының орындалуын ақпараттық қауіпсіздікті қамтамасыз ету жөніндегі құрылымдық бөлімше бақылайды.
3. Интернетке және электрондық пошта жүйесіне кіруді ұйымдастыруға арналған аппараттық және бағдарламалық қамтамасыз ету мектепке тиесілі. Электрондық пошта жүйесі мен Интернет арқылы жасалған, жіберілген немесе алынған барлық хабарламалар, материалдар, сондай-ақ мектептің басқа да ақпараттық ресурстары мектептің меншігі болып табылады және болып қала береді және қызметкерлердің ешқайсысының жеке меншігі бола алмайды..
4. Барлық адамдарға пайдаланушылардың хабарламалары мен ақпараттарын рұқсатсыз қарауға тыйым салынады.
5. Қызметкердің ақпараттық ресурстарды пайдалануы оның осы ресурстармен қамтамасыз ету шартгарымен келісуін білдіреді.
6. Ақпараттың мазмұны мектеп басшылығының шешімі бойынша уәкілетті тұлғалардың назарына жеткізілуі мүмкін.
7. Мектептің ақпараттық қауіпсіздігіне жауапты IT мамандары зиянды интернет-ресурстарды блоктауға құқылы.
8. Сыртқы Интернет пошта ресурстарына кіруге тыйым салынады.

Ақпараттық қауіпсіздікті қамтамасыз ету

1. Электрондық пошта мен Интернет қызметтерін пайдаланған кезде мыналарға тыйым салынады:

1) ресурстарды коммерциялық кәсіпорындарды үгіт-насихат жүргізуге немесе жарнамалауға, діни немесе саяси идеяларды насихаттауға немесе қызметтік міндеттерді орындауға байланысты емес өзге де мақсаттарға пайдалануға;

2) қорлайтын немесе арандатушылық хабарламалар жасауға. Жас немесе жыныстық бағдар мәселелерін, діни немесе саяси бейімділіктерді, ұлтын немесе денсаулық жағдайын, сондай-ақ Қазақстан Республикасының заңнамасында тыйым салынған басқа да ақпаратты қорлайтын нысанда қозғайтын жыныстық қудалауды, нәсілдік қорлауды, жыныстық белгісі бойынша кемсітуді немесе басқа да түсініктемелерді қамтитын хабарламалар осындай болып саналады;

3) қызметтік іске жатпайтын графикалық, бейне, орындалатын және т. б. файлдардың, сондай-ақ мөлшері белгіленгеннен асатын файлдардың тіркемелерін пайдалануға;

4) қызметтік және/немесе құпия ақпаратқа қолжетімділігі шектеулі және/немесе таратылуы шектеулі мәліметтерді қамтитын хабарламаларды ашық (мемлекеттік шифрлау құралдарын - ақпаратты криптографиялық қорғау құралдарын (СҚА) пайдалана отырып, шифрланбаған түрде, сондай-ақ шетелдік пошта серверлерін пайдалана отырып жіберуді сұратуға;

5) жеке мақсаттарда топтық поштаны пайдалану;

6) пирамидалық хаттарды, тізбекті хаттарды, жарнамалық хабарламаларды және ресми қызметке қатысы жоқ басқа да ұқсас ақпаратты жіберу үшін ресурстарды пайдалануға;

7) зиянды файлдар мен бағдарламаларды, сондай-ақ авторлық құқықпен қорғалған бағдарламалық қамтамасыз ету мен материалдарды таратуға;

8) басқа пошталық жүйелері мен пайдаланушылардың тіркелгілерін пайдалануға; басқа пайдаланушылардың электрондық хабарламаларына қол жеткізуге (мектеп басшылығы рұқсат берген жағдайларды қоспағанда);

Интернетті пайдалану кезінде тыйым салынады:

1) қолжетімділігі шектелген және/немесе ашық түрде (мемлекеттік шифрлау құралдарын пайдалана отырып шифрланбаған – ақпаратты криптографиялық қорғау құралдары (CIPF) пайдалана отырып шифрланбаған) құпия ақпаратты қамтитын материалдарды беру және тарату мақсатында интернетті пайдалануға;

