Бекітемін
Қостанай облысы әкімдігі білім
басқармасының «Қостанай қаласы білім
бөлімінің №15 жалпы білім беретін
мектебі» КММ директоры
Ж.Ж.Мирамова
«28» тамыз 2023ж

Қостанай облысы әкімдігі білім басқармасының «Қостанай қаласы білім бөлімінің №15 жалпы білім беретін мектебі» КММ

АҚПАРАТТЫҚ ҚАУІПСІЗДІК САЯСАТЫ

Костанай қаласы, 2023ж

1. Интернетті және электрондық поштаны пайдалану шарттары

Терминдер мен анықтамалар

Осы Ережеде келесі негізгі ұғымдар мен терминдер қолданылады:

1) Электрондық ақпараттық ресурстар - ақпараттық жүйелерде қамтылған электронды түрде (ақпараттық мәліметтер базасы) сақталған ақпарат;
2) Ақпараттық жүйе (бұдан әрі - АЖ) - аппараттық-бағдарламалық кешенді пайдалану арқылы ақпаратты сақтауға, өңдеуге, іздеуге, таратуға, беруге және беруге арналған жүйе.
3) Интернет-ресурс - электрондық ақпараттық ресурс, оны ұстау және (немесе) пайдалану технологиясы, жұмыс істейтін және ашық ақпараттық-коммуникациялық желі, сондай-ақ ақпараттық өзара әрекеттесуді қамтамасыз ететін ұйымдастырушылық құрылым;
4) Интернет-провайдер - Интернетке қол жетімділік қызметтерін және Интернет қызметіне қатысты басқа да қызметтерді ұсынатын ұйым;
5) Жұмыс станциясы - белгілі бір міндеттер ауқымын шешуге арналған аппараттық және бағдарламалық жасақтама жиынтығы;
6) Құпия ақпарат - мемлекеттік құпияларды қамтымайтын, оларға қол жеткізу Қазақстан Республикасының заңдарына сәйкес шектелген немесе олардың иесі, немесе Қазақстан Республикасының заңнамасында көзделген жағдайларда меншік иесі.
7) Электронды пошта мониторингі - спамның алдын-алу, зиянды кодтың болуын және электронды байланыс құралдарын пайдалану арқылы жіберілуін болдырмау мақсатында электрондық хабарламаларды (қайдан, қайдан, хабарламалардың мөлшері) қадағалау;
8) Интернет-ресурстардың мониторингі - зиянды сайттарды бұғаттау мақсатында тек интернет-ресурстың атауын (сайттың мекен-жайын) қарау кезінде сайттардың пайдаланушылары кірген тақырыптарды анықтау, Интернетке кіру орнын анықтау;
9) Ақпараттық жүйенің мониторингі - қабылданған бақылаудың тиімділігін тексеру және қол жеткізу саясатының үлгісіне сәйкестігін тексеру үшін қолданылады;
10) Электрондық пошта арқылы тарату - бұқаралық коммуникация, топтық байланыс және жарнама құралы;
11) Директорының АКТ жөніндегі орынбасары, жабдықтаушы инженер мектептің ақпараттық жүйелеріндегі күрделі ақаулардың дамуын және жойылуын қамтамасыз етуге, сондай-ақ ақпараттық ресурстар мен жүйелерді техникалық қамтамасыз етуге жауапты.

Құжаттың атауы

1. Электрондық пошта мен Интернет қызметтерін мектеп жұмыс орындарында пайдалану осы ережелері (бұдан әрі - Ережелер) электрондық поштамен және Интернет қызметімен жұмыс істеу ережелерін реттейді.
2. Интернетке қосылуды басқарудың тиімділігі, Интернет-ресурстарды пайдалану кезінде ақпараттық қауіпсіздікті ұйымдастырудың талаптарын сақтауды ақпараттық қауіпсіздік жөніндегі құрылымдық бөлім бақылайды.
3. Интернетке қол жетімділікті және электрондық пошта жүйелерін жабдықтауға арналған бағдарламалық жасақтама мектепке жатады. Электрондық пошта жүйесі мен Интернетті қолданып жасалған, жіберілген немесе алынған барлық хабарламалар, материалдар, сондай-ақ мектептің басқа да ақпараттық ресурстары мектептің меншігі болып табылады және болып қалады және қызметкерлердің ешқайсысының жеке меншігі бола алмайды.
4. Барлық адамдарға хабарламалар мен пайдаланушы туралы ақпаратты рұқсатсыз қарауға тыйым салынады.
5. Қызметкердің ақпараттық ресурстарды қолдануы оның осы ресурстарды ұсыну шарттарымен келісуін білдіреді.
6. Ақпараттың мазмұны мектеп басшылығының шешімі бойынша уәкілетті адамдарға жеткізілуі мүмкін.
7. Мектептін ақпараттық қауіпсіздігі жөніндегі құрылымдық бөлім зиянды интернет-ресурстарды бұғаттауға құқылы.
8. Интернет-ресурстардың сыртқы поштасына кіруге тыйым салынады.

