Бекітемін
Директоры
Қостанай қаласы әкімдігінің Қостанай қаласы әкімдігінің білім бөлімінің №3 бөбекжай-бақшасы "МКҚК»

_____ Хамзина К. Б.

2020 жылғы " 16 " қазан

Утверждаю
Директор
ГККП «Ясли-сад №3 акимата города Костаная отдела образования акимата города Костаная»

_____ Хамзина К.Б.

«16 » октября 2020 г.

Ақпараттық қауіпсіздік саясаты «Қостанай қаласы әкімдігінің Қостанай қаласы әкімдігінің білім бөлімінің №3 бөбекжай-бақшасы» МКҚК

Политика информационной безопасности ГККП «Ясли-сад №3 акимата города Костаная отдела образования акимата города Костаная»

На ___ листах

РАЗРАБОТАНО

Отдел информатизации
ГУ «Отдел образования акимата города Костаная»

«____»_____2020 г.

Костанай, 2020ж/г

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 Қазақстан 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 қол жеткізу 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) бөлімнің ақпараттық жүйелеріндегі күрделі ақауларды дамыту мен жоюды қамтамасыз етуге, сондай-ақ ақпараттық ресурстар мен жүйелерді техникалық қолдауға жауапты ақпараттандыру бөлімінің (бұдан әрі-СБ) қызметкерлері.

Құжаттың мақсаты

1. Осы бөлімнің жұмыс станцияларында электрондық поштаны және Интернет қызметтерін пайдалану жөніндегі қағидалар (бұдан әрі-қағидалар) электрондық поштамен және Интернет қызметімен жұмыс істеу қағидаларын регламенттейді.
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 және Интернет жүйесі, сондай-ақ бөлімнің басқа да ақпараттық ресурстары арқылы жасалған, берілген немесе алынған барлық хабарламалар, материалдар бөлімнің 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. Ақпараттың мазмұны бөлім басшылығының шешімі бойынша уәкілетті тұлғалардың назарына жеткізілуі мүмкін.
7. Бөлімнің ақпараттық қауіпсіздікті қамтамасыз ету жөніндегі құрылымдық бөлімшесі интернеттің зиянды ресурстарын бұғаттауға құқылы.
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 құдалауды, 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 (бөлім басшылығы рұқсат берген 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) бөлімнің компьютерлерін бөгде интернет - провайдерлер арқылы Интернет желісіне қосуды жүзеге асыруға, сондай-ақ санкцияланбаған модемдік қосуды пайдалануға міндетті.

2. Аутентификация рәсімін ұйымдастыру ережелері

Жалпы ережелер

Осы аутентификация рәсімін ұйымдастыру қағидалары (бұдан әрі-қағидалар) пайдаланушылардың есепке алу жазбаларын тіркеуге және ақпараттық жүйелерді парольмен қорғауға қойылатын талаптарды айқындайды және ақпараттық қауіпсіздік қатерлерін іске асырудан болатын залалды барынша азайтуға, сондай-ақ бөлімнің 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) бөлімнің АЖ әкімшісі-бөлімнің барлық АЖ кешенін әкімшілендіруге, сүйемелдеуге және үздіксіз жұмыс істеуін қамтамасыз етуге жауапты маман;

4) бөлімнің АЖ пайдаланушылары-бөлімнің АЖ-мен жұмыс істейтін қызметкерлер;

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-бөлім АЖ әкімшісіне ғана белгілі, есептік жазба иесінің түпнұсқалығын растау үшін пайдаланылатын символдар комбинациясы (әріптер, сандар, арнайы таңбалар);
10) есептік жазба Пайдаланушы туралы ақпарат: Пайдаланушының аты, оның паролі, ресурстарға қол жеткізу құқығы және бөлімнің АЖ-да жұмыс істеген кездегі артықшылықтар.

Бөлімнің АЖ әкімшілері мен пайдаланушыларына қойылатын талаптар

1. Бөлімнің АЖ әкімшілері мен пайдаланушылары міндетті:
1) өз құпиясөзін есте сақтау және ешбір түрде басқа тұлғаларға бермеу және бермеу;
2) бөлімнің домендік қызметінде 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.) қамтамасыз етіледі.);
7) логин мен құпиясөздің құпиялылығын және сақталуын қамтамасыз етуге міндетті.