2) террористік, экстремистік, антиконституциялық және өзге де деструктивті материалдардан тұратын веб-сайттарға кіруге;

3) күмәнді және зиянды сайттарға, сондай-ақ ақпараттық функционалдық міндеттерді орындауға қатысы жоқ сайттарға кіруге;

4) зиянды файлдар мен бағдарламаларды, бағдарламалық қамтамасыз ету мен авторлық құқықпен қорғалған материалдарды, сондай-ақ барлық түрдегі мультимедиялық файлдарды жүктеп салуға (беруге);

5) Интернет чат қызметтерін пайдалануға;

6) жұмыс станцияларында интернетке кіру мүмкіндігі бар қашықтан қол жеткізу арқылы жұмыс істеуге арналған бағдарламаларды орнатуға;

7) мектептің компьютерлерін Интернет желісіне бөгде Интернет-провайдерлер арқылы қосуды жүзеге асыруға, сондай-ақ рұқсат етілмеген модемдік қосылымды пайдалануға.

2. Аутентификация процедурасын ұйымдастыру ережелері

Жалпы ережелер

Осы аутентификация рәсімін ұйымдастыру ережелері (бұдан әрі – Ережелер) пайдаланушы тіркелгілерін тіркеуге және ақпараттық жүйелерді парольмен қорғауға қойылатын талаптарды анықтайды және ақпараттық қауіпсіздікке қатерлерді жүзеге асырудан келетін залалды барынша азайтуға, сондай-ақ ақпараттық жүйедегі ақпараттың құпиялылығының, тұтастығы мен қолжетімділігінің жалпы деңгейін арттыруға арналған мектептер.

1. Осы құжатта қолданылатын терминдер келесі анықтамаларға ие:

1) ақпараттық қауіпсіздік (бұдан әрі – АҚ) – ақпараттық ресурстарды рұқсат етілмеген қол жеткізуден, қасақана немесе кездейсоқ бұрмалау мен жоюдан, физикалық жойылудан, оның ішінде техногендік әсердің салдарынан қорғауды қамтамасыз етуге бағытталған құқықтық, техникалық және ұйымдастырушылық шаралар кешені.

жасалған және табиғи әсерлер, сондай-ақ ақпараттың құпиялылығын, тұтастығын және қолжетімділігін қамтамасыз ететін мемлекеттік ақпараттық ресурстар мен жүйелердің қауіпсіздік жағдайы;

2) ақпараттық жүйе (бұдан әрі – АЖ) – ақпараттық өзара әрекеттесу арқылы белгілі бір технологиялық әрекеттерді жүзеге асыратын және нақты функционалдық міндеттерді шешуге арналған ақпараттық-коммуникациялық технологиялардың, қызмет көрсететін персоналдың және техникалық құжаттаманың ұйымдық реттелген жиынтығы.

3) Жүйелік әкімші-мектептің барлық АЖ кешенін басқаруға, сүйемелдеуге және оның үздіксіз жұмыс істеуін қамтамасыз етуге жауапты маман;

4) Мектеп АЖ пайдаланушылары – АЖ-мен жұмыс істейтін қызметкерлермектептер;

5) Ақпараттың құпиялылығы – ақпараттың тек уәкілетті тұлғаларға берілуін қамтамасыз ету;

6) Ақпараттың тұтастығы – ақпараттың жай-күйі (автоматтандырылған ақпараттық жүйенің ресурстары), онда оны (оларды) өзгерту оған құқығы бар субъектілер әдейі ғана жүзеге асырады;

7) Аутентификация – ұсынылған рұқсат тіркелгі деректерінің жүйеде іске асырылғандарға сәйкестігін анықтау арқылы қол жеткізу субъектісінің немесе объектісінің түпнұсқалығын растау;

8) Бастапқы құпия сөз – жаңа есептік жазбаны құру кезінде ОЖ, ДҚБЖ, бағдарламалық қамтамасыз ету әкімшісі белгілейтін символдар (әріптер, сандар, арнайы символдар) комбинациясы;

9) Негізгі пароль-тек жүйелік әкімшіге белгілі, есептік жазба иесінің түпнұсқалығын растау үшін пайдаланылатын таңбалардың (әріптер, сандар, арнайы таңбалар) тіркесімі;

10) Пайдаланушы туралы тіркелгі ақпараты: пайдаланушы аты, құпия сөз, ресурстарға кіру құқығы және мектепттің АЖ-де жұмыс істеу кезіндегі артықшылықтар.

Мектептің АЖ әкімшілері мен пайдаланушыларына қойылатын талаптар

1. Мектептетің АЖ әкімшілері мен пайдаланушылары міндетті:

1) Құпия сөзді есте сақтауға және оны ешбір нысанда сақтамауға немесе басқаларға бермеуге;

2) Мектептің домендік қызметінде міндетті түрде тіркелуі керек.

3) Құпия сөз жоғалған немесе бұзылған жағдайда ол дереу басшылықты бұл факті туралы хабардар етуге және құпия сөзді өзгертуге міндетті;

4) Парольді айына кемінде бір рет өзгерту қажет;

5) Құпия сөзді өзгерту кезінде 1-қосымшадағы талаптарды сақтау;

6) Құпия сөзді енгізген кезде оны бөгде адамдардың (артыңыздағы адам, тікелей көрінетін жерде немесе шағылысқан жарықта саусақтардың қозғалысын бақылайтын

адам және т.б.) және техникалық құралдардың (стационарлық және кірістірілген бейне) көру мүмкіндігін болдырмау, ұялы телефондардағы камералар және т.б.);

7) Логин мен құпия сөздің құпиялылығы мен қауіпсіздігін қамтамасыз етілуі.

Мектепттің АЖ әкімшілері мен пайдаланушыларының құқығы жоқ:

1) Біреудің есептік жазбасында жұмыс істеуге. Егер мектептің АЖ пайдаланушысының жетекшісі мектептің АЖ пайдаланушысына осындай жағдайларда жұмыс істеуді ұсынған жағдайда, мектептің АЖ пайдаланушысы басшының жазбаша нұсқауын (бұйрығын) талап етуге және мұндай нұсқауды (бұйрықты)алғанға дейін жұмысқа кіріспеуге құқылы;

2) Компьютерлік жабдықты мектептің домен қызметіне тіркемей-ақ мектептің корпоративтік желісіне қосуға.

3) Жеке құпия сөзіңізді біреуге айтуға;

4) Құпия сөздерді қағазға, файлға, электронды блокнотқа және басқа сақтау құралдарына, соның ішінде объектілерге жазуға;

5) Макростар немесе функционалдық пернелер сияқты автоматты кіру сценарийлеріне құпия сөздерді қосуға.

+

Тіркеу элементтері мен құпия сөздерге қойылатын талаптар

1. Мектептің АЖ-да жұмыс істеу үшін мектептен пайдаланушының есептік жазбасы (логин және пароль) болуы қажет.

2. Жаңа тіркелгіні жасау кезінде жүйе әкімшісі оны негізгі құпия сөзбен жасайды және пайдаланушыға уақытша құпия сөзді электрондық пошта арқылы жібереді. Жүйеге бірінші рет кірген кезде пайдаланушы уақытша құпия сөзді өзгертуі қажет Құпия сөзді таңдаған кезде «Құпия талаптары» (1-қосымша) басшылыққа алынуы керек.

3. Негізгі құпия сөздің құпиялылығын сақтау үшін иесі жеке жауап береді. Құпия сөзді басқа адамдарға, оның ішінде мектеп қызметкерлеріне ашуға, жазуға немесе электронды хабарламаларда анық мәтінмен жіберуге тыйым салынады.