Ақпараттық қауіпсіздікпен қамтамасыз ету.

1. Электронды почта және Интернет қызметін қолданғанда тиым салынады:

1) Діни немесе саяси идеяларды насихаттайтын, коммерциялық кәсіпорындарды үгіттеу немесе жарнамалау үшін қызметтік міндеттерді орындаумен байланысты емес басқа да мақсаттарды пайдалануға;
2) қорлаушы немесе арандатушылық хабарламалар жасауға. Мұндай хабарламалар жыныстық қысым көрсету, нәсілдік қорлау, жыныстық дискриминация немесе қорлайтын тәртіпте жас немесе жыныстық бағдар, діни немесе саяси қалау, ұлт немесе денсаулық жағдайы мәселелерін қозғайтын хабарламалар, сондай-ақ Қазақстан Республикасының заңнамасында тыйым салынған өзге де ақпарат болып саналады Қазақстан Республикасы;
3) тіркемелерді графика, видео, орындалатын және т.б. ресми қызметке қатысы жоқ файлдар, сондай-ақ талаптарда көрсетілген көлемнен асатын файлдар;
4) қол жетімділігі шектеулі және / немесе таралуы шектеулі ресми және / немесе құпия ақпаратты құрайтын мәліметтерді (мемлекеттік шифрлау

құралдары - криптографиялық ақпаратты қорғау құралдары - шифрлаусыз), сондай-ақ шетелдік пошта серверлерін пайдалану арқылы жіберуді сұрау;

5) топтық пошта жөнелтілімдерін жеке мақсаттар үшін пайдалануға;

6) ресурстарды пирамида хаттарын, бақыт хаттарын, жарнамалық хабарламаларды және қызметтік қызметке қатысы жоқ басқа да осыған ұқсас ақпаратты жіберу үшін пайдалануға;

7) зиянды файлдар мен бағдарламаларды, сондай-ақ авторлық құқықпен қорғалатын бағдарламалық жасақтама мен материалдарды таратуға;

8) басқа пошта жүйелерінің және пайдаланушылардың шоттарын пайдалануға; басқа пайдаланушылардың электронды хаттарына қол жеткізу (егер мектеп директоры рұқсат етпесе);

Интернетті пайдалану кезінде тыйым салынады:

1) қол жетімділігі шектеулі және / немесе таралуы шектеулі құпия ақпараты бар материалдарды беру және тарату мақсатында Интернетті пайдалануға (мемлекеттік шифрлау құралдары - криптографиялық ақпаратты қорғау құралдары (шифрлаусыз) қолдану арқылы шифрланбаған;

2) террористік, экстремистік, конституцияға қарсы және басқа да деструктивті материалдар бар веб-сайттарға кіруге;

3) күмәнді және зиянды сайттарға, сондай-ақ ақпарат функционалдық міндеттерді орындаумен байланысты емес сайттарға кіруге;

зиянды файлдар мен бағдарламаларды, авторлық құқықпен қорғалатын бағдарламалық жасақтама мен материалдарды, сондай-ақ барлық типтегі мультимедиялық файлдарды жүктеуге (беруге);

4) Интернет-чат қызметтерін пайдалануға;

5) интерактивті интернет-провайдерлер арқылы мектеп компьютерлерін Интернетке қосуға, сондай-ақ рұқсат етілмеген қосылуды пайдалануға.

2. Аутентификация процедурасын ұйымдастыру ережелері

Жалпы ережелер

Аутентификация процедурасын ұйымдастырудың осы Ережесі (бұдан әрі - Ереже) пайдаланушы тіркелгілерін тіркеу және ақпараттық жүйелерді парольмен қорғау талаптарын анықтайды және ақпараттық қауіпсіздік қатерлерін жүзеге асырудан болатын зиянды азайтуға, сондай-ақ жалпы жағдайды арттыруға арналған мектептегі құпиялылық, тұтастық және ақпараттың деңгейі.

1. Осы құжатта қолданылатын терминдердің келесі анықтамалары бар:

1) ақпараттық қауіпсіздік (бұдан әрі – АҚ) - ақпараттық ресурстарды санкцияланбаған қол жетімділіктен, қасақана немесе кездейсоқ бұрмалау мен

жоюдан, физикалық жоюдан, оның ішінде техногендік және табиғи нәтижелерден қорғауды қамтамасыз етуге бағытталған құқықтық, техникалық және ұйымдастырушылық шаралар кешені, сондай-ақ ақпараттың құпиялылығын, тұтастығын және қол жетімділігін қамтамасыз ететін мемлекеттік ақпараттық ресурстар мен жүйелерді қорғау 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 ұйымдастырылған реттелген жиынтығы.

3) АҚ мектепте жауапты - директордың орынбасары, жабдықтаушы инженер мектептің барлық АЖ кешенін басқаруға, күтіп ұстауға және үздіксіз жұмыс істеуін қамтамасыз етуге жауапты;

4) мектеп АЖ пайдаланушылары - мектепте АЖ-мен жұмыс жасайтын мұғалімдер;

5) ақпараттың құпиялығы - ақпараттың тек уәкілетті адамдарға берілуін қамтамасыз ету;

6) ақпараттың тұтастығы - оны (олардың) өзгеруін оған құқығы бар субъектілер тек қасақана жүзеге асыратын ақпараттың жағдайы (автоматтандырылған ақпараттық жүйенің ресурстары);

7) түпнұсқалық растама - ұсынылған қол жетімділік туралы мәліметтердің жүйеде енгізілген мәліметтерге сәйкестігін анықтау жолымен субъектінің немесе қол жеткізу объектісінің шынайылығын растау;

8) бастапқы пароль - жаңа тіркеуді құрған кезде ОЖ, ДҚБЖ, қолданбалы бағдарламалық жасақтама әкімшісі орнатқан таңбалардың тіркесімі (әріптер, сандар, арнайы таңбалар);

9) негізгі-пароль - шот иесінің түпнұсқалығын растау үшін қолданылатын белгілердің (әріптер, сандар, арнайы таңбалар) комбинациясы инженерге және кабинетке жауапты адамға ғана белгілі;

10) пайдаланушы туралы есептік ақпарат: пайдаланушы аты, пароль, ресурстарға қол жеткізу құқықтары және мектептің АЖ-де жұмыс істеу кезінде артықшылықтар.

АЖ қолданатын мектептің әкімшілері мен қолданушыларына қойылатын талаптар

1. Мектеп әкімшілері мен пайдаланушылары:

1) парольді ұмытпаңыз, сақтамаңыз немесе басқа тұлғаларға кез-келген нысанда бермеңіз;

2) Мектептің домендік қызметіне тіркелу қажет.

3) пароль жоғалған немесе ымыраға келген жағдайда, ол дереу бұл туралы тікелей басшылыққа хабарлауы және парольді өзгертуі керек;

4) парольді айына кемінде бір рет ауыстыру қажет;

5) парольді ауыстырған кезде 1-қосымшаға сәйкес талаптарды орындаңыз;

6) құпия сөзді енгізу кезінде рұқсат етілмеген адамдардың (артқы жағындағы адам, саусақтарының көру сызығында немесе шағылысқан жарықта қозғалуын қадағалайтын және т.б.) және техникалық құралдардың (стационарлық және кіріктірілген бейне) байқап қалу мүмкіндігін алып тастаңыз. камералар және т.б.);

7) Пайдаланушы аты мен парольдің құпиялығы мен қауіпсіздігін қамтамасыз етіңіз.

Мектеп әкімшілері мен АЖ пайдаланушылары мыналарға құқылы емес:

1) Басқа біреудің есебімен жұмыс жасаңыз. Егер мектеп директоры мектептің АЖ пайдаланушысына осындай жағдайда жұмыс жасауды ұсынса, мектептің АЖ пайдаланушысы директордан жазбаша нұсқама (бұйрық) талап етуге және мұндай нұсқаулық (бұйрық) алынғанға дейін жұмысты бастамауға құқылы;

2) Компьютерлік техниканы мектептің домендік қызметінде тіркеусіз мектеп желісіне қосыңыз.

3) Біреуге жеке пароль беру;

4)Парольдерді қағазға, файлға, электронды дәптерге және басқа тасымалдағыштарға, соның ішінде объектілерге жазыңыз;

5) Авто-кіру сценарийлеріне парольдерді қосыңыз, мысалы макростар немесе функционалдық пернелер.

Тіркеу элементтері мен парольдерге қойылатын талаптар

1. Мектептің АЖ-де жұмыс істеу үшін сізде мектептің АЖ пайдаланушы тіркеу жазбасы болуы керек (логин мен пароль).

2. Жаңа тіркеу жасау кезінде мектептің АЖ әкімшісі оны негізгі парольмен жасайды және пайдаланушыға электрондық пошта арқылы уақытша пароль беріледі. Жүйеге бірінші рет кіру кезінде пайдаланушы уақытша құпия сөзді өзгертуге міндетті. Құпия сөзді таңдағанда «Парольдерге қойылатын талаптар» басшылыққа алынуы қажет (1-қосымша).

3. Негізгі құпия сөздің құпия болуына иесі жеке жауап береді. Құпия сөзді басқа адамдарға, оның ішінде бөлім қызметкерлеріне ашуға, оны жазуға, сондай-ақ электронды пошта хабарламаларында нақты мәтінмен жіберуге тыйым салынады.

4. Құпия сөз ешқашан компьютерлік жүйеде қорғалмаған түрде сақталмауы керек. Иесі құпия сөздердің қауіпсіз сақталуына кепілдік бермей және сақтау әдісін мақұлдамай (мысалы, қағазда, файлда, бағдарламалық жасақтамада немесе портативті құрылғыда) жазбалар жасаудан аулақ болуы керек.

1. Контроль блокирования учетных записей осуществляется зам директором и инженером школы, в соответствии с записями журнала регистрации учетных записей.

2. Ответственный сотрудник за системно-техническое обслуживание компьютеров, а также иной оргтехники на нейтральном аппарате школы, должен обеспечить обязательную регистрацию всех пользователей школы в доменной службе школы согласно построенным правилам домена школы.

3. Политика доменной службы школы регулируется ответственным сотрудником за обеспечение информационной безопасности школы.

1. Блокировать етуді бақылауды мектеп директорының орынбасары және жабдықтаушы инженер тіркеу журналындағы жазбаларға сәйкес жүзеге асырады.

2. Бейтарап мектеп аппараттарындағы компьютерлерді, сондай-ақ басқа кеңсе жабдықтарын жүйеге және техникалық қызмет көрсетуге жауапты қызметкер мектеп доменінің салынған ережелеріне сәйкес барлық мектеп пайдаланушыларын мектептің домендік қызметіне міндетті тіркеуді қамтамасыз етуі керек.

3. Мектептің домендік қызмет саясатын мектептің ақпараттық қауіпсіздік офицері басқарады.

Парольдерді қалай өзгертуге болады

1. Мектептің пайдаланушысы / инженері қосымшаға сәйкес айына кемінде бір рет негізгі парольді өзгертуі керек.

2. Негізгі құпия сөзді тек пайдаланушы / инженер өзі жасай алады.

3. Мектеп компьютерлік бағдарламалармен және бөгде адамдармен пароль жасауға тыйым салады.

4. Мектептің пайдаланушысы / инженері негізгі парольді жоспардан тыс өзгерту кез-келген уақытта АЖ-дағы жауапты адамдардың өтініші бойынша жүзеге асырылуы мүмкін.

Мектептің АЖ-де парольдерін басқару

1. Құпия сөз - бұл пайдаланушының мектептің АЖ-ға кіру құқығын растайтын негізгі құрал. АЖ мектебі күшті құпия сөздерді ұсынудың тиімді интерактивті құралдарымен қамтамасыз етілуі керек (1-қосымша).

2. АЖ-да парольдерді басқару кезінде келесі функционалдылықты іске асыру қажет:

1) бірінші кіру кезінде жүйедегі негізгі құпия сөзді өзгерту талабы;

2) теру қателерін болдырмау үшін оларды құптау рәсімімен парольдерді таңдау және өзгерту (қажет болған жағдайда);

3) 1-қосымшаға сәйкес парольдердің беріктігін тексереді;

4) парольдерді белгіленген жиілікте міндетті түрде өзгерту;

5) соңғы үш парольді пайдалануды жою;

6) алдыңғы үш соңғы парольден 4 позициядан аз ерекшеленетін парольді қолдану мүмкіндігін алып тастау;

7) шифрланған құпия сөздерді сақтау;

8) парольдерді пернетақтада терген кезде оларды парольде көрсетпеңіз;

3. Құпия сөзді табу әрекеттерін болдырмау үшін пайдаланушының тіркелгісін авторизациялау бойынша 5 сәтсіз әрекеттен кейін құлыптау керек. Бағдарламалық қамтамасыз етудің оқиғалар журналы пайдаланушыға бірнеше рет сәтсіз авторизациялау әрекеттері туралы хабарламаны қамтуы керек.

Жауапкершілік

1. Осы ережесінің талаптары бұзылған жағдайда, мектептің АЖ әкімшілігі, инженері Қазақстан Республикасының қолданыстағы заңнамасына сәйкес әкімшілік немесе өзге де жауапкершілікке тартылады.

2. Қызметтік құпия болып табылатын пароль туралы ақпаратты жария еткені үшін қызметкер Қазақстан Республикасының қолданыстағы заңнамасына және ішкі тәртіп ережелеріне сәйкес тәртіптік жауапкершілікке тартылады.

Ұйымдастыру ережелеріне
аутентификация процедураларына
Қосымша

Парольге қойылатын талаптар

1) пароль кем дегенде 8 таңбадан тұруы керек;

2) пароль үлкен және кіші әріптік белгілерді, сондай-ақ сандарды және (немесе) арнайы таңбаларды (#, $, @ және т.б.) қамтуы керек;

3) пароль қарапайым қысқартулар (мысалы, әкімші, жүйе, қолданушы, sys, құдай) сияқты оңай есептелетін таңбалар тізбегін, сондай-ақ жеке және жалпыға қол жетімді басқа жазбаларды (мысалы, даталар, аттар, тақырыптар) қамтымауы керек ;

4) парольде пернетақтада реттілігі оңай есептелетін таңбалар тобы болмауы керек (мысалы,! 234, qWErty, qwerty123, 321369);

5) парольді ауыстырған кезде жаңа мән алдыңғы мәннен кем дегенде 4 позицияда ерекшеленуі керек.

3. Антивирустық бақылауды ұйымдастыру ережелері

Жалпы ережелер

Бұл ережелер антивирустық бақылау жүргізу процедурасын ұйымдастыруға және бағдарламалық жасақтама мен ақпараттық жүйелерді компьютерлік вирустармен жұқтыру фактілерінің алдын алуға арналған.

Ережелер мектептің электрондық технологияларын антивирустық қорғауды ұйымдастыру кезінде қолданушылардың әрекеттерін реттейді.

Антивирустық құралдарды орнату және жаңарту

1. Бөлімде лицензияланған антивирустық құралдарды ғана пайдалануға рұқсат етіледі.

2. Антивирустық құралдарды орнатуды және жаңартуды ақпараттық жүйелерге қызмет көрсетуді келісімшарт негізінде жүзеге асыратын бөлімше жүзеге асырады.

3. Антивирустық мәліметтер базасы, егер мүмкін болса, кем дегенде 2 күнде бір рет жаңартылады.

Антивирустық бақылау процедурасы

1. Компьютерлер мен жергілікті желіге арналған жүйелік және қолданбалы бағдарламалық жасақтаманы орнату (өзгерту) тек маманның қатысуымен жүзеге асырылады.

2. Компьютерде орнатылған (өзгертілген) бағдарламалық жасақтама компьютерлік вирустардың жоқтығына тексеріледі. Компьютерлік бағдарламалық қамтамасыздандыруды орнатқаннан (өзгерткеннен) кейін, антивирустық тексеруді бағдарламалық жасақтаманы орнатқан Сервистік ұйымның (бұдан әрі - ЖК) қызметкері жүзеге асырады.

3. Міндетті антивирустық бақылау телекоммуникация арналары арқылы алуға кез келген ақпаратқа (кез-келген форматтағы тест файлдары, деректер файлдары, орындалатын файлдар), сондай-ақ алынбалы медиадан (магниттік дискілер, таспалар: CD-ROM, Үшінші тараптар мен ұйымдардан алынған FlashUSB және т.б.).

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

5. Қорғалған компьютерлерде орнатылған барлық бағдарламалық жасақтама зиянды бағдарламалар үшін алдын-ала тексеріледі. Алынбалы тасығыштағы ақпаратты бақылау оны қолданар алдында дереу жүзеге асырылады.

6. Айына кемінде бір рет қорғалған компьютердің қатты дискілерінде сақталған барлық файлдарды толық сканерлеу жүргізіледі.

7. Қорғалған компьютердегі барлық дискілер мен файлдарды кезектен тыс антивирустық бақылау жүзеге асырылады:

- бағдарламалық жасақтаманы орнатқаннан немесе өзгерткеннен кейін бірден;
- дербес компьютерді жергілікті желіге қосқаннан кейін;
- зиянды бағдарламалардың болуы туралы күдік туындаса (бағдарламалардың типтік емес жұмысы, графикалық және дыбыстық эффектілердің пайда болуы, мәліметтердің бұрмалануы, файлдардың жоғалуы, жүйелік қателер туралы хабарламалардың жиі пайда болуы және т.б.).

8. Күмәнді жағдайларда зиянды бағдарламалардың бар немесе жоқтығын анықтау үшін сканерлеуге техникалық қолдау мамандарын тарту қажет.

9. Пайдаланушыларға жұмыс станцияларында лицензияланбаған бағдарламалық жасақтаманы орнатуға, конфигурация параметрлеріне дербес өзгерістер енгізуге, сондай-ақ антивирустық бағдарламаларды өшіруге немесе жоюға тыйым салынады.

Қызметкерлердің компьютерлік вирусты анықтаудағы әрекеттері

1. Егер компьютерлік вирустың болуы туралы күдік болса, мектеп қызметкері кезектен тыс антивирустық бақылау жүргізеді немесе қажет болған жағдайда компьютерлік вирустың бар-жоғын анықтау үшін жабдықтаушы инженерді тартады.
2. Егер компьютерлік вирус анықталса, мектеп қызметкері жұмысты тоқтатып, мектептің жабдықтаушы инженеріне вирус жұқтырған файлдардың табылғаны туралы хабарлауға міндетті;

Антивирустық қорғанысты ұйымдастыру кезіндегі бақылау

1. Мектепте вирусқа қарсы қорғанысты ұйымдастыруды бақылау және оның жүріс-тұрыс тәртібін ақпараттық қауіпсіздік тұрғысынан белгілеу мектеп инженеріне жүктелген (вирусқа қарсы қорғаныс жүйесін, адаптивті қауіпсіздік жүйесін басқару және т.б.)).
2. Осы нұсқаулық ережелерінің сақталуын мерзімді бақылау АКТ жөніндегі директорының орынбасарына, инженерге жүктеледі.

Антивирустық қорғанысты ұйымдастыру

1. Пайдаланушы антивирустық базаны үнемі тексеріп отыруға міндетті.
2. Егер антивирустық бағдарлама болмаса, дереу IT бөліміне хабарлаңыз.
3. Антивирустық базаны жаңарту түскі үзіліс кезінде сағат 13:00-де жүзеге асырылады. Жаңарту компьютердің конфигурациясына байланысты 20 минуттан 2 сағатқа дейін созылуы мүмкін.

4. Ақпараттық қауіпсіздік оқиғаларына және төтенше (дағдарыстық) жағдайларда әрекет ету үшін пайдаланушының іс-әрекеті тәртібі туралы нұсқаулық

Жалпы ережелер және негізгі түсініктер

Ақпараттық қауіпсіздік инциденттеріне және төтенше (дағдарыстық) жағдайларда жауап беру бойынша қолданушылардың іс-қимылдары туралы осы нұсқаулық әртүрлі дағдарыстық жағдайлар туындаған кезде ақпараттық жүйелердің (бұдан әрі - КС) жұмыс істеу қабілетін сақтаудың (сақтаудың) негізгі шараларын, әдістері мен құралдарын анықтайды, сондай-ақ ақпаратты қалпына келтіру әдістері мен құралдары және АЖ және оның негізгі компоненттері дұрыс жұмыс істемеген жағдайда оны өңдеу процестері. Сонымен қатар, дағдарыс жағдайындағы жүйенің әр түрлі санаттағы персоналының олардың салдарын жою және келтірілген зиянды азайту жөніндегі әрекеттері сипатталады.

1. Ақпараттық қауіпсіздікке қауіп төндіретін АЖ-ге жағымсыз әсер ету нәтижесінде туындаған жағдайды дағдарыс деп атайды. Дағдарыстық жағдай бұзушының қасақана әрекеттері немесе пайдаланушылардың білместен әрекеттері, жазатайым оқиғалар, табиғи апаттар нәтижесінде туындауы мүмкін.

2. Дағдарыстық жағдайлар ауырлық дәрежесі мен келтірілген зиян мөлшері бойынша келесі санаттарға бөлінеді:

1) қорқыту - АЖ-нің толық істен шығуына және оның функцияларын әрі қарай орындай алмауына, сондай-ақ маңызды ақпаратты жоюға, бұғаттауға, заңсыз өзгертуге немесе ымыраға әкелуге әкеледі.

3. Қауіпті дағдарыстық жағдайларға мыналар жатады:

1) ғимараттың электрмен жабдықталуын бұзу;

2) файлдық сервердің істен шығуы (ақпараттың жоғалуымен);

3) файл серверінің істен шығуы (ақпаратты жоғалтпай);

4) өнімділігін жоғалтпай, сервердегі ақпараттың ішінара жоғалуы;

5) жергілікті желінің істен шығуы (деректерді берудің физикалық ортасы);

6) елеулі - жүйенің жекелеген компоненттерінің істен шығуына (өнімділіктің ішінара жоғалуына), өнімділіктің жоғалуына, сондай-ақ рұқсат етілмеген қол жеткізу нәтижесінде бағдарламалар мен деректердің тұтастығы мен құпиялылығының бұзылуына әкеледі.

4. Ауыр дағдарыстық жағдайларға мыналар жатады:

1) жұмыс станциясының істен шығуы (ақпаратты жоғалтумен);

2) жұмыс станциясының істен шығуы (ақпаратты жоғалтпай);

3) жұмыс станциясында оның өнімділігін жоғалтпастан ақпараттың ішінара жоғалуы;

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

5. Төтенше (дағдарыстық) жағдайларда пайдалану процедурасының толық сипаттамасы осы нұсқаулықтың 1-қосымшасында келтірілген.

6. Дағдарыстық жағдайдың пайда болуы туралы ақпарат көздері:

1) жүйенің жұмысында немесе конфигурациясында немесе оны қорғау құралдарында олардың жауапкершілік саласындағы күдікті өзгерістерді анықтаған пайдаланушылар;

2) дағдарыстық жағдайды анықтаған қорғау құралдары;

3) дағдарыстық жағдайдың туындауын немесе мүмкіндігін көрсететін жазбалар бар жүйелік журналдар.