Бөлімнің АЖ әкімшілері мен пайдаланушыларының құқығы жоқ:

1) біреудің есептік жазбасында жұмыс істеу. Егер бөлімнің АЖ пайдаланушысының басшысы бөлімнің АЖ пайдаланушысына осындай жағдайларда жұмыс істеуді ұсынған жағдайда, бөлімнің АЖ пайдаланушысы басшының жазбаша нұсқауын (бұйрығын) талап етуге және осындай нұсқауды (бұйрықты) алғанға дейін жұмысқа кіріспеуге құқылы);
2) бөлімнің домендік қызметінде тіркеусіз бөлімнің корпоративтік желісіне есептеу техникасы құралдарын 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 қосыңыз.

Тіркеу элементтері мен парольдерге қойылатын талаптар

1. Бөлімнің АЖ-да жұмыс істеу үшін бөлімнің АЖ пайдаланушысының есептік жазбасы (логин және пароль) болуы қажет.
2. Жаңа есептік жазбаны жасаған кезде бөлімнің АЖ әкімшісі оны бастапқы парольмен жасайды және пайдаланушыға электрондық пошта арқылы идентификаторға уақытша пароль 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 бөлімнің АЖ әкімшілендіруді жүзеге асыратын басшысы есепке алу жазбаларын тіркеу журналының жазбаларына сәйкес жүзеге асырады.
6. Бөлімнің бейтарап аппаратында компьютерлерге, сондай-ақ басқа да оргтехникаға жүйелік-техникалық қызмет көрсетуге жауапты қызметкер бөлімнің барлық пайдаланушыларын бөлімнің домендік ережелеріне сәйкес бөлімнің домендік қызметінде міндетті түрде тіркеуді қамтамасыз етуі тиіс.
7. Бөлімнің домендік қызметінің саясаты бөлімнің ақпараттық қауіпсіздігін қамтамасыз етуге жауапты қызметкермен реттеледі.

Құпия сөздерді өзгерту тәртібі

1. Бөлімнің АЖ пайдаланушысы/әкімшісі қосымшаға сәйкес айына кемінде бір рет негізгі парольді ауыстыруы тиіс.
2. Негізгі құпиясөзді тек пайдаланушы / АЖ әкімшісі ғана жасай алады
3. Бөлім компьютерлік бағдарламалар мен үшінші тараптардың құпия сөздерін жасауға тыйым салады.
4. Пайдаланушы/бөлімнің АЖ әкімшісінің негізгі паролін жоспардан тыс ауыстыру АҚ-ға жауапты тұлғалардың талап етуі бойынша кез келген сәтте жүргізілуі мүмкін.

Бөлімнің АЖ парольдерді басқару

1. Парольдер пайдаланушының бөлімнің АЖ-не кіру өкілеттігін растаудың негізгі құралы болып табылады. Бөлімнің 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, бөлімнің 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.

Қосымша
ұйымдастыру Ережелеріне
аутентификация рәсімдері

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 қоғамдық 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 қағидалары

Жалпы ережелер

Осы Қағидалар вирусқа қарсы бақылау жүргізу тәртібін ұйымдастыруға және бағдарламалық қамтылым мен ақпараттық жүйелерді компьютерлік вирустармен жұқтыру фактілерінің туындауын болдырмауға арналған.
Қағидалар бөлімнің электрондық технологияларын вирусқа қарсы қорғауды ұйымдастыру кезіндегі пайдаланушылардың іс-қимылдарын регламенттейді.

Вирусқа қарсы құралдарды орнату және жаңарту

1. Бөлімде қолдануға лицензиялық вирусқа қарсы құралдар ғана 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 жасақтаманы орнатқан қызмет көрсету ұйымының (бұдан әрі - ҚБ) қызметкері антивирустық тексеруді орындайды.

3. Міндетті вирусқа қарсы бақылауға телекоммуникациялық арналар арқылы берілетін кез келген ақпарат (кез келген форматтағы тест файлдары, деректер файлдары, орындалатын файлдар), сондай-ақ бөгде адамдар мен ұйымдардан алынатын алмалы-салмалы тасығыштардан алынатын ақпарат (магниттік дискілер, таспалар: CD-ROM, FlashUSB және т.б.) 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 Бөлім 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 Бөлім қызметкері
жұмысты тоқтата тұру, ақпараттандыру бөлімінің техникалық қызмет көрсетуді жүзеге асыратын қызметкерлеріне вирус жұқтырған файлдардың

табылу фактісі туралы хабарлау;

Вирусқа қарсы қорғауды ұйымдастыру кезіндегі бақылау

1. Бөлімде вирусқа қарсы қорғанудың ұйымдастырылуын бақылау және оның мінез-құлық тәртібін белгілеу ақпараттандыру бөлімінің қызметкерлеріне ақпараттық қауіпсіздік бөлігінде (вирусқа қарсы қорғау жүйесін, бейімделген қауіпсіздікті қамтамасыз ету жүйесін әкімшілендіру және т.б.) жүктеледі.
2. Осы Нұсқаулық ережелерінің сақталуын мерзімді бақылау ақпараттандыру бөліміне жүктеледі.

Вирусқа қарсы қорғауды ұйымдастыру

1. Пайдаланушы антивирустық базаны үнемі тексеріп отыруы керек.
2. Вирусқа қарсы бағдарлама болмаған жағдайда дереу ақпараттандыру бөлімінің қызметкерлеріне 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 (деректерді 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 ОИ 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 сыртқы (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, ОС қызметкерлері, 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 қызмет көрсететін ұйымның (бұдан әрі - ББ), ЖБ қызметкерлері электрондық байланыс құралдарының көмегімен хабардар етіледі.
12. Тәуліктің күндізгі уақытында штаттан тыс (дағдарыстық) жағдайды анықтаған пайдаланушы ақпараттық ресурстар мен жүйелерді және серверлік қызмет көрсетуді техникалық қолдау бөлігінде ҚБ, АА 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. ОИ қызметкерлері СА-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.

1. Правила использования интернета и электронной почты

Термины и определения

В данных Правилах используются следующие основные понятия и термины:

1) Электронные информационные ресурсы - информация, хранимая в электронном виде (информационные базы данных), содержащаяся в информационных системах;

2) Информационная система (далее - ИС) - система, предназначенная для хранения, обработки, поиска, распространения, передачи и предоставления информации с применением аппаратно-программного комплекса.

3) Интернет ресурс - электронный информационный ресурс, технология его ведения и (или) использования, функционирующие и открытой информационно-коммуникационной сети, а также организационная структура, обеспечивающая информационное взаимодействие;

4) Интернет-провайдер - организация, предоставляющая услуги доступа к Интернету и иные, связанные с Интернет услугой;

5) Рабочая станция - комплекс аппаратных и программных средств, предназначенных для решения определенного круга задач;

6) Конфиденциальная информация - информация, не содержащая государственных секретов, доступ к которой ограничен в соответствии с законами Республики Казахстан или их собственником, или владельцем в случаях, предусмотренных законодательством Республики Казахстан;

7) Мониторинг электронной почты — отслеживание электронных сообщений (куда, откуда, размер сообщений) в целях предотвращения спама, наличия вредоносного кода, которые могут передаваться с помощью электронных средств связи и защиты от него;

8) Мониторинг интернет-ресурсов - выявление тематики, посещаемых пользователями сайтов, выявление места доступа в Интернет, при этом, осуществляется только просмотр названия Интернет-ресурса (адрес сайта) в целях блокирования вредоносных сайтов;

9) Мониторинг информационной системы - применяется для проверки эффективности принятых средств контроля и проверки соответствия модели политики доступа;

10) Рассылка электронной почты - средство массовой коммуникации, группового общения и рекламы;

11) Сотрудники отдела информатизации (далее ОИ), ответственные за обеспечение развития и устранения сложных неисправностей в информационных системах Отдела, а также технической поддержке информационных ресурсов и систем.

Назначение документа

1. Настоящие Правила по использованию электронной почты и служб Интернет на рабочих станциях Отдела (далее - Правила) регламентирует правила работы с электронной почтой и службой Интернет.

2. Эффективность управления доступа к Интернету, выполнение требований к организации информационной безопасности в использовании Интернет-ресурсов контролируется структурным подразделением по обеспечению информационной безопасности.

3. Аппаратное и программное обеспечение для организации доступа в сеть Интернет и системы электронной почты принадлежит отделу. Все сообщения, материалы, созданные, переданные или полученные с помощью системы электронной почты и Интернет, а также другими информационными ресурсами Отдела, являются и остаются собственностью Отдела и не могут быть личной собственностью ни одного из сотрудников.

4. Всем лицам запрещается несанкционированный просмотр сообщений и информации пользователей.

5. Использование сотрудником информационных ресурсов означает его согласие с условиями предоставления данных ресурсов.

6. Содержание информации может быть доведено до сведения уполномоченных лиц по решению руководства Отдела.

7. Структурное подразделение по обеспечению информационной безопасности Отдела имеет право блокировать вредоносные ресурсы Интернет.

8. Доступ к внешним почтовым Интернет-ресурсам запрещен.

Обеспечение информационной безопасности

1. При использовании электронной почты и служб Интернет запрещается:

1) использовать ресурсы для агитации или рекламы коммерческих предприятий, пропаганды религиозных или политических идей, иных целей, не связанных, с выполнением служебных обязанностей;

2) создавать оскорбительные или провокационные сообщения. Таковыми считаются сообщения, содержащие сексуальные домогательства, расовые оскорбления, дискриминацию по половому признаку или другие комментарии, затрагивающие в оскорбительной форме вопросы возраста или сексуальной ориентации, религиозные или политические пристрастия, национальность или состояние здоровья, а также другую информацию, запрещенную законодательством Республики Казахстан;

3) использовать вложения графических, видео, исполняемых и т.п. файлов, не относящиеся к служебной деятельности, а также файлов, размер которых превышает установленный в требованиях;

4) запрашивать отправлять сообщения, содержащие сведения составляющие служебную и/или конфиденциальную информацию с ограниченным доступом и/или распространением в открытом (незашифрованном с использованием государственных шифровальных средств - средств криптографической защиты информации (СКЗИ) виде, а также с использованием зарубежных почтовых серверов;

5) пользоваться групповой рассылкой в личных целях;

6) использовать ресурсы для рассылки писем-пирамид, писем счастья, сообщений рекламного характера и другой подобной информации, не имеющей отношения к служебной деятельности;

7) распространять вредоносные файлы и программы, а также программное обеспечение и материалы, защищенные авторским правом;

8) использовать учетные записи других почтовых систем и пользователей; получать доступ к электронным сообщениям других пользователей (за исключением случаев, санкционированных руководством Отдела);

При использовании Интернет запрещается:

1) использовать Интернет в целях передачи и распространения материалов, содержащих конфиденциальную информацию с ограниченным доступом и/или распространением в открытом (незашифрованном с использованием государственных шифровальных средств - средств криптографической защиты информации (СКЗИ);

2) посещать веб-сайты, содержащие материалы террористической, экстремисткой, антиконституционной и иной деструктивной направленности;

3) посещать сомнительные и вредоносные сайты, а также сайты, информация на которых не связана с исполнением функциональных обязанностей;

4) загружать (передавать) вредоносные файлы и программы, программное обеспечение и материалы, защищенные авторским правом, а также мультимедийные файлы всех типов;

5) использовать службы Интернет-чатов;

6) осуществлять подключение компьютеров Отдела к сети Интернет через сторонних Интернет - провайдеров, а также использовать несанкционированное модемное подключение.

2. Правила организации процедуры аутентификации

Общие положения

Настоящие Правила организации процедуры аутентификации (далее - Правила) определяют требования к регистрации учетных записей пользователей и парольной защиты информационных систем и предназначены для минимизации ущерба от реализации угроз информационной безопасности, а также для повышения общего уровня конфиденциальности, целостности и доступности информации в ИС отдела.

1. Термины, использованные в настоящем документе, имеют следующие определения:

1) информационная безопасность (далее - ИБ) - комплекс правовых, технических, и организационных мероприятий, направленных на обеспечение защиты информационных ресурсов от несанкционированного доступа, преднамеренного или случайного искажения и разрушения, физического разрушения, в том числе в результате воздействий техногенного и природного характера, а также состояние защищенности государственных информационных ресурсов и систем, обеспечение конфиденциальности, целостности и доступности информации;

2) информационная система (далее - ИС) – организационно - упорядоченная совокупность информационно-коммуникационных технологий, обслуживающего персонала и технической документации, реализующая определенные технологические действия посредством информационного взаимодействия и предназначенных для решения конкретных функциональных задач.

3) Администратор ИС Отдела - специалист, ответственный за администрирование, сопровождение и обеспечение бесперебойного функционирования всего комплекса ИС Отдела;

4) Пользователи ИС Отдела - сотрудники, работающие с ИС Отдела;

5) Конфиденциальность информации - обеспечение предоставления информации только авторизованным лицам;

6) Целостность информации - состояние информации (ресурсов автоматизированной информационной системы), при котором ее (их) изменение осуществляется только преднамеренно субъектами, имеющими на него право;

7) Аутентификация - подтверждение подлинности субъекта или объекта доступа путем определения соответствия предъявленных реквизитов доступа реализованными в системе;

8) Первичный пароль — комбинация символов (буквы, цифры, специальные символы), устанавливаемые администратором ОС, СУБД, ППО при создании новой учетной записи;

9) Основной пароль - комбинация символов (буквы, цифры, специальные

символы), известная только Администратору ИС Отдела, используемая для подтверждения подлинности владельца учетной записи;

10) Учетная запись информация о пользователе: имя пользователя, его пароль, права доступа к ресурсам и привилегии при работе в ИС Отдела.

Требования к администраторам и пользователям ИС Отдела

1. Администраторы и пользователи ИС Отдела обязаны:

1) Запомнить свой пароль, и ни в каком виде не сохранять и не передавать другим лицам;

2) Быть обязательно зарегистрированными в доменной службе Отдела.

3) В случае утраты или компрометации пароля должен незамедлительно оповестить непосредственнее руководство о данном факте и провести смену пароля;

4) Необходимо производить смену пароля не реже чем один раз в месяц;

5) При смене пароля, соблюдать требования согласно Приложению 1;

6) При вводе пароля исключить возможность его подсматривания посторонними лицами (человек за спиной, наблюдение человеком за движением пальцев в прямой видимости или в отраженном свете и тп.) и техническими средствами (стационарными и встроенными в мобильные телефоны видеокамерам и т.п.);

7) Обеспечить конфиденциальность и сохранность логина и пароля.

Администраторы и пользователи ИС Отдела не имеют право:

1) Работать под чужой учетной записью. В случае, если руководитель пользователя ИС Отдела предлагает пользователю ИС Отдела работать в таких условиях, пользователь ИС Отдела вправе потребовать письменного указания (приказа) руководителя и не приступать к работе до получения такого указания (приказа);

2) Подключать средства вычислительной техники в корпоративную сеть Отдела без регистрации его в доменной службе Отдела.

3) Сообщать кому-либо личный пароль;

4) Записывать пароли на бумаге, в файле, электронной записной книжке и других носителях информации, в том числе на предметах;

5) Включать пароли в сценарии автоматического входа в систему, например, в макросы или функциональные клавиши.

Требования к элементам регистрации и паролям

1. Для работы в ИС Отдела необходимо иметь учетную запись пользователя ИС Отдела (логин и пароль).
2. При создании новой учетной записи администратор ИС Отдела создает ее с первичным паролем и пользователю по электронной почте сообщает идентификатор временный пароль. При первом входе в систему пользователь обязан произвести смену временного пароля, При выборе пароля необходимо руководствоваться «Требования к паролям» (Приложение 1).
3. Владелец несет персональную ответственность за сохранение о тайне основного пароля. Запрещается сообщать пароль другим лицам, в том числе сотрудникам отдела, записывать его, а также пересылать открытым текстом в электронных сообщениях.
4. Пароль никогда не следует хранить в компьютерной системе в незащищенной форме. Владелец должен избегать делать записи (например, на бумаге, в файлах, программного обеспечения или портативном устройстве) паролей, без гарантии их безопасного хранения и утверждения метода хранения.
5. Контроль блокирования учетных записей осуществляется руководителем, осуществляющего администрирование ИС Отдела, в соответствии с записями журнала регистрации учетных записей.
6. Ответственный сотрудник за системно-техническое обслуживание компьютеров, а также иной оргтехники на нейтральном аппарате Отдела, должен обеспечить обязательную регистрацию всех пользователей Отдела в доменной службе Отдела согласно построенным правилам домена Отдела.
7. Политика доменной службы Отдела регулируется ответственным сотрудником за обеспечение информационной безопасности Отдела.

Порядок смены паролей

1. Пользователь/администратор ИС Отдела должен сменить основной пароль не реже чем один раз в месяц в соответствии С Приложением.
2. Основной пароль может быть создан только самим пользователем/администратором ИС
3. Отдел запрещает генерировать пароли компьютерными программами и сторонними лицами.
4. Внеплановая смена основное пароля пользователем/администратора ИС Отдела может быть произведена в любой момент по требованию ответственных лиц на ИБ.

Управление паролями в ИС Отдела

1. Пароли являются основным средством подтверждения полномочий доступа пользователя к ИС Отдела. ИС Отдела должна предоставлять эффективное интерактивное средство обеспечения надежных паролей (Приложение 1).

2. При Управлении паролями в ИС должен быть реализован следующий функционал:

1) Требование смены первичного пароля при первом входе и систему;
2) Выбор и изменение паролей с процедурой их подтверждения для исключения ошибок при наборе (при необходимости);
3) Проверки надежности паролей в соответствии с Приложением 1;
4) Обязательная смена паролей с заданной периодичностью,
5) Исключение использования трех последних паролей;
6) Исключение возможность использования пароля, отличающегося от предыдущих трех последних паролей менее чем в 4 позициях;
7) Хранить пароли в зашифрованном виде;
8) Не выводить пароли на экран при их наборе на клавиатуре;

3. Для предотвращения попыток подбора пароля после 5 неудачных попыток авторизации учетная запись пользователя должна блокироваться. В журнал событий ППО должно заноситься сообщение о многократно неудавшихся попытках авторизации пользователя.

Ответственность

1. В случае нарушения требований настоящего положения Правил, администраторы ИС Отдела привлекаются к административной или иной ответственности в соответствии с действующим законодательством Республики Казахстан.

2. За разглашение парольной информации, которая представляет служебную тайну, работник привлекается к дисциплинарной ответственности в соответствии с действующим законодательством РК и внутренними нормативными актами.

Приложение
к Правилам организации
процедуры аутентификации

Требования к паролям

1) Пароль должен содержать не менее 8 символов;
2) В пароле должны присутствовать прописные и заглавные буквенные

символы, а также цифры и (или) специальные символы (#, $, @ и др.);

3) Пароль не должен включать легко вычисляемые последовательности символов, такие как общепринятые сокращения, (например, admin, system, user, sys, god), также личные и иные общедоступные введения (например, даты, имена, названия);

4) Пароль не должен включать группы символов, последовательности расположения которых на клавиатуре легко вычисляется (например, !234, qWErty, qwerty123, 321369);

5) При смене пароля новое значение должны отличаться от предыдущего не менее, чем в 4 позициях.

3. Правила организации антивирусного контроля

Общие положения

Настоящие правила предназначены для организации порядка проведения антивирусного контроля и предотвращения возникновения фактов заражения программного обеспечения и информационных систем компьютерными вирусами.

Правила регламентируют действия пользователей при организации антивирусной защиты электронных технологий Отдела.

Установка и обновление антивирусных средств

1. К применению в отделе допускаются только лицензионные антивирусные средства.
2. Установку и обновление антивирусных средств осуществляется подразделением, осуществляющим на договорных отношениях сервисное обслуживание информационных систем.
3. Обновление антивирусных баз производится по возможности не реже 1 раза в 2 дня.

Порядок проведения антивирусного контроля

1. Установка (изменение) системного и прикладного обеспечения компьютеров и локальной вычислительной сети осуществляется только в присутствии специалиста.
2. Устанавливаемое (изменяемое) на компьютер программное обеспечение проверяется на отсутствие компьютерных вирусов. Непосредственно после установки (изменения) программного обеспечения компьютера выполняется антивирусная проверка сотрудником Обслуживающей организации (далее - ОО),

установившем программное обеспечение.

3. Обязательному антивирусному контролю подлежит любая информация (тестовые файлы любых форматов, файлы данных, исполняемые файлы), получаемая к передаваемая по телекоммуникационным каналам, а также информаций со съемных носителей (магнитные диски, ленты: CD-ROM, FlashUSB, и т.п.), получаемых от сторонних лиц и организаций.

4. Пользователь осуществляет контроль за целевым использованием автоматизированного рабочего места, а также всех его внешних устройств.

5. Все программное обеспечение, устанавливаемое на защищаемые компьютеры, предварительно проверяется на наличие вредоносных программ. Контроль информации на съемных носителях производится непосредственно перед ее использованием.

6. Не реже одного раза в месяц проводится полная проверка всех файлов, хранящихся на жестких дисках защищаемого компьютера.

7. Внеочередной антивирусный контроль всех дисков и файлов защищаемого компьютера выполняется:

- сразу после установки или изменения ПО;
- после подключения автономного компьютера к локальной сети;
- при возникновении подозрения на наличие вредоносных программ (нетипичная работа программ, появление графических и звуковых эффектов, искажение данных, пропадание файлов, частое появление сообщений о системных ошибках и т.п.).

8. В сомнительных случаях для определения факта наличия или отсутствия вредоносных программ к проверке необходимо привлечь специалистов технической поддержки.

9. Пользователям запрещается установка нелицензированного программного обеспечения на рабочие станции, самостоятельного внесения изменений в настройки конфигурации, а также отключение, удаление антивирусных программ.

Действия сотрудников при обнаружении компьютерного вируса

1. При возникновении подозрения на наличие компьютерного вируса сотрудник Отдела проводит внеочередной антивирусный контроль или при необходимости привлекает специалиста отдела информатизации для определения ими факта наличия или отсутствия компьютерного вируса.

2. При обнаружении компьютерного вируса сотрудник Отдела обязан приостановить работу, поставить в известность о факте обнаружения зараженных вирусом файлов сотрудников отдела информатизации, осуществляющих техническое обслуживание;

Контроль при организации антивирусной защиты

1. Контроль за организацией антивирусной зашиты в отделе и установление порядка её поведения возлагается на сотрудников отдела информатизации, в части информационной безопасности (администрирование антивирусной системы защиты, системы обеспечения адаптивной безопасности и т.д.).
2. Периодический контроль за соблюдением положений данной инструкции возлагается на отдел информатизации.

Организация антивирусной зашиты

1. Пользователь обязан регулярно проверять антивирусную базу.
2. При отсутствии антивирусной программы немедленно сообщить сотрудникам отдел информатизации.
3. Обновление антивирусной базы проводится в обеденное время с 13.00 ч. Обновление может длиться от 20 минут до 2-х часов в зависимости от конфигурации компьютера.

4 Инструкции о порядке действий пользователей по реагированию на инциденты ИБ и во внештатных (кризисных) ситуациях

Общие положения и основные понятия

Настоящая Инструкция о порядке действий пользователей по реагированию на инциденты ИБ и во внештатных (кризисных) ситуациях определяет основные меры, методы и средства сохранения (поддержания) работоспособности информационных систем (далее КС) при возникновении различных кризисных ситуаций, а также способы и средства восстановления информации и процессов ее обработки в случае нарушения работоспособности ИС и ее основных компонентов. Кроме того, она описывает действия различных категорий персонала системы в кризисных ситуациях по ликвидации их последствий и минимизации наносимого ущерба.

1. Ситуация, возникающая в результате нежелательного воздействия на ИС, приведшая к угрозе информационной безопасности, называется кризисной. Кризисная ситуация может возникнуть в результате преднамеренных действий злоумышленника или непреднамеренных действий пользователей, аварий, стихийных бедствий.
2. По степени серьезности и размерам наносимого ущерба кризисные ситуации разделяются на следующие категории:

1) угрожающая - приводящая к полному выходу из строя ИС и неспособности выполнять далее свои функции, а также к уничтожению, блокированию, неправомерной модификации или компрометации наиболее важной информации.

3. К угрожающим кризисным ситуациям относятся:

1) нарушение подачи электроэнергии в здании;

2) выход из строя файлового сервера (с потерей информации);

3) выход из строя файлового сервера (без потери информации),

4) частичная потеря информации на сервере без потери его работоспособности;

5) выход из строя локальной сети (физической среды передачи данных);

6) серьезная - приводящая к выходу из строя отдельных компонентов системы (частичной потере работоспособности), потере производительности, а также к нарушению целостности и конфиденциальности программ и данных в результате несанкционированного доступа.

4. К серьезным кризисным ситуациям относятся:

1) выход из строя рабочей станции (с потерей информации);

2) выход из строя рабочей станции (без потери информации);

3) частичная потеря информации на рабочей станции без потери ее работоспособности;

4) стихийные бедствия (пожар, наводнение, ураган и т.д.).

5. Подробное описание о порядке действий пользований во внештатных (кризисных) ситуациях находится в Приложении 1 к данной инструкции.

6. Источники Информации о возникновении кризисной ситуации:

1) пользователи, обнаружившие подозрительные изменения в работе или конфигурации системы, или средств ее защиты в своей зоне ответственности;

2) средства защиты, обнаружившие кризисную ситуацию;

3) системные журналы, в которых имеются записи, свидетельствующие о возникновении или возможности возникновения кризисной ситуации.

Общие требования

1. Все пользователи, работа которых нарушена в результате возникновения угрожающей или серьезной кризисной ситуации, немедленно оповещаются посредством электронной почты администраторами ИС. Дальнейшие действия по устранению причин нарушения работоспособности ИС, возобновлению обработки и восстановлению поврежденных (утраченных) ресурсов определяются функциональными обязанностями персонала и пользователей системы.

2. Каждая кризисная ситуация анализируется ОИ. По результатам этого анализа вырабатываются предложения по изменению полномочий пользователей, атрибутов доступа к ресурсам, созданию дополнительных резервов по изменению конфигурации системы или параметров настройки средств защиты и т.п., при необходимости приводится расследование причин ее возникновения, оценка причинного ущерба, определение виновных и принятие соответствующих мер.

3. Серьезная и угрожающая кризисная ситуация требует оперативной замены и ремонта вышедшего из строя оборудования, а также восстановления поврежденных программ и наборов данных из резервных копий.

4. Оперативное восстановление программ (используя эталонные копии) и данных (используя страховые копии) в случае их уничтожения или порчи с серьезной или угрожающей кризисной ситуации обеспечивается резервным (страховым) копированием и внешним (по отношению к основным компонентам системы) хранения копий. Внешнее хранение подразумевает нахождение копий в выделенных хранилищах (сейфах), находящихся в специально отведенных помещениях.

5. Резервному копированию подлежат все программы и данные, обеспечивающие работоспособность и выполнение задач системы (системное и прикладное программное обеспечение, открытых данных и другие наборы данных), а также архивы, журналы транзакций, системные журналы и т.д.

6. Все программные средства, используемые в системе, имеют эталонные (дистрибутивные) копии.

7. Необходимые действия персонала по созданию, хранению и использованию резервных копий программ и данных отражаются в функциональных обязанностях соответствующих категорий персонала, как правило это - Системные администраторы, администраторы автоматизированных рабочих мест, сотрудники ОИ, а также фиксируются в реестре.

8. Обязанности и действия персонала по обеспечению непрерывной работы и восстановлению информационных систем.

9. Действия персонала в кризисной ситуации зависят от степени ее тяжести.

10. В случае возникновения угрожающей или серьезной критической ситуации действия персонала включают следующие этапы:

1) немедленная реакция ответственного персонала;

11. В кризисных (внештатных) ситуациях пользователи немедленно оповещаются посредством внутренней электронной почты, устно по телефону или с помощью электронных средств связи сотрудниками Обслуживающей организации (далее - ОО), ОИ.

12. В дневное время суток пользователь, обнаруживший внештатную (кризисную) ситуацию, ставит в известность сотрудников ОО, СА в части технической поддержки информационных ресурсов и систем и серверного обслуживания.

13. В ночное время суток, при возникновении внештатