БЕКІТЕМІН
Қостанай облысы әкімдігі білім басқармасының «Қостанай жоғары политехникалық колледжі» КМҚК директоры
_____ К.А. Каткенов
2024 ж. «_1_» _қаңтар_

Қостанай облысы әкімдігі білім басқармасының «Қостанай жоғары политехникалық колледжі» КМҚК ақпараттық қауіпсіздік саясаты

13 парақта

ӘЗІРЛЕНДІ
Директордың АТ жөніндегі орынбасары
И.С. Храмей
Қостанай облысы әкімдігі білім басқармасының «Қостанай жоғары политехникалық колледжі» КМҚК
2024 ж. «_1_» _қаңтар_

Қостанай қ., 2024 ж.

1. Интернет пен электрондық поштаны пайдалану ережелері

Терминдер мен анықтамалар

Бұл Ережелерде келесі негізгі ұғымдар мен терминдер қолданылады:

1) Электрондық ақпараттық ресурстар – электрондық түрде сақталатын (ақпараттық деректер қоры), ақпараттық жүйелерде қамтылатын ақпарат;

2) Ақпараттық жүйе – ақпараттарды аппараттық-бағдарламалық кешенді қолдана отырып сақтауға, өңдеуге, іздеуге, таратуға, беруге және ұсынуға арналған жүйе (бұдан әрі – АЖ);

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

4) Интернет-провайдер – Интернетке қол жеткізу қызметтерін және Интернет қызметіне байланысты өзге де қызметтерді ұсынатын ұйым;

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

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 поштаның мониторингі – электрондық байланыс және одан қорғау құралдары арқылы берілуі мүмкін спамның және зиянды кодтың болуын болдырмау мақсатында электрондық хабарламаларды (қайда, қайдан, хабарламалардың мөлшері) 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 моделінің сәйкестігін тексеру үшін қолданылады;

10) Электрондық поштаны тарату – бұқаралық коммуникация, топтық қарым-қатынас және жарнама құралы;

11) IT мамандар – колледждің ақпараттық жүйелеріндегі күрделі ақауларды дамыту мен жоюды, сондай-ақ ақпараттық ресурстар мен жүйелерді техникалық қолдауды қамтамасыз етуге жауапты.

Құжаттың мақсаты

1. Колледждің жұмыс станцияларында электрондық поштаны және Интернет қызметтерін пайдалану жөніндегі осы Қағидалар электрондық поштамен және Интернет қызметімен жұмыс істеу қағидаларын регламенттейді.

2. Интернетке қол жеткізуді басқару тиімділігін, Интернет-ресурстарды пайдалануда ақпараттық қауіпсіздікті ұйымдастыруға қойылатын

талаптардың орындалуын ақпараттық қауіпсіздікті қамтамасыз ету жөніндегі құрылымдық бөлімше бақылайды.

3. Интернетке және электрондық пошта жүйесіне кіруді ұйымдастыруға арналған аппараттық және бағдарламалық қамтамасыз ету колледжге тиесілі. Электрондық пошта жүйесі мен Интернет арқылы жасалған, жіберілген немесе алынған барлық хабарламалар, материалдар, сондай-ақ колледждің басқа да ақпараттық ресурстары колледждің меншігі болып табылады және болып қала береді және қызметкерлердің ешқайсысының жеке меншігі бола алмайды.

4. Барлық тұлғарға пайдаланушылардың хабарламалары мен ақпараттарын рұқсатсыз қарауға тыйым салынады.

5. Қызметкердің ақпараттық ресурстарды пайдалануы оның осы ресурстарды беру шарттарымен келісуін білдіреді.

6. Ақпараттың мазмұны колледж басшылығының шешімі бойынша уәкілетті тұлғалардың назарына жеткізілуі мүмкін.

7. Колледждің ақпараттық қауіпсіздігіне жауапты IT мамандары Интернеттің зиянды ресурстарын бұғаттауға құқылы.

8. Сыртқы электрондық пошта Интернет-ресурстарына кіруге тыйым салынады.

Ақпараттық қауіпсіздікті қамтамасыз ету

1. Электрондық поштаны және интернет қызметтерін пайдалану кезінде мыналарға тыйым салынады:

1) ресурстарды коммерциялық кәсіпорындарды үгіт-насихаттау немесе жарнамалау, діни немесе саяси идеяларды, қызметтік міндеттерін орындаумен байланысты емес өзге де мақсаттарды насихаттау үшін пайдалануға;
2) қорлайтын немесе арандатушылық хабарламалар жасауға. Оларға жыныстық қудалау, нәсілдік қорлау, жыныстық белгісі бойынша кемсітушілік, жас немесе жыныстық бағдар мәселелерін қорлайтын нысанда қозғайтын басқа да пікірлер, діни немесе саяси бейімділіктер, ұлты немесе денсаулық жағдайы, сондай-ақ Қазақстан Республикасының заңнамасында тыйым салынған басқа да пікірлері бар хабарламалар жатады;
3) қызметтік әрекетке қатысы жоқ графикалық, бейне, орындалатын және т.б. файлдардың, сондай-ақ көлемі белгіленген шектен асатын файлдардың қосымшаларын пайдалануға;
4) ашық (мемлекеттік шифрлау құралдары арқылы шифрланбаған - ақпаратты криптографиялық қорғау құралдары (АКҚҚ) түрде, сондай-ақ шетелдік пошта серверлерін пайдалана отырып, қолжетімділігі шектеулі және/немесе таратылуы бар қызметтік және/немесе құпия ақпаратты құрайтын мәліметтерді қамтитын хабарламаларды сұратуға/жіберуге;
5) топтық таратылымды жеке мақсаттарда пайдалануға;

6) ресурстарды пирамида хаттарын, бақыт хаттарын, жарнамалық сипаттағы хабарламаларды және қызметтік әрекетке қатысы жоқ басқа да осындай ақпаратты тарату үшін пайдалануға;
7) зиянды файлдар мен бағдарламаларды, сондай-ақ авторлық құқықпен қорғалған бағдарламалық қамтамасыз ету мен материалдарды таратуға;
8) басқа пошта жүйелері мен пайдаланушылардың есептік жазбаларын пайдалануға;

басқа пайдаланушылардың электрондық хабарламаларына қол жеткізу (колледж басшылығы рұқсат берген жағдайларды қоспағанда);

Интернетті пайдалану кезінде мыналарға тыйым салынады:

1) Интернетті ашық (мемлекеттік шифрлау құралдары арқылы шифрланбаған - ақпаратты криптографиялық қорғау құралдары (АККҚ) пайдалана отырып, шифрланбаған) қолжетімділігі шектеулі және/немесе таратылуы шектеулі құпия ақпаратты қамтитын материалдарды жіберу және тарату мақсатында пайдалануға;
2) террористік, экстремистік, конституцияға қарсы және өзге де деструктивті бағыттағы материалдарды қамтитын веб-сайттарға кіруге;
3) күмәнді және зиянды сайттарға, сондай-ақ ақпараты функционалдық міндеттерін атқарумен байланысты емес сайттарға кіруге;
4) зиянды файлдар мен бағдарламаларды, бағдарламалық қамтамасыз етуді және авторлық құқықпен қорғалған материалдарды, сондай-ақ барлық түрдегі мультимедиялық файлдарды жүктеуге (жіберуге);
5) Интернет-чат қызметтерін пайдалануға;
6) жұмыс станцияларында Интернетке қолжетімділігі бар қашықтан қол жеткізу арқылы жұмыс істеуге арналған бағдарламаларды орнатуға;
7) колледж компьютерлерін Интернет желісіне бөгде Интернет-провайдерлер арқылы қосылуды, сондай-ақ рұқсат етілмеген модемдік қосылымды пайдалануға.

2. Аутентификация рәсімін ұйымдастыру қағидалары

Жалпы ережелер

Осы Аутентификация рәсімін ұйымдастыру қағидалары (бұдан әрі – Қағидалар) пайдаланушы тіркелгілерін тіркеуге және ақпараттық жүйелерді парольмен қорғауға қойылатын талаптарды айқындайды және ақпараттық қауіпсіздік қатерлерін жүзеге асырудан келетін залалды барынша азайтуға, сондай-ақ ақпараттық қауіпсіздікке қатер төндіруді арттыруға арналған. колледждің АЖ-дағы құпиялылық, тұтастық және ақпараттың қолжетімділігінің жалпы деңгейі.

1. Осы құжатта қолданылатын терминдер келесі анықтамаларға ие:

1) Ақпараттық қауіпсіздік (бұдан әрі – АЖ) – ақпараттық ресурстарды рұқсат етілмеген қол жеткізуден, қасақана немесе кездейсоқ бұрмалау мен жоюдан, физикалық жойылудан, оның ішінде техногендік және табиғи әсердің салдарынан қорғауды қамтамасыз етуге бағытталған

құқықтық, техникалық және ұйымдастырушылық шаралар кешені. ықпал ету, сондай-ақ ақпараттың құпиялылығын, тұтастығын және қолжетімділігін қамтамасыз ететін мемлекеттік ақпараттық ресурстар мен жүйелердің қауіпсіздігінің жай-күйі;

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 әкімшісі – колледждің АЖ кешенін басқаруға, техникалық қызмет көрсетуге және үздіксіз жұмыс істеуін қамтамасыз етуге жауапты маман;
4) Колледждің АЖ пайдаланушылары – колледждің АЖ-мен жұмыс істейтін қызметкерлер;
5) Ақпараттың құпиялылығы – ақпараттың тек уәкілетті тұлғаларға берілуін қамтамасыз ету;
6) Ақпараттың тұтастығы – оны (оларды) өзгертуді оған құқығы бар субъектілер әдейі ғана жүзеге асыратын ақпараттың жай-күйі (автоматтандырылған ақпараттық жүйенің ресурстары);
7) Аутентификация – ұсынылған рұқсат деректемелерінің жүйеде іске асырылғандарға сәйкестігін анықтау арқылы қол жеткізу субъектісінің немесе объектісінің түпнұсқалығын растау;
8) Бастапқы құпиясөз – жаңа есептік жазбаны құру кезінде ОЖ, ДББЖ, қолданбалы бағдарламалық қамтамасыз ету әкімшісі белгілейтін символдар (әріптер, сандар, арнайы символдар) комбинациясы;
9) Негізгі құпиясөз – тек жүйелік әкімшіге белгілі, пайдаланушы тіркелгінің растау үшін пайдаланылатын таңбалардың (әріптер, сандар, арнайы таңбалар) комбинациясы;
10) Пайдаланушы туралы тіркеулік жазба: пайдаланушы аты, пароль, ресурстарға кіру құқығы және колледждің АЖ-де жұмыс істеу кезіндегі артықшылықтар.

Колледж АЖ әкімшілеріне және пайдаланушыларына қойылатын талаптар

1. Колледж АЖ әкімшілері мен пайдаланушылары мыналарға міндетті:

1) Құпия сөзді есте сақтау және ешбір түрде сақтамай, басқа адамдарға бермеуге;
2) Колледждің домендік қызметінде тіркелуге;
3) Құпия сөз жоғалған немесе бұзылған жағдайда, осы факт туралы тікелей басшылықты дереу хабардар етуге және құпиясөзді ауыстыруға;
4) Айына кемінде бір рет құпиясөзді ауыстыруға;
5) Құпия сөзді ауыстырған кезде 1-қосымшаға сәйкес талаптарды сақтауға;
6) Құпия сөзді енгізген кезде оның рұқсат етілмеген адамдардың (артыңыздағы адам, тікелей көрінетін жерде немесе шағылысқан жарықта

саусақтардың қозғалысын бақылайтын адам және т.б.) және техникалық құралдардың (стационарлық және кірістірілген бейне, ұялы телефондардағы камералар және т.б.) көру мүмкіндігін болдырмауға;
7) Логин мен парольдің құпиялылығы мен қауіпсіздігін қамтамасыз етуге.

Колледж АЖ әкімшілері мен пайдаланушылары мыналарға құқығы жоқ:

1) Басқа біреудің тіркеулік жазбасы арқылы жұмыс істеуге. Егер Басқарманың АЖ пайдаланушысы Басқарманың АЖ пайдаланушысына осындай жағдайларда жұмыс істеуді ұсынса, Басқарманың АЖ пайдаланушысы басшыдан жазбаша нұсқауды (өкімді) талап етуге және мұндай нұсқама (өкім) алынғанға дейін жұмысқа кіріспеуге құқылы;
2) Есептеу техникасы құралдарын колледждің домендік қызметінде тіркеусіз колледждің корпоративтік желісіне қосуға;
3) Жеке құпия сөзді басқа біреуге хабарлау;
4) Құпия сөздерді қағазға, файлға, электронды блокнотқа және басқа сақтау құралдарына, соның ішінде бір заттарға жазуға;
5) Құпия сөздерді автоматты кіру сценарийлеріне, мысалы, макростарға немесе функционалдық пернелерге қосуға.

Тіркеу элементтері мен парольдерге қойылатын талаптар

1. Колледж АЖ-да жұмыс істеу үшін колледж АЖ пайдаланушысының тіркеулік жазбасы (логин және пароль) болуы қажет.
2. Жаңа тіркеулік жазбаны жасау кезінде жүйе әкімшісі оны бастапқы парольмен жасайды және пайдаланушыға электрондық пошта арқылы уақытша пароль идентификаторы туралы хабарлайды. Жүйеге алғаш кірген кезде пайдаланушы уақытша парольді өзгертуге міндетті, парольді таңдағанда «Парольдерге қойылатын талаптар» (1-қосымша) басшылыққа алынуы қажет.
3. Негізгі парольдің құпиялылығын сақтау үшін иесі дербес жауапкершілік алады. Құпия сөзді басқа адамдарға, соның ішінде колледж қызметкерлеріне хабарлауға, оны жазуға, сондай-ақ электрондық хабарламаларда ашық мәтінмен жіберуге тыйым салынады.
4. Құпия сөзді ешқашан компьютерлік жүйеде қорғалмаған түрде сақтауға болмайды. Иесі парольдердің жазбаларын (мысалы, қағазда, файлдарда, бағдарламалық жасақтамада немесе портативті құрылғыда) қауіпсіз сақтауға кепілдік бермей және сақтау әдісін мақұлдамай жасаудан аулақ болу қажет.
5. Тіркеулік жазбаларды тіркеу журналының жазбаларына сәйкес, тіркеулік жазбалардың бұғатталуын бақылауды колледж АЖ әкімшілігіне жауапты тұлға жүзеге асырады.
6. Колледж доменінің құрастырылған ережелеріне сәйкес, колледждің бейтарап аппаратында компьютерлерге, сондай-ақ өзге де ұйымдастыру техникаларына жүйелік-техникалық қызмет көрсетуге жауапты

қызметкер, колледждің барлық пайдаланушыларын колледждің домендік қызметіне міндетті түрде тіркеуді қамтамасыз етуі қажет.
7. Колледждің домендік қызмет саясатын колледждің ақпараттық қауіпсіздігін қамтамасыз ету жөніндегі жауапты қызметкер реттейді.

Құпия сөзді ауыстыру тәртібі

1. Пайдаланушы/жүйе әкімшісі негізгі құпия сөзді қосымшаға сәйкес айына кемінде бір рет өзгертуі қажет.
2. Негізгі құпия сөзді тек пайдаланушының өзі/әкімші АЖ жасай алады.
3. Колледж компьютерлік бағдарламалар мен үшінші тараптардың құпия сөздерді жасауына тыйым салады.
4. Пайдаланушы/жүйе әкімшісі негізгі құпия сөзді жоспардан тыс ауыстыруды АҚ-дағы жауапты тұлғалардың талабы бойынша кез келген уақытта жүргізе алады.

Колледж АЖ-да құпия сөздерді басқару

1. құпия сөздер пайдаланушының колледж АЖ-не қол жеткізу өкілеттігін растаудың негізгі құралы болып табылады. Колледж АЖ сенімді құпия сөздерді қамтамасыз етудің тиімді интерактивті құралын ұсынуы тиіс (1-қосымша).
2. Құпия сөздерді басқару кезінде АЖ келесі функционалдылықты іске асыруы қажет:
    1) жүйеге алғаш кірген кезде бастапқы құпия сөзді өзгерту талабы;
    2) теру кезінде қателерді болдырмау үшін оларды растау рәсімімен құпия сөздерді таңдау және өзгерту (қажет болған жағдайда);
    3) 1-қосымшаға сәйкес құпия сөздердің сенімділігін тексеру;
    4) берілген кезеңділікпен құпия сөздерді міндетті түрде ауыстыру,
    5) соңғы үш құпия сөзді пайдалануды болдырмау;

Жауапкершілік

1. Қағидалардың осы ережесінің талаптары бұзылған 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. Антивирустық бақылауды ұйымдастыру ережелері

Жалпы ережелер

Осы ереже вирусқа қарсы бақылауды жүргізу тәртібін ұйымдастыруға және бағдарламалық қамтамасыз ету мен ақпараттық жүйелерді компьютерлік вирустармен жұқтыру фактілерінің туындауын болдырмауға арналған.

Ережелер колледждің электрондық технологияларын вирусқа қарсы

қорғауды ұйымдастыру кезіндегі пайдаланушылардың әрекеттерін реттейді.

Антивирустық құралдарды орнату және жаңарту

1. Колледжде қолдануға тек лицензияланған антивирустық құралдар ғана рұқсат етіледі.
2. Вирусқа қарсы құралдарды орнатуды және жаңартуды шарттық қатынастарда ақпараттық жүйелерге сервистік қызмет көрсетуді жүзеге асыратын бөлімше жүзеге асырады.

Антивирустық құралдарды орнату және жаңарту

1. Колледжде қолдануға тек лицензияланған антивирустық құралдар ғана рұқсат етіледі.
2. Вирусқа қарсы құралдарды орнатуды және жаңартуды шарттық қатынастарда ақпараттық жүйелерге сервистік қызмет көрсетуді жүзеге асыратын бөлімше жүзеге асырады.

Вирусқа қарсы бақылау жүргізу тәртібі

1. Компьютерлер мен жергілікті есептеу желісін жүйелік және қолданбалы қамтамасыз етуді орнату (өзгерту) маманның қатысуымен ғана жүзеге асырылады.
2. Компьютерге орнатылатын (өзгертілетін) бағдарламалық қамтамасыз ету компьютерлік вирустардың жоқтығына тексеріледі. Компьютердің бағдарламалық жасақтамасын орнатқаннан (өзгерткеннен) кейін бағдарламалық қамтамасыз етуді орнатқан Қызмет көрсету ұйымының (бұдан әрі – ҚҰ) қызметкері вирусқа қарсы тексеруді орындайды.
3. Телекоммуникациялық арналар арқылы алынатын және берілетін кез келген ақпарат (кез келген форматтағы сынақ файлдары, деректер файлдары, орындалатын файлдар), сондай-ақ үшінші тараптар мен ұйымдардан алынатын алынбалы тасығыштардан (магниттік дискілер, таспалар: CD-ROM, FlashUSB және т.б.) ақпарат міндетті антивирустық бақылауға жатады.
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 қатқыл дискілерінде сақталған барлық файлдарға толық тексеру жүргізіледі.
7. Қорғалған компьютердің барлық дискілері мен файлдарын кезектен тыс антивирустық бақылау:
   - БЖ-ны орнатқаннан немесе өзгерткеннен кейін бірден орындалады;
   - 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 бағдарламалардың болу немесе болмау фактісін анықтау үшін тексеруге техникалық қолдау мамандарын тарту қажет.

9. Пайдаланушыларға жұмыс станцияларына лицензияланбаған бағдарламалық жасақтаманы орнатуға, конфигурация параметрлеріне өз бетінше өзгерістер енгізуге, сондай-ақ антивирустық бағдарламаларды өшіруге, жоюға тыйым салынады.

Компьютерлік вирус анықталған кездегі қызметкерлердің әрекеттері

1. Компьютерлік вирустың болуына күдік туындаған кезде колледж қызметкері кезектен тыс антивирустық бақылау жүргізеді немесе қажет болған жағдайда компьютерлік вирустың болуы немесе болмауы фактісін анықтау үшін it-маманды тартады;

2. Компьютерлік вирус анықталған жағдайда колледж қызметкері жұмысты тоқтата тұрып, вирус жұқтырған файлдардың табылғаны туралы техникалық қызмет көрсетуді жүзеге асыратын қызметкерлерді хабардар етуге міндетті.

Антивирустық қорғауды ұйымдастыру кезіндегі бақылау

1. Колледжде 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 мерзімді бақылау директордың АКТ жөніндегі орынбасарына жүктеледі.

Антивирустық қорғауды ұйымдастыру

1. Пайдаланушы антивирустық базаны үнемі тексеріп отыруы міндетті.

2. Антивирустық бағдарлама болмаған жағдайда ақпараттық қауіпсіздікке жауапты қызметкерлерге дереу хабарлау тиіс.

4. Пайдаланушылардың АҚ инциденттеріне және штаттан тыс (дағдарыстық) жағдайларда әрекет ету жөніндегі іс-қимыл тәртібі туралы нұсқаулар

Жалпы ережелер мен негізгі ұғымдар

АҚ инциденттеріне және штаттан тыс (дағдарыстық) жағдайларда әрекет ету бойынша пайдаланушылардың іс-қимыл тәртібі туралы осы Нұсқаулық әр түрлі дағдарыстық жағдайлар туындаған кезде ақпараттық жүйелердің (бұдан әрі - АЖ) жұмыс қабілеттілігін сақтаудың (қолдаудың) негізгі шараларын, әдістері мен құралдарын, сондай-ақ АЖ және оның негізгі компоненттерінің жұмыс қабілеттілігі бұзылған жағдайда ақпаратты және оны өңдеу процестерін қалпына келтіру тәсілдері мен құралдарын

айқындайды. Сонымен қатар, ол дағдарыс жағдайында жүйенің әртүрлі санаттағы қызметкерлерінің олардың салдарын жою және келтірілген зиянды азайту жөніндегі әрекеттерін сипаттайды.

1. Ақпараттық жүйеге жағымсыз әсер ету нәтижесінде туындайтын, ақпараттық қауіпсіздікке қауіп төндіретін жағдай дағдарыс деп аталады. Дағдарыстық жағдай қасқүнемнің қасақана әрекетінен немесе пайдаланушылардың байқаусызда жасаған әрекеттерінен, апаттардан, дүлей апаттардан туындауы мүмкін.
2. Келтірілген залалдың ауырлығы мен мөлшері бойынша дағдарыстық жағдайлар келесі санаттарға бөлінеді:
    1) қауіп төндіретін - АЖ-ның толық істен шығуына және одан әрі өз функцияларын орындай алмауына, сондай-ақ аса маңызды ақпаратты жоюға, бұғаттауға, заңсыз түрлендіруге немесе компаға келтіруге әкеп соғады.
3. Қауіпті дағдарыстық жағдайларға мыналар жатады:
    1) ғимаратта электр энергиясын беруді бұзу;
    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 станциясында оның жұмыс қабілеттілігін жоғалтпай ақпараттың ішінара жоғалуы;
    5) жергілікті желінің істен шығуы (мәліметтерді физикалық тасымалдау ортасы);
    6) күрделі жағдай-жүйенің жекелеген компоненттерінің істен шығуына (жұмыс қабілеттілігінің ішінара жоғалуына), өнімділіктің жоғалуына, сондай-ақ рұқсатсыз қол жеткізу нәтижесінде бағдарламалар мен деректердің тұтастығы мен құпиялылығының бұзылуына әкелетін жағдай.
4. Ауыр дағдарыстық жағдайларға мыналар жатады:
    1) жұмыс станциясының істен шығуы (ақпараттың жоғалуымен);
    2) жұмыс станциясының істен шығуы (ақпаратты жоғалтпай);
    3) жұмыс станциясында оның жұмыс қабілеттілігін жоғалтпай ақпараттың ішінара жоғалуы;
    4) табиғи апаттар (өрт, су тасқыны, дауыл және т.б.).
5. Штаттан тыс (дағдарыстық) жағдайларда пайдаланушылардың іс-қимыл тәртібі туралы толық сипаттама осы Қауіпсіздік саясатының 1-қосымшасында орналасқан.
6. Дағдарыс жағдайының пайда болуы туралы ақпарат көздері:
    1) өз жауапкершілігі аймағында жүйенің жұмысында немесе конфигурациясында немесе оның қауіпсіздік шараларында күдікті өзгерістерді анықтаған пайдаланушылар;
    2) дағдарыстық жағдайды анықтаған қорғаныс құралдары;
    3) дағдарыс жағдайының туындағанын немесе туындау мүмкіндігін куәландыратын жазбалары бар жүйелік журналдар.

Жалпы талаптар

1. Қауіпті немесе ауыр дағдарыс жағдайының нәтижесінде жұмысы бұзылған барлық пайдаланушылар, АЖ әкімшілерімен дереу электрондық пошта арқылы хабардар етіледі. АЖ жұмыс қабілеттілігінің бұзылу себептерін жою, бүлінген (жоғалған) ресурстарды қайта өңдеу және қалпына келтіру жөніндегі одан әрі іс-қимылдар жүйе персоналы мен пайдаланушыларының функционалдық міндеттерімен айқындалады.
2. Әрбір дағдарыстық жағдайды АБ талдайды. Осы талдаудың нәтижелері бойынша пайдаланушылардың өкілеттіктерін, ресурстарға қол жеткізу атрибуттарын өзгерту, жүйенің конфигурациясын немесе қорғаныс құралдарын теңшеу параметрлерін өзгерту үшін қосымша резервтер құру және т. б. бойынша ұсыныстар жасалады, қажет болған жағдайда оның пайда болу себептерін тексеру, келтірілген залалды бағалау, кінәлілерді анықтау және тиісті шаралар қабылдау жүргізіледі.
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) жедел қалпына келтіру, олар елеулі немесе қауіпті дағдарыстық жағдайдан жойылған немесе бүлінген жағдайда, көшірмелерді сақтаудың резервтік (сақтандыру) көшірмесімен және сыртқы (жүйенің негізгі компоненттеріне қатысты) көшірмелерімен қамтамасыз етіледі. Арнайы бөлінген үй-жайларда орналасқан сыртқы қойма көшірмелерді арнайы сақтау орындарында (сейфтерде) орналастыруды 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, АБ 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 - ҚҰ), АБ қызметкерлерімен электрондық байланыс құралдарының көмегімен дереу хабардар етіледі.
12. Күндізгі уақытта штаттан тыс (дағдарыстық) жағдайды анықтаған пайдаланушы ақпараттық ресурстар мен жүйелерді техникалық қолдау бөлігінде ҚҰ, ЖӘ қызметкерлерін хабардар етеді.
13. Тәуліктің түнгі уақытында, штаттан тыс жағдай туындаған кезде, анықтаған пайдаланушы АБ қызметкеріне хабарлауға тиіс және шұғыл түрде телефон байланысы құралдарымен: осы жұмыс учаскесі жөніндегі құрылымдық бөлімшелердің жауапты басшыларына, АБ басшылығына хабардар етіледі. 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) бұзушылықтардың себептерін жою және кейіннен осындай фактілерге жол бермеу жөнінде шешімдер әзірлеу.

14. Дағдарыс жағдайларында жұмыстардың ұйымдастырылуын бақылауды АБ 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 құрамына, мұғалімдерге, әлеуметтік педагогтарға арналған компьютерлерде *флэш-карталарды (E-token, KAZtoken, Save-Token, Usb-тасымалдағыштар)* пайдалануға рұқсат беру.

Аутентификация рәсімін
ұйымдастыру қағидаларына
1-қосымша

Құпия сөздерге (пароль) қойылатын талаптар

1) Құпия сөзде кемінде 8 таңба болуы керек;
2) Құпия сөзде бас және үлкен 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, аттар, атаулар) сияқты оңай анықталатын таңбалар тізбегін қамтымауы керек;
4) Құпия сөз пернетақтада орналасу реттілігі оңай есептелетін таңбалар тобын қамтымауы керек (мысалы 1234, qWErty, qwerty123, 321369).