Бекітемін: _____

Қостанай облысы әкімдігі білім басқармасының «Ы.Алтынсарин атындағы мамандандырылған мектеп-гимназия-интернаты» КММ директоры Ы.С.Келинбердиева

«31» тамыз 2023 ж.

Қостанай облысы әкімдігі білім басқармасының «Ы.Алтынсарин атындағы мамандандырылған мектеп-гимназия-интернаты» КММ

АҚПАРАТТЫҚ ҚАУІПСІЗДІК САЯСАТЫ

Қостанай қаласы, 2023-2024 оқу жылы

1. Интернет және электрондық поштаны пайдалану ережелері

Терминдер мен анықтамалар

Осы Қағидаларда мынадай негізгі ұғымдар мен терминдер пайдаланылады:

1) Электрондық ақпараттық ресурстар - ақпараттық жүйелерде қамтылған, электрондық түрде сақталатын ақпарат (ақпараттық деректер базасы);

2) Ақпараттық жүйе (бұдан әрі - АЖ) - аппараттық-бағдарламалық кешенді қолдана отырып, ақпаратты сақтауға, өңдеуге, іздеуге, таратуға, беруге және ұсынуға 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 Интернет қызметіне байланысты өзге де қызметтерді ұсынатын ұйым;

5) Жұмыс станциясы - міндеттердің белгілі бір шеңберін шешуге арналған аппараттық және бағдарламалық құралдар кешені;

6) Құпия ақпарат - Қазақстан Республикасының заңдарында көзделген жағдайларда 6Қазақстан Республикасының заңдарына сәйкес қол жеткізілуі шектелген, мемлекеттік құпияларды қамтымайтын ақпарат немесе олардың меншік иесі немесе иеленушісі;

7) Электрондық пошта мониторингі - спамның алдын алу, электрондық байланыс құралдарының көмегімен берілуі мүмкін зиянды кодтың болуы және одан қорғану мақсатында электрондық хабарламаларды (қайда, қайдан, хабарламалар мөлшері) қадағалау;

8) Интернет-ресурстардың мониторингі - пайдаланушылар кіретін сайттардың тақырыптарын 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) Ақпараттық жүйелеріндегі күрделі ақауларды дамытуды және жоюды, сондай-ақ ақпараттық ресурстар мен жүйелерді техникалық қолдауды қамтамасыз етуге жауапты қызметкерлер.

Құжаттарды тағайындау

1. Жұмыс станцияларында электрондық поштаны және Интернет қызметтерін пайдалану жөніндегі ережелер электрондық поштамен және Интернет қызметімен жұмыс істеу ережелерін реттейді.

2. Интернетке қол жеткізуді басқарудың тиімділігін, Интернет-ресурстарды пайдалануда ақпараттық қауіпсіздікті ұйымдастыруға қойылатын талаптардың орындалуын ақпараттық қауіпсіздікті қамтамасыз ету жөніндегі құрылымдық бөлімше бақылайды.

3. Интернет желісіне және электрондық пошта жүйесіне қол жеткізуді ұйымдастыруға арналған аппараттық және бағдарламалық қамтамасыз ету бөлімге тиесілі. Электрондық пошта жүйесі мен Интернет, сондай-ақ мектептің басқа да ақпараттық ресурстары арқылы жасалған, берілген немесе алынған барлық хабарламалар, материалдар мектептің меншігі болып табылады және болып қалады және қызметкерлердің ешқайсысының жеке меншігі бола алмайды.

4. Барлық тұлғаларға пайдаланушылардың хабарламалары мен ақпаратын рұқсатсыз қарауға тыйым салынады.

5. Қызметкердің ақпараттық ресурстарды пайдалануы оның осы ресурстарды ұсыну шарттарымен келісетіндігін білдіреді.

6. Ақпарат мазмұны мектеп басшылығының шешімі бойынша уәкілетті тұлғалардың назарына жеткізілуі мүмкін.

7. Ақпараттық қауіпсіздікті қамтамасыз ету бойынша құрылымдық бөлімшесінің интернеттің зиянды ресурстарын бұғаттауға құқығы бар.

8. Сыртқы пошта интернет-ресурстарына кіруге тыйым салынады.

Ақпараттық қауіпсіздікті қамтамасыз ету

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

1) коммерциялық кәсіпорындарды үгіттеу немесе жарнамалау, діни немесе саяси идеяларды насихаттау, қызметтік міндеттерін орындаумен байланысты емес өзге де мақсаттар үшін ресурстарды пайдалануға құқылы;

2) қорлайтын немесе арандатушылық хабарламалар жасауға құқылы. Жыныстық кудалауды, нәсілдік қорлауды, жыныстық белгісі бойынша кемсітушілікті немесе жас немесе жыныстық бағдар мәселелерін, діни немесе саяси құмарлықтарды, ұлтын немесе денсаулық жағдайын қорлайтын нысанда қозғайтын басқа да түсініктемелерді, сондай-ақ Қазақстан Республикасының заңнамасында тыйым салынған басқа да ақпаратты қамтитын хабарламалар осындай деп есептеледі;

3) қызметтік әрекетке қатысы жоқ графикалық, бейне, орындалатын және т. б. файлдардың, сондай-ақ мөлшері талаптарда белгіленгеннен асатын файлдардың салынымдарын пайдалануға тыйым салынады;

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

5) топтық таратуды жеке мақсатта пайдалануға жол берілмейді;

6) пирамида-хаттарды, бақыт хаттарын, жарнамалық сипаттағы хабарламаларды және қызметтік әрекетке қатысы жоқ басқа да осыған ұқсас ақпаратты жіберу үшін ресурстарды пайдалануға құқылы емес;

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

8) басқа пошта жүйелері мен пайдаланушылардың есептік жазбаларын пайдалануға; басқа пайдаланушылардың электрондық хабарламаларына қол жеткізуге (мектеп басшылығы санкциялаған жағдайларды қоспағанда).

Интернетті пайдалану кезінде тыйым салынады:

1) интернетті қолжетімділігі шектеулі және/немесе ашық (мемлекеттік шифрлау құралдарын - ақпаратты криптографиялық қорғау құралдарын (АККҚ) пайдалана отырып шифрланбаған) таратылатын құпия ақпаратты қамтитын материалдарды беру және тарату мақсатында пайдалануға;

2) террористік, экстремистік, конституцияға қарсы және өзге де деструктивті бағыттағы материалдары бар веб-сайттарға кіру;

3) күмәнді және зиянды сайттарға, сондай-ақ ақпараты функционалдық міндеттерін атқарумен байланысты емес сайттарға кіру;

4) зиянды файлдар мен бағдарламаларды, авторлық құқықпен қорғалған бағдарламалық қамтылым мен материалдарды, сондай-ақ барлық түрдегі мультимедиялық файлдарды жүктеуге (беруге) құқылы;

5) Интернет-чат қызметтерін пайдалану;

6) Мектеп компьютерлерін бөгде интернет - провайдерлер арқылы Интернет желісіне қосуды жүзеге асыруға, сондай-ақ санкцияланбаған модемдік қосылуды пайдалануға тыйым салынады.

2. Аутентификация рәсімін ұйымдастыру ережелері

Жалпы ережелер

Осы аутентификация рәсімін ұйымдастыру қағидалары (бұдан әрі-қағидалар) пайдаланушылардың есептік жазбаларын тіркеуге және ақпараттық жүйелерді парольмен қорғауға қойылатын талаптарды айқындайды және ақпараттық қауіпсіздік қатерлерін іске асырудан болатын зиянды барынша азайтуға, сондай-ақ мектеп АЖ-да құпиялылықтың,

тұтастықтың және ақпараттың қолжетімділігінің жалпы деңгейін арттыруға арналған.

1. Осы құжатта пайдаланылған терминдердің мынадай анықтамалары бар:

1) ақпараттық қауіпсіздік (бұдан әрі - АҚ) - ақпараттық ресурстарды санкцияланбаған қол жеткізуден, әдейі немесе кездейсоқ бұрмалаудан және бұзылудан, физикалық бұзылудан, оның ішінде техногендік және табиғи сипаттағы әсерлер нәтижесінде қорғауды қамтамасыз етуге, сондай-ақ мемлекеттік ақпараттық ресурстар мен жүйелердің қорғалуының жай-күйіне, ақпараттың құпиялылығын, тұтастығын және қолжетімділігін қамтамасыз етуге бағытталған құқықтық, техникалық және ұйымдастырушылық іс-шаралар кешені;

2) ақпараттық жүйе (бұдан әрі - АЖ) – ақпараттық өзара іс - қимыл арқылы белгілі бір технологиялық әрекеттерді іске асыратын және нақты функционалдық міндеттерді шешуге арналған ақпараттық-коммуникациялық технологиялардың, қызмет көрсетуші персоналдың және техникалық құжаттаманың ұйымдастырылып ретке келтірілген жиынтығы.

3) мектеп әкімшісі - АЖ барлық кешенін үздіксіз жұмыс істеуін қамтамасыз ету және сүйемелдеу, әкімшілендіруге жауапты маман;

4) мектептің АЖ пайдаланушылары – мектептің АЖ-мен жұмыс істейтін қызметкерлері;

5) ақпараттың құпиялылығы-ақпараттың тек авторизацияланған тұлғаларға берілуін қамтамасыз ету;

6) ақпараттың тұтастығы - ақпаратты (автоматтандырылған ақпараттық жүйе ресурстарын) Өзгертуді оған құқығы бар субъектілер әдейі ғана жүзеге асыратын ақпараттың (олардың) жай-күйі;

7) Аутентификация - жүйеде іске асырылған қол жеткізудің ұсынылған деректемелерінің сәйкестігін айқындау арқылы қол жеткізу субъектісінің немесе объектісінің төлнұсқалығын растау;

8) бастапқы пароль - жаңа есептік жазбаны жасау кезінде ОЖ, ДҚБЖ, ҚБҚ әкімшісі белгілейтін символдар комбинациясы (әріптер, сандар, арнайы таңбалар);

9) негізгі пароль - №20 ЖББМ АЖ әкімшісіне ғана белгілі, есептік жазба иесінің түпнұсқалығын растау үшін пайдаланылатын символдар (әріптер, сандар, арнайы символдар) комбинациясы;

10) есепке алу жазбасы пайдаланушы туралы ақпарат: пайдаланушының аты, оның паролі, ресурстарға қол жеткізу құқығы және№20 ЖББМ АЖ-да жұмыс істеу кезіндегі артықшылықтар.

Мектептің ақпараттық жүйелерінің әкімшілері мен пайдаланушыларына қойылатын талаптар

1. Мектептің АЖ-нің әкімшілері мен пайдаланушылары міндетті:

1) өз құпиясөзін есте сақтау және ешбір түрде басқа тұлғаларға бермеу және бермеу;

2) мектептің домендік қызметіне міндетті түрде тіркелу қажет.

3) пароль жоғалған немесе жария етілген жағдайда осы факт туралы басшылықты дереу хабардар етуге және парольдің ауысуын жүргізуге тиіс;

4) құпия сөзді айына бір реттен кем емес ауыстыру қажет;

5) құпиясөзді ауыстырған кезде, 1 қосымшаға сәйкес талаптарды сақтау;

6) құпиясөзді енгізген кезде оны бөгде адамдардың қарау мүмкіндігін болдырмауы тиіс (арқадағы адам, адамның саусақтардың қозғалысын тікелей көріністе немесе шағылысқан жарықта бақылауы және т.б.).) және техникалық құралдармен (стационарлық және ұялы телефондарға жапсарлас салынған бейнекамералармен және т. б.);

7) логин мен құпиясөздің құпиялылығын және сақталуын қамтамасыз етуге міндетті.

Мектептің ақпараттық жүйелерінің әкімшілері мен пайдаланушыларының құқығы жоқ:

1) біреудің есептік жазбасында жұмыс істеу. Егер мектептің АЖ пайдаланушысының басшысы мектептің АЖ пайдаланушысына осындай жағдайларда жұмыс істеуді ұсынса, мектептің АЖ пайдаланушысы басшының жазбаша нұсқауын (бұйрығын) талап етуге және осындай нұсқауды (бұйрықты) алғанға дейін жұмысқа кіріспеуге құқылы;

2) Есептеу техникасы құралдарын мектеп корпоративтік желісіне оны мектептің домендік қызметінде тіркеусіз қосуға.

3) біреуге жеке құпиясөзді хабарлау;

4) парольдерді қағазға, файлға, электрондық жазба кітапшасына және басқа да ақпарат тасығыштарға, оның ішінде заттарға жазуға жол берілмейді;

5) макростар немесе функционалдық пернелер сияқты автоматты кіру сценарийіне парольдерді қосу.

Тіркеу элементтері мен парольдерге қойылатын талаптар

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

2. Жаңа есептік жазбаны құру кезінде мектептің АЖ әкімшісі оны бастапқы құпиясөзбен жасайды және пайдаланушыға электрондық пошта арқылы сәйкестендіргішке уақытша құпиясөз хабарлайды. Жүйеге бірінші рет кірген кезде пайдаланушы уақытша құпиясөзді ауыстыруға міндетті,

құпиясөзді таңдаған кезде "құпиясөздерге қойылатын талаптарды" (1-қосымша) басшылыққа алу қажет.

3. Иесі негізгі парольдің құпиясын сақтау үшін жеке жауап береді. Парольді басқа тұлғаларға, оның ішінде бөлім қызметкерлеріне хабарлауға, оны жазуға, сондай-ақ электрондық хабарламаларда ашық мәтінмен жіберуге тыйым салынады.

4. Пароль ешқашан компьютерлік жүйеде қорғалмаған түрде сақталмауы керек. Иесі құпия сөздерді (мысалы, қағазда, файлдарда, бағдарламалық жасақтамада немесе портативті құрылғыда) қауіпсіз сақтау кепілдігінсіз және сақтау әдісін мақұлдамай-ақ жазудан аулақ болу керек.

5. Есепке алу жазбаларының бұғатталуын бақылауды мектептің АЖ әкімшілендіруді жүзеге асыратын басшы есепке алу жазбаларын тіркеу журналының жазбаларына сәйкес жүзеге асырады.

6. Мектеп компьютерлеріне, сондай-ақ бейтарап аппараттағы өзге де ұйымдастыру техникаларына жүйелі-техникалық қызмет көрсетуге жауапты қызметкер мектеп доменінің ережелеріне сәйкес мектептің барлық пайдаланушыларын мектептің Домен қызметінде міндетті түрде тіркеуді қамтамасыз етуі тиіс.

7. Мектептің домендік қызмет саясаты мектептің ақпараттық қауіпсіздікті қамтамасыз ету үшін жауапты қызметкермен реттеледі.

Құпия сөздерді өзгерту тәртібі

1. Мектептің АЖ-н пайдаланушы/әкімшісі қосымшаға сәйкес айына кемінде бір рет негізгі паролін ауыстыруы тиіс.

2. Негізгі құпиясөзді тек пайдаланушы/АЖ әкімшісі ғана жасай алады

3. Мектеп компьютерлік бағдарламалармен және бөгде тұлғалармен құпиясөздер жасауға тыйым салады.

4. Мектептің АЖ әкімшісінің/пайдаланушының негізгі паролін жоспардан тыс ауыстыру ақ жауапты тұлғалардың талабы бойынша кез келген сәтте жүргізілуі мүмкін.

Мектеп ақпараттық жүйесінің парольдерін басқару

1. Парольдер мектеп АЖ-не пайдаланушының кіру өкілеттілігін растаудың негізгі құралы болып табылады. Мектептің АЖ сенімді парольдерді қамтамасыз етудің тиімді интерактивті құралын ұсынуы тиіс (1-қосымша).

2. АЖ-да парольдерді басқару кезінде мынадай функционал іске асырылуы тиіс:

1) жүйеге алғаш кірген кезде бастапқы құпиясөзді ауыстыру талабы;

2) теру кезінде қателерді болдырмау үшін парольдерді оларды растау рәсімімен таңдау және өзгерту (қажет болған жағдайда);

3) 1-қосымшаға сәйкес парольдердің сенімділігін тексеру;

4) берілген кезеңділікпен парольдерді міндетті түрде ауыстыру,

5) соңғы үш құпия сөзді пайдалануды болдырмау;

6) алдыңғы соңғы үш парольден кемінде 4 позицияда ерекшеленетін парольді пайдалану мүмкіндігін болдырмау;

7) құпия сөздерді шифрланған түрде сақтау;

8) пернетақтада теру кезінде құпия сөздерді экранға шығармаңыз;

3. 5 сәтсіз авторизация әрекетінен кейін құпия сөзді таңдау әрекетін болдырмау үшін пайдаланушының есептік жазбасы бұғатталуы керек. БПҰ Оқиғалар журналына пайдаланушыны авторландырудың бірнеше рет сәтсіз әрекеттері туралы хабарлама жазылуы тиіс.

Жауапкершілік

1. Қағидалардың осы ережесінің талаптары бұзылған жағдайда, мектептің АЖ әкімшілері Қазақстан Республикасының қолданыстағы заңнамасына сәйкес әкімшілік немесе өзге де жауапкершілікке тартылады.

2. Қызметтік құпияны құрайтын құпия ақпаратты жария еткені үшін қызметкер ҚР қолданыстағы заңнамасына және ішкі нормативтік актілерге сәйкес тәртіптік жауапкершілікке тартылады.

Аутентификация рәсімдерін
ұйымдастыру Ережесіне
Қосымша

Парольдерге қойылатын талаптар

1) Парольде кемінде 8 таңба болуы керек;

2) парольде бас және бас әріптер, сондай-ақ сандар және (немесе) арнайы таңбалар (#, $, @ және т. б.) болуы керек.;

3) Парольде жалпы қабылданған қысқартулар (мысалы, admin, system, user, sys, god), сондай-ақ жеке және басқа да жалпыға қол жетімді енгізулер (мысалы, күндер, атаулар, атаулар) сияқты оңай есептелетін таңбалар тізбегі болмауы керек;

4) Пароль пернетақтада орналасу реті оңай есептелетін таңбалар тобын қамтымауы керек (мысалы,!234, qWErty, qwerty123, 321369);

5) құпиясөзді ауыстырған кезде жаңа мән алдыңғыдан кемінде 4 позицияда ерекшеленуі тиіс.

3. Вирусқа қарсы бақылауды ұйымдастыру ережелері

Жалпы ережелер

Осы ережелер вирусқа қарсы бақылау жүргізу тәртібін ұйымдастыруға және бағдарламалық қамтылым мен ақпараттық жүйелерді компьютерлік вирустармен жұқтыру фактілерінің туындауын болдырмауға арналған.

Ережелер мектептің электрондық технологияларын вирусқа қарсы қорғауды ұйымдастыру кезіндегі пайдаланушылардың іс-қимылдарын регламенттейді.

Вирусқа қарсы құралдарды орнату және жаңарту

1. Мектеп тек лицензиялық вирусқа қарсы құралдарды қолдануға рұқсат етіледі.

2. Вирусқа қарсы құралдарды орнатуды және жаңартуды шарттық қатынастарда ақпараттық жүйелерге сервистік қызмет көрсетуді жүзеге асыратын бөлімше жүзеге асырады.

3. Вирусқа қарсы базаларды жаңарту мүмкіндігінше 2 күнде кемінде 1 рет жүргізіледі.

Вирусқа қарсы бақылауды жүргізу тәртібі

1. Компьютерлерді және 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. Тікелей компьютердің бағдарламалық жасақтамасын орнатқаннан (өзгерткеннен) кейін бағдарламалық қамтамасыз етуді орнатқан мектеп қызметкері вирусқа қарсы тексеру жүргізеді.

3. Міндетті вирусқа қарсы бақылауға телекоммуникациялық арналар арқылы берілетін кез келген ақпарат (кез келген форматтағы тест файлдары, деректер файлдары, орындалатын файлдар), сондай-ақ бөгде адамдардан және мектептен алынатын алмалы-салмалы тасығыштардан (магниттік дискілер, таспалар: CD-ROM, FlashUSB және т.б.) алынатын ақпараттар жатады.

4. Пайдаланушы автоматтандырылған жұмыс орнының, сондай-ақ оның барлық сыртқы құрылғыларының мақсатты пайдаланылуын бақылауды жүзеге асырады.

5. Қорғалатын компьютерлерге Орнатылатын барлық бағдарламалық қамтамасыз ету зиянды бағдарламалардың болуына алдын ала тексеріледі. Алынатын жеткізгіштердегі ақпаратты бақылау оны тікелей пайдалану алдында жүргізіледі.

6. Айына кемінде бір рет қорғалатын Компьютердің қатты дискілерінде сақталатын барлық файлдарға толық тексеру жүргізіледі.

7. Қорғалатын компьютердің барлық дискілері мен файлдарын кезектен тыс антивирустық бақылау орындалады:

- БҚ орнатылғаннан немесе өзгергеннен кейін бірден;
- дербес компьютерді жергілікті желіге қосқаннан кейін;
- зиянды бағдарламалардың болуына күдік туындаған кезде (бағдарламалардың типтік емес жұмысы, графикалық және дыбыстық әсерлердің пайда болуы, деректердің бұрмалануы, файлдардың жоғалуы, жүйелік қателер 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 қамтамасыз етуді орнатуға, конфигурация параметрлеріне өз бетінше өзгерістер енгізуге, сондай-ақ вирусқа қарсы бағдарламаларды өшіруге, жоюға тыйым салынады.

Қызметкерлердің компьютерлік вирусты анықтаудағы әрекеттері

1. Компьютерлік вирустың болуына күдік туындаған жағдайда мектеп қызметкері кезектен тыс вирусқа қарсы бақылау жүргізеді немесе қажет болған жағдайда компьютерлік вирустың болу немесе болмау фактісін анықтау үшін ақпараттандыру бөлімінің маманын тартады.

2. Компьютерлік вирус анықталған жағдайда мектеп қызметкері жұмысты тоқтата тұруға, техникалық қызмет көрсетуді жүзеге асыратын

мектеп қызметкерлеріне вирус жұқтырған файлдардың табылу фактісі туралы хабарлауға міндетті;

Вирусқа қарсы қорғауды ұйымдастыру кезіндегі бақылау

1. Мектепте вирусқа қарсы қорғауды ұйымдастыруды бақылау және оның тәртібін белгілеу АКТ директорының орынбасарына және ақпараттық қауіпсіздік бөлігінде жабдық жөніндегі инженерге жүктеледі (вирусқа қарсы қорғау жүйесін, бейімделген қауіпсіздікті қамтамасыз ету жүйесін әкімшілендіру және т.б.).

2. Осы Нұсқаулық ережелерінің сақталуын мерзімді бақылау АТ қызметкерлеріне жүктеледі.

Вирусқа қарсы қорғауды ұйымдастыру

1. Пайдаланушы антивирустық базаны үнемі тексеріп отыруы керек.

2. Вирусқа қарсы бағдарлама болмаған жағдайда дереу жабдық жөніндегі инженерге хабарлау қажет.

3. Вирусқа қарсы базаны жаңарту түскі уақытта сағат 13.00-ден бастап жүргізіледі, жаңарту компьютер конфигурациясына байланысты 20 минуттан 2 сағатқа дейін созылуы мүмкін.

4. Пайдаланушылардың АҚ инциденттеріне ден қою және штаттан тыс (дағдарысты) жағдайларда әрекет ету жөніндегі іс-қимыл тәртібі туралы Нұсқаулық

Жалпы ережелер және негізгі ұғымдар

Осы пайдаланушылардың АҚ инциденттеріне ден қою және штаттан тыс (дағдарыстық) жағдайларда әрекет ету жөніндегі іс-қимыл тәртібі туралы Нұсқаулық әртүрлі дағдарыстық жағдайлар туындаған кезде ақпараттық жүйелердің (бұдан әрі КЖ) жұмыс қабілеттілігін сақтаудың (ұстап тұрудың) негізгі шараларын, әдістері мен құралдарын, сондай-ақ АЖ және оның негізгі компоненттерінің жұмыс қабілеттілігі бұзылған жағдайда ақпаратты қалпына келтіру тәсілдері мен құралдарын және оны өңдеу процестерін айқындайды. Сонымен қатар, ол дағдарыс жағдайындағы жүйе қызметкерлерінің әртүрлі санаттарының олардың салдарын жою және келтірілген залалды азайту жөніндегі әрекеттерін сипаттайды.

1. Ақпараттық қауіпсіздікке қауіп төндіретін АЖ-ға жағымсыз әсер ету нәтижесінде туындайтын жағдай дағдарыс деп аталады. Дағдарыстық жағдай шабуылдаушының қасақана әрекеттері немесе пайдаланушылардың байқаусызда жасаған әрекеттері, апаттар, табиғи апаттар нәтижесінде туындауы мүмкін.

2. Келтірілген залалдың ауырлығы мен мөлшері бойынша дағдарыстық жағдайлар мынадай санаттарға бөлінеді:

1) қауіп төндіретін - АЖ-ның толық істен шығуына және бұдан әрі өз функцияларын орындай алмауына, сондай-ақ неғұрлым маңызды ақпаратты жоюға, бұғаттауға, заңсыз түрлендіруге немесе жария етуге әкеп соғатын.

3. Дағдарыстық жағдайларға мыналар жатады:

1) ғимаратта электр энергиясын беруді бұзу;

2) файлдық сервердің істен шығуы (ақпараттың жоғалуымен);

3)файлдық сервердің істен шығуы (ақпаратты жоғалтпай),

4) сервердегі ақпараттың жұмыс қабілеттілігін жоғалтпай ішінара жоғалуы;

5)локальдық желінің (деректер берудің физикалық ортасының) істен шығуы;

6) Елеулі - жүйенің жекелеген компоненттерінің істен шығуына (жұмыс қабілеттілігін ішінара жоғалтуға), өнімділіктің жоғалуына, сондай-ақ санкцияланбаған қол жеткізу нәтижесінде бағдарламалар мен деректердің тұтастығы мен құпиялылығының бұзылуына әкеп соғатын.

4. Күрделі 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 пайдалану әрекеттерінің тәртібі туралы толық сипаттама осы Нұсқаулықтың 1-қосымшасында берілген.

6. Дағдарыстық жағдайдың туындауы туралы ақпарат көздері:

1) жүйенің немесе оның қорғаныс құралдарының жұмысында немесе конфигурациясында күдікті өзгерістерді анықтаған пайдаланушылар өздерінің жауапкершілік аймағында;

2) дағдарыстық жағдайды анықтаған қорғаныс құралдары;

3) дағдарыстық жағдайдың туындауын немесе туындау мүмкіндігін куәландыратын жазбалары бар жүйелі журналдар.

Жалпы талаптар

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

2. Әрбір дағдарыстық жағдайды мектеп әкімшілігі талдайды. Осы талдаудың нәтижелері бойынша пайдаланушылардың өкілеттіктерін, ресурстарға қол жеткізу атрибуттарын өзгерту, жүйенің конфигурациясын немесе қорғау құралдарын баптау параметрлерін өзгерту бойынша қосымша

резервтер құру және т.б. бойынша ұсыныстар әзірленеді, қажет болған жағдайда оның туындау себептерін тексеру, себептік залалды бағалау, кінәлілерді айқындау және тиісті шаралар қабылдау келтіріледі.

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

4. Бағдарламаларды (эталондық көшірмелерді пайдалана отырып) және деректерді (сақтандыру көшірмелерін пайдалана отырып) олар жойылған немесе күрделі немесе қатер төндіретін дағдарысты ахуалмен бүлінген жағдайда жедел қалпына келтіру резервтік (сақтандыру) көшірумен және көшірмелерді сақтаудың сырткы (жүйенің негізгі компоненттеріне қатысты) көшірілуімен қамтамасыз етіледі. Сыртқы сақтау көшірмелердің арнайы бөлінген үй-жайларда орналасқан бөлінген қоймаларда (сейфтерде) болуын білдіреді.

5. Резервтік көшіруге 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. жатады.

6. Жүйеде қолданылатын барлық бағдарламалық құралдардың анықтамалық (дистрибутивтік) 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, сондай-ақ тізілімде тіркеледі.

8. Үздіксіз жұмысты қамтамасыз ету және ақпараттық жүйелерді қалпына келтіру жөніндегі персоналдың міндеттері мен іс-әрекеттері.

9. Қызметкерлердің дағдарыс жағдайындағы әрекеттері оның ауырлығына байланысты.

10. Қауіпті немесе күрделі сыни жағдай туындаған жағдайда персоналдың іс-әрекеті келесі кезеңдерді қамтиды:

1) жауапты персоналдың дереу реакциясы;

11. Дағдарыстық (штаттан тыс) жағдайларда пайдаланушылар дереу ішкі электрондық пошта арқылы, ауызша телефон арқылы немесе электрондық байланыс құралдары арқылы мектеп қызметкерлерімен, мектеп әкімшілігімен хабардар етіледі.

12. Тәуліктің күндізгі уақытында штаттан тыс (дағдарыстық) жағдайды анықтаған пайдаланушы ақпараттық ресурстар мен жүйелерді техникалық қолдау және серверлік қызмет көрсету бөлігінде мектеп, АТ қызметкерлерін хабардар етеді.

13. Тәуліктің түнгі уақытында, штаттан тыс жағдай туындаған кезде анықтаушы пайдаланушы ТҚ қызметкерін хабардар етуі тиіс және Жедел

тәртіппен телефон байланысы құралдарымен: осы жұмыс учаскесі үшін құрылымдық бөлімшелердің жауапты басшылары, ТҚ басшылығы хабардар етіледі. Оқиға міндетті түрде инциденттің нақты уақытын, хабарландырылған құрылымдық бөлімшелер басшыларының Т.А. Ә., дағдарыстық жағдайды жоюға бағытталған іс-қимылдардың сипаттамасын көрсете отырып, оқиғалардың қысқаша сипаттамасын көрсете отырып, журналда тіркеледі.

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

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

3) дағдарыстық жағдайдың туындау себептерін тексеру және кінәлілерді анықтау;

4) себептерді жою және кейіннен осындай бұзушылық фактілеріне жол бермеу бойынша шешімдер әзірлеу болып табылады.

14. Дағдарыс жағдайында жұмысты ұйымдастыруды бақылауды ДЦ жүзеге асырады.

Тіркеуді жүргізу жөніндегі іс-шаралар және штаттан тыс жағдайлардың сипаттамасы

1. Мектеп әкімшілігі АА-мен бірлесіп штаттан тыс жағдайларды есепке алу және тіркеу журналын жүргізеді. Бұл журналда міндетті түрде тіркеледі: жағдайдың себептері, оның ұзақтығы және штаттан тыс жағдай кезіндегі параметрлердің мәні. Қажет болған жағдайда акт жасалады және қиын жағдайды түзету бойынша қажетті түзету шараларының жоспары әзірленеді.

Флэш-карталарды пайдалану

Қызметтік қажеттілікке байланысты флеш-карталарды (E-token, KAZ-token, Save-Token, Usb-тасығыштарды)пайдалануға рұқсат ету