4. Құпия сөз ешқашан компьютер жүйесінде қорғалмаған түрде сақталмауы керек. Иесі құпия сөздердің қауіпсіз сақталуын қамтамасыз етпей және сақтау әдісін бекітпестен жазбаларды (мысалы, қағазда, файлдарда, бағдарламалық құралда немесе портативті құрылғыда) жасаудан аулақ болуы керек.

5. Есептік жазбалардың бұғатталуын бақылауды мектеп АЖ әкімшілендіруді жүзеге асыратын басшы есептік жазбаларды тіркеу журналының жазбаларына сәйкес жүзеге асырады

6. Компьютерлерге, сондай-ақ мектептің бейтарап аппаратындағы өзге де ұйымдастыру техникасына жүйелік-техникалық қызмет көрсетуге жауапты қызметкер мектептің барлық пайдаланушыларын мектеп доменінің салынған ережелеріне сәйкес мектептің домендік қызметінде міндетті түрде тіркеуді қамтамасыз етуі тиіс.

7. Мектептің домендік қызмет саясатын мектептің ақпараттық қауіпсіздігін қамтамасыз етуге жауапты қызметкер реттейді.

Құпия сөздерді өзгерту тәртібі

1. Пайдаланушы/жүйе әкімшісі Қосымшаға сәйкес басты құпия сөзді кемінде айына бір рет өзгертуі керек.
2. Негізгі құпия сөзді тек пайдаланушы/АЖ әкімшісі жасай алады
3. Мектеп компьютерлік бағдарламалар мен үшінші тараптардың құпия сөздерді жасауына тыйым салады.
4. Пайдаланушы/жүйе әкімшісінің негізгі құпия сөзді жоспардан тыс өзгертуі ақпараттық қауіпсіздік бөліміндегі жауапты тұлғалардың өтініші бойынша кез келген уақытта жүзеге асырылуы мүмкін

Мектептің АЖ-де құпия сөздерді басқару

1. Құпия сөздер ьпайдаланушының мектептің АЖ-не қол жеткізу өкілеттігін растаудың негізгі құралы болып табылады. Мектептің АЖ сенімді құпия сөздері қамтамасыз етудің тиімді интерактивті құралын ұсынуы тиіс (1-қосымша).
2. АЖ-де құпия сөздерді басқару кезінде келесі функцияларды іске асыру қажет:

1) Жүйеге бірінші рет кіру кезінде негізгі құпия сөзді өзгерту талабы;
2) Теру қателерін жою үшін оларды растау процедурасымен құпия сөздерді таңдау және өзгерту (қажет болған жағдайда);
3) 1-қосымшаға сәйкес құпия сөздердің беріктігін тексеру;
4) Белгіленген аралықтарда құпия сөздерді міндетті түрде өзгерту,
5) Соңғы үш құпия сөзді пайдалануды жою;
6) 4 позициядан кем алдыңғы соңғы үш құпия сөзден ерекшеленетін құпия сөзді пайдалану мүмкіндігін болдырмау;
7) Құпия сөздерді шифрланған түрде сақтау;
8) Пернетақтада теру кезінде құпия сөздерді экранға шығармау керек;

Жауапкершілік

1. Қағидалардың осы ережесінің талаптарын бұзған жағдайда жүйелік әкімші Қазақстан Республикасының қолданыстағы заңнамасына сәйкес әкімшілік немесе өзге де жауапкершілікке тартылады.
2. Қызметтік құпияны білдіретін құпия ақпаратты жария еткені үшін қызметкер ҚР қолданыстағы заңнамасына және ішкі нормативтік актілерге сәйкес тәртіптік жауапкершілікке тартылады.

3. Вирусқа қарсы бақылауды ұйымдастыру ережелері

Жалпы ережелер

Бұл ережелер вирусқа қарсы бақылауды жүргізу тәртібін ұйымдастыруға және бағдарламалық және ақпараттық жүйелерді компьютерлік вирустармен жұқтыру

жағдайларының алдын алуға арналған.

Ережелер пайдаланушылардың мектептің электрондық технологияларын вирусқа қарсы қорғауды ұйымдастыру кезіндегі әрекеттерін реттейді.