Жалпы талаптар

1. Қауіпті немесе күрделі дағдарыстық жағдайдың салдарынан жұмысы бұзылған барлық пайдаланушыларға АЖ әкімшілері электрондық пошта арқылы дереу хабарлайды. АЖ-нің дұрыс жұмыс істемеу себептерін жою, өңдеуді қалпына келтіру және бүлінген (жоғалған) ресурстарды қалпына келтіру

жөніндегі одан әрі әрекеттер персонал мен жүйені пайдаланушылардың функционалдық міндеттерімен анықталады.

2. Әр дағдарыстық жағдайды АЖ жауаптылар талдайды. Осы талдаудың нәтижелері бойынша пайдаланушы күштерін, ресурстарға қол жеткізу атрибуттарын өзгерту, жүйенің конфигурациясын өзгерту үшін қосымша резервтер құру немесе қорғау құралдарын орнату параметрлері және т.с.с. ұсыныстар әзірленеді.

3. Ауыр және қауіпті дағдарыстық жағдай істен шыққан жабдықты жедел ауыстыруды және жөндеуді, сондай-ақ бүлінген бағдарламалар мен мәліметтер жинағын резервтік көшірмелерден қалпына келтіруді талап етеді.

4. Бағдарламалардың (негізгі көшірмелерін қолданумен) және оларды (сақтандыру көшірмелерін қолдану арқылы) жойылған немесе қауіпті немесе дағдарыстық жағдайдан зақымданған жағдайда онлайн қалпына келтіру резервтік (сақтандыру) көшіру және сыртқы (негізгі компоненттеріне қатысты) арқылы жүзеге асырылады. жүйе) көшірмелерді сақтау. Сыртқы сақтау дегеніміз - арнайы бөлінген орындарда орналасқан қоймалардағы (сейфтердегі) көшірмелерді табу.

5. Жүйелік тапсырмалардың жұмыс қабілеттілігі мен орындалуын қамтамасыз ететін барлық бағдарламалар мен мәліметтер (жүйелік және қолданбалы бағдарламалық жасақтама, ашық мәліметтер және басқа мәліметтер жиынтығы), сондай-ақ архивтер, транзакциялар журналдары, жүйелік журналдар және т.б.

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

7. Бағдарламалар мен деректердің резервтік көшірмелерін құру, сақтау және пайдалану бойынша персоналдың қажетті әрекеттері персоналдың тиісті санаттарының функционалдық міндеттерінде көрінеді, әдетте бұл жүйелік әкімшілер, мектеп қызметкерлері және тұрақты тізімге де жазылады.

8. Ақпараттық жүйелердің үздіксіз жұмысын және қалпына келуін қамтамасыз ету жөніндегі персоналдың міндеттері мен әрекеттері.

9. Дағдарыс жағдайындағы персоналдың әрекеті оның ауырлығына байланысты.

10. Қауіп төндіретін немесе күрделі критикалық жағдай туындаған кезде персоналдың әрекеті келесі кезеңдерді қамтиды:

1) жауапты персоналдың жедел реакциясы;

11. Дағдарыстық (штаттық емес) жағдайларда пайдаланушыларға ішкі электрондық пошта арқылы, ауызша телефонмен немесе электрондық байланыс құралдары арқылы Қызмет көрсету ұйымының қызметкерлері (бұдан әрі - ПО), мектептің жабдықтаушы инженеріне дереу хабарлайды.

12. Күндіз апаттық (дағдарыстық) жағдайды анықтаған пайдаланушы ОО, ОА қызметкерлеріне ақпараттық ресурстар мен жүйелерді техникалық қолдау және серверлерге қызмет көрсету туралы хабарлайды.

13. Түнде, төтенше жағдай туындаған кезде, анықтаған пайдаланушы мектептегі АЖ жауапты қызметкеріне бұл туралы хабарлауы керек және шұғыл түрде телефон арқылы мектеп директорына хабарды жеткізу керек. Оқиға журналға

міндетті түрде тіркелу керек, оқиғаның нақты уақытын көрсете отырып, толық аты-жөнін көрсете отырып, оқиғалардың қысқаша сипаттамасын жазу керек, мектеп директорына, АЖ жауаптыға жеткізгені туралы, дағдарыстық жағдайды жоюға бағытталған іс-қимылдардың сипаттамаларын баяндайды.

1) жұмыс қабілетін ішінара қалпына келтіру және қайта өңдеуді бастау;
2) жүйенің толық қалпына келуі және өңдеуді толық көлемде қалпына келтіру;
3) дағдарыстық жағдайдың себептерін зерттеу және кінәлілерді анықтау;
4) себептерді жою және болашақта мұндай құқық бұзушылықтардың алдын алу бойынша шешімдер әзірлеу.

14. Дағдарыстық жағдайларда жұмысты ұйымдастыруды бақылауды ДК жүзеге асырады.

Тіркеу қызметі және төтенше жағдайлардың сипаттамасы

Мектеп қызметкерлері ОА-мен бірге төтенше жағдайларды есепке алу және тіркеу журналын жүргізеді. Бұл журналда тіркелу қажет: жағдайдың себептері, оның ұзақтығы және төтенше жағдай кезіндегі параметрлердің мәні. Қажет болған жағдайда акт жасалады және сыни жағдайды түзету үшін қажетті түзету шараларының жоспары жасалады.

Флэш-карталарды пайдалану

Жұмысқа қажетті болған жағдайда флэш-карталарды (E-token, KAZ-token, Save-Token, Usb-тасымалдаушылар) пайдалануға рұқсат беріледі.

Қосымша
Бұйрық №474, №__ .
28.09.2023ж.

Таныстым:

1.	АБДРАШЕВА А.К.	
2.	АЙТУ Б. Н.	
3.	АЛМАГАМБЕТОВА Н.А.	
4.	АЛШИМБАЕВА С.А.	
5.	АЛЬМАГАМБЕТОВА Т.Ш.	
6.	АНАСОВА А.Б.	
7.	АРЫСТАН Н.Н.	
8.	АСЫЛБЕКОВ Т.Р.	
9.	АХМЕТЖАНОВА А.М.	
10.	АХМЕТЖАНОВА Д.М.	
11.	БАЙМУХАМБЕТОВА Г.С.	
12.	БАЯНБАЕВА А.Ж.	
13.	БЕКБУЛАТОВА А.Б.	
14.	БОРАНБАЙҚЫЗЫ Д.	
15.	БРАЛИНА Т.Т.	
16.	ДОСАНОВА А.	
17.	ДАНИЯРОВА А.Д.	
18.	БИСЕКЕНОВА А.С.	
19.	ЕСИНГОЖИНА З.П.	
20.	ЕСЕЕВА А.Е.	
21.	ЕРГАЗИНА Б.К.	
22.	ЖАКАНОВ М.А.	
23.	ЖАЛҒАСБЕКОВ Н.Н.	
24.	ЖАЛМЕНДИНА Л.К.	
25.	ЖЕДИЛКАНОВА Н.Н.	
26.	ЖҮСІПБЕК А.Қ.	
27.	ИБРАГИМОВА А.К.	
28.	ИРАЛИНОВА Л.М.	
29.	ИСМАГУЛОВА Г.Д.	
30.	КАЛИЕВ С.К.	
31.	КАЛИЕВА Ж.Ш.	
32.	КАРШАЛОВА Э.Ғ.	
33.	КОЖАГАЛИЕВА Б.З.	
34.	КОШТАЕВА А.Е.	
35.	КУДЕСОВА Г.М.	
36.	ҚҰДАЙБЕРГЕН Ш.С.	
37.	МАЙШИНА А.К.	
38.	МАЖЕНОВА С.Т.	
39.	МАКАНАЕВ А.Б.	
40.	МИРАМОВА Ж.Ж.	
41.	МОЛДАХМЕТОВА Г.	
42.	МЕДЕБАЕВА А.А.	
43.	МҰКАШОВА И.Ж.	
44.	МУРЗАЛИН Е.М.	
45.	МЕШЕЛОВА Р.Ж.	
46.	НЫСАНБАЕВА А.Б.	
47.	ОМАРОВА Л.А.	
48.	РАМАЗАНОВ Ш.Ж.	
49.	САКЕНОВА Ж.Б.	
50.	СЕРИКОВА А.А.	
51.	СЕРІК Б.Қ.	
52.	СҰЛТАНОВ Қ.Қ.	
53.	СЕРІКОВА А.Қ.	
54.	СЕРКЕБАЕВА А.Б.	
55.	СЕИЛОВА А.А.	
56.	СУЛЕКИНА Н.М.	
57.	ТАСМАГАМБЕТОВА К.А.	
58.	ТОБОЛОВ А.Т.	
59.	ТӨЛЕБАЙ Г.Ө.	
60.	ТУЛЕПОВА Д.М.	
61.	УМИРЖАНОВА А.А.	
62.	УТИГЕНОВА Р.К.	
63.	ШАЯХМЕТОВА К.Х.	
64.	ХАЛИКУЛОВА Г.И.	
65.	НАМИЯЛЫ Ж.Н.	
66.	ШРІМБЕТОВА М.О.	
67.	МҰҚАТ Ж.Қ.	
68.	МУХАНГАЛИЕВ С.М.	
69.	УТЕПКАЛИЕВА Ж.Б.	
70.		
71.		
72.		
73.		
74.		
75.		
76.		
77.		
78.		
79.		
80.		
81.		
82.		
83.		
84.		
85.		
86.		

Нөмірленген, баумен байланған
және мөрмен бекітілген осы
журналда 14 бет бар.
Мектеп директоры Ж.Ж.Мирамова