Вирусқа қарсы құралдарды орнату және жаңарту

1. Мектепте қолдануға тек лицензияланған антивирустық құралдар ғана рұқсат етіледі.
2. Вирусқа қарсы құралдарды орнатуды және жаңартуды шарттық негізде ақпараттық жүйелерге сервистік қызмет көрсететін бөлімше жүзеге асырады.

Вирусқа қарсы бақылау жүргізу тәртібі

1. Компьютерлер мен жергілікті желілерге арналған жүйелік және қолданбалы бағдарламалық қамтамасыз етуді орнату (өзгерту) маманның қатысуымен ғана жүзеге асырылады.
2. Компьютерде орнатылған (өзгертілген) бағдарламалық құралда компьютерлік вирустардың жоқтығы тексеріледі. Компьютердің бағдарламалық құралын орнатқаннан (өзгерткеннен) кейін дереу бағдарламалық жасақтаманы орнатқан Қызмет көрсету ұйымының қызметкері (бұдан әрі – ҚБ) вирусқа қарсы тексеруді жүзеге асырады.
3. Телекоммуникациялық арналар арқылы берілетін кез келген ақпарат (кез келген форматтағы сынақ файлдары, деректер файлдары, орындалатын файлдар), сондай-ақ үшінші тараптар мен ұйымдардан алынатын алынбалы тасымалдағыштардан (магниттік дискілер, таспалар: CD-ROM, FlashUSB және т. б.) ақпарат міндетті антивирустық бақылауға жатадыПайдаланушы автоматтандырылған жұмыс станциясын, сондай-ақ оның барлық сыртқы құрылғыларын мақсатты пайдалануды бақылауды жүзеге асырады.
4. Пайдаланушы автоматтандырылған жұмыс орнының, сондай-ақ оның барлық сыртқы құрылғыларының мақсатты пайдаланылуын бақылауды жүзеге асырады.
5. Қорғалған компьютерлерге орнатылған барлық бағдарламалық жасақтама зиянды бағдарламаларға алдын-ала тексеріледі. Алынбалы тасығыштардағы ақпаратты бақылау оны қолданар алдында жүргізіледі.
6. Айына кемінде бір рет қорғалған компьютердің қатты дискілерінде сақталған барлық файлдарға толық тексеру жүргізіледі.
7. Қорғалған компьютердің барлық дискілері мен файлдарын кезектен тыс антивирустық бақылау орындалады:

-БҚЕ орнатқаннан немесе өзгерткеннен кейін бірден;

-дербес компьютерді жергілікті желіге қосқаннан кейін;

-зиянды бағдарламалардың болуына күдік болса (бағдарламалардың типтік емес жұмысы, графикалық және дыбыстық әсерлердің пайда болуы, деректердің бүлінуі, файлдардың болмауы, жүйелік қате туралы хабарламалардың жиі пайда болуы және т.б.).

8. Күмәнді жағдайларда зиянды бағдарламаның болуын немесе жоқтығын

анықтау үшін тексеруге техникалық қолдау көрсету мамандарын тарту қажет.
9. Пайдаланушыларға жұмыс станцияларына лицензиясыз бағдарламалық құралды орнатуға, конфигурация параметрлеріне тәуелсіз өзгертулер енгізуге, сондай-ақ антивирустық бағдарламаларды өшіруге немесе жоюға тыйым салынады.

Компьютерлік вирусты анықтау кезіндегі қызметкерлердің әрекеттері

1. Егер компьютерлік вирусқа күдік болса, мектеп қызметкері кезектен тыс антивирустық бақылауды жүзеге асырады немесе қажет болған жағдайда компьютерлік вирустың бар-жоғын анықтау үшін IT маманын тартады.
2. Компьютерлік вирус анықталған жағдайда мектеп қызметкері жұмысты тоқтата тұруға, техникалық қызмет көрсетуді жүзеге асыратын қызметкерлердің вирус жұқтырған файлдарын табу фактісі туралы хабардар етуге міндетті;

Вирусқа қарсы қорғауды ұйымдастыру кезінде бақылау

1. Мектепте антивирустық қорғауды ұйымдастыруды бақылау және оны жүргізу тәртібін белгілеу ақпараттық қауіпсіздікті қамтамасыз ететін қызметкерлерге жүктеледі (антивирустық қорғау жүйесін, адаптивті қауіпсіздікті қамтамасыз ету жүйесін әкімшілендіру және т.б.).
2. Осы нұсқаулықтың ережелерінің сақталуын кезеңді бақылау директордың АКТ жөніндегі орынбасарына жүктеледі.

Вирусқа қарсы қорғанысты ұйымдастыру

1. Пайдаланушы антивирустық дерекқорды жүйелі түрде тексеруге міндетті.
2. Антивирустық бағдарлама болмаса, ақпарат қауіпсіздігіне жауапты қызметкерлерге дереу хабарлаңыз.

4. Ақпараттық қауіпсіздік инциденттеріне және төтенше (дағдарыс) жағдайларда әрекет етудің пайдаланушы рәсімдері туралы нұсқаулар

Жалпы ережелер және негізгі ұғымдар

Бұл Нұсқаулық пайдаланушылардың АҚ инциденттеріне және штаттан тыс (дағдарыстық) жағдайларда ден қою жөніндегі іс-қимылдарының тәртібі туралы осы Нұсқаулық әртүрлі дағдарыстық жағдайлар туындаған кезде ақпараттық жүйелердің (бұдан әрі КЖ) жұмысқа қабілеттілігін сақтаудың (қолдаудың) негізгі шараларын, әдістері мен құралдарын, сондай-ақ АЖ және оның жұмысқа қабілеттілігі бұзылған жағдайда ақпаратты және оны өңдеу процестерін қалпына келтіру тәсілдері мен құралдарын айқындайды негізгі компоненттер. Сонымен қатар, ол дағдарыс жағдайында жүйенің әртүрлі санаттағы қызметкерлерінің олардың салдарын жою және келтірілген зиянды азайту жөніндегі әрекеттерін сипаттайды.

1. Ақпараттық қауіпсіздікке қауіп төндіретін АЖ-ға жағымсыз әсер ету

нәтижесінде туындайтын жағдай дағдарыс деп аталады. Дағдарыстық жағдай қаскүнемнің қасақана әрекетінен немесе пайдаланушылардың байқаусызда жасаған әрекеттерінен, апаттардан, табиғи апаттардан туындауы мүмкін.

2. Келтірілген залалдың ауырлығы мен дәрежесіне байланысты дағдарыстық жағдайлар келесі санаттарға бөлінеді:

1) қауіп төндіретін – ақпараттық жүйенің толық істен шығуына және оның функцияларын одан әрі орындауға қабілетсіздігіне, сондай-ақ аса маңызды ақпаратты жоюға, бұғаттауға, заңсыз өзгертуге немесе бүлінуге әкеп соғады.

3. Қауіпті дағдарыс жағдайларына мыналар жатады:

1) ғимараттағы электрмен жабдықтаудың бұзылуы;

2) файл алмасуға жауапты жұмыс станциясының істен шығуы (ақпараттың жоғалуымен);

3) файл алмасуға жауапты жұмыс станциясының істен шығуы (ақпаратты жоғалтпай),

4) файл алмасуға жауапты жұмыс станциясы туралы ақпаратты оның функционалдығын жоғалтпай ішінара жоғалту;

5) жергілікті желінің істен шығуы (мәліметтерді физикалық тасымалдау ортасы);

6) Елеулі-жүйенің жекелеген компоненттерінің істен шығуына (жұмыс қабілеттілігінің ішінара жоғалуына), өнімділіктің жоғалуына, сондай-ақ рұқсатсыз қол жеткізу нәтижесінде бағдарламалар мен деректердің тұтастығы мен құпиялылығының бұзылуына әкеп соғады

4. Ауыр дағдарыс жағдайларына мыналар жатады:

1) жұмыс станциясының істен шығуы (ақпараттың жоғалуымен);

2) жұмыс станциясының істен шығуы (ақпаратты жоғалтпай);

3) жұмыс станциясы туралы ақпаратты оның функционалдығын жоғалтпай ішінара жоғалту;

4) табиғи апаттар (өрт, су тасқыны, дауыл және т.б.).

5. Төтенше (дағдарыс) жағдайларда пайдалану тәртібінің толық сипаттамасы осы Қауіпсіздік саясатының 1-қосымшасында келтірілген.

6. Дағдарыс жағдайының туындауы туралы ақпарат көздері:

1) жүйенің жұмысында немесе конфигурациясында күдікті өзгерістерді немесе олардың жауапкершілік аймағында оның қауіпсіздік шараларын анықтаған пайдаланушылар;

2) дағдарыс жағдайын анықтайтын қорғаныс құралдары;

3) дағдарыстық жағдайдың туындауын немесе мүмкіндігін көрсететін жазбаларды қамтитын жүйелік журналдар.

Жалпы талаптар

1. Қауіпті немесе ауыр дағдарыстық жағдайдың туындауы нәтижесінде жұмысы бұзылған барлық пайдаланушыларға АЖ әкімшілері дереу электрондық пошта арқылы хабарлайды. АЖ жұмыс қабілеттілігінің бұзылу себептерін жою, бүлінген (жоғалған) ресурстарды қайта өңдеу және қалпына келтіру жөніндегі одан арғы іс-қимылдар жүйе персоналы мен пайдаланушыларының функционалдық міндеттерімен айқындалады.

2. Әрбір дағдарыстық жағдайды АИ талдайды. Осы талдау нәтижелері бойынша пайдаланушылардың өкілеттіктерін, ресурстарға қол жеткізу атрибуттарын өзгерту, жүйенің конфигурациясын немесе қорғаныс құралдарын баптау параметрлерін өзгерту бойынша қосымша резервтер құру және т. б. бойынша ұсыныстар әзірленеді, қажет болған жағдайда оның пайда болу себептерін тексеру, себептік залалды бағалау, кінәлілерді анықтау және тиісті шаралар қабылдау келтіріледі.

3. Күрделі және қауіпті дағдарыс жағдайы істен шыққан жабдықты жедел ауыстыруды және жөндеуді, сондай-ақ бүлінген бағдарламалар мен деректер жиынтығын резервтік көшірмелерден қалпына келтіруді талап етеді.

4. Бағдарламаларды (эталондық көшірмелерді пайдалана отырып) және деректерді (сақтандыру көшірмелерін пайдалана отырып) күрделі немесе қауіпті дағдарыстық жағдайдан жойылған немесе бүлінген жағдайда жедел қалпына келтіру көшірмелерді сақтаудың резервтік (сақтандыру) көшірмесімен және сыртқы (жүйенің негізгі компоненттеріне қатысты) көшірмелерімен қамтамасыз етіледі. Сыртқы сақтау арнайы бөлінген үй-жайларда орналасқан бөлінген қоймаларда (сейфтерде) көшірмелердің болуын білдіреді.

5. Жүйенің жұмыс қабілеттілігін және міндеттерін орындауды қамтамасыз ететін барлық бағдарламалар мен деректер (жүйелік және қолданбалы бағдарламалық қамтамасыз ету, ашық деректер және басқа да деректер жиынтығы), сондай-ақ мұрағаттар, транзакциялар журналдары, жүйелік журналдар және т. б. сақтық көшірмелеуге жатады.

6. Жүйеде қолданылатын барлық бағдарламалық құралдардың анықтамалық (тарату) көшірмелері бар.

7. Бағдарламалар мен деректердің резервтік көшірмелерін жасау, сақтау және пайдалану жөніндегі персоналдың қажетті іс-әрекеттері персоналдың тиісті санаттарының функционалдық міндеттерінде көрсетіледі, әдетте бұл жүйелік әкімшілер, автоматтандырылған жұмыс орындарының әкімшілері, АИ қызметкерлері, сондай-ақ тізілімде тіркеледі.

8. Ақпараттық жүйелердің үздіксіз жұмысын қамтамасыз ету және қалпына келтіру жөніндегі персоналдың міндеттері мен іс-әрекеттері.

9. Дағдарыс жағдайындағы қызметкерлердің әрекеттері оның ауырлығына байланысты.

10. Қауіпті немесе ауыр сыни жағдай туындаған жағдайда қызметкерлердің әрекеттері келесі кезеңдерді қамтиды:

1) жауапты қызметкерлердің жедел реакциясы;

11. Дағдарыстық (штаттан тыс) жағдайларда пайдаланушылар ішкі электрондық пошта арқылы, ауызша телефон арқылы немесе қызмет көрсететін ұйымның (бұдан әрі - ҚБ), АҚ қызметкерлерімен электрондық байланыс құралдарының көмегімен дереу хабардар етіледі.

12. Күндізгі уақытта штаттан тыс (дағдарыстық) жағдайды анықтаған пайдаланушы ақпараттық ресурстар мен жүйелерді техникалық қолдау бөлігінде ҚБ, АА қызметкерлерін хабардар етеді.

13. Тәуліктің түнгі уақытында, штаттан тыс жағдай туындаған кезде анықтаған пайдаланушы АИ қызметкеріне хабарлауға тиіс және шұғыл түрде телефон байланысы құралдарымен: осы жұмыс учаскесі үшін құрылымдық бөлімшелердің жауапты басшыларына, АИ басшылығына хабарланады. Оқиға міндетті түрде журналда оқиғаның нақты уақытын, оқиғалардың қысқаша сипаттамасын көрсете отырып, құрылымдық бөлімшелердің хабарланған басшыларының Т.А. Ә., дағдарыстық жағдайды жоюға бағытталған іс-қимылдардың сипаттамасын көрсете отырып тіркеледі.

1) жұмыс қабілеттілігін ішінара қалпына келтіру және өңдеуді қайта бастау;

2) жүйені толық қалпына келтіру және өңдеуді толық көлемде қалпына келтіру;

3) дағдарыс жағдайының туындау себептерін тергеу және кінәлілерді анықтау;

4) кейіннен осындай бұзушылық фактілерінің себептерін жою және оларға жол бермеу жөнінде шешімдер әзірлеу.

14. Дағдарыс жағдайларында жұмыстардың ұйымдастырылуын бақылауды жүзеге асырады.

Қашықтан қол жеткізуді пайдалану

Интернетке қосылған жұмыс станцияларында қашықтан қол жеткізу арқылы жұмыс істеуге арналған бағдарламаларды орнатуға тыйым салу.

Флэш-карталарды пайдалану

Қызметтік қажеттілікке байланысты Бухгалтерия қызметкерлеріне, әкімшілік құрамға, мұғалімдерге, әлеуметтік педагогтарға арналған компьютерлерде флэш-карталарды (E-token, KAZtoken, Save-Token, Usb-тасымалдағыштар) пайдалануға рұқсат беру.

1-қосымша
ұйымның Ережелеріне
аутентификация процедуралары

Құпия сөзге қойылатын талаптар

1) Құпия сөз кемінде 8 таңбадан тұруы керек;

2) Құпия сөзде бас және бас әріптердің алфавиттік таңбалары, сондай-ақ сандар болуы керек;

3) Құпия сөз қарапайым қысқартулар (мысалы, admin, system, user, sys, god), сондай-ақ жеке және басқа жалпыға қолжетімді жазбалар (мысалы, күндер, атаулар, тақырыптар) сияқты оңай анықталатын таңбалар тізбегін қамтымауы керек;

4) Құпия сөз пернетақтадағы реттілігін оңай есептеуге болатын таңбалар тобын қамтымауы керек (мысалы, !234, qWErty, qwerty123, 321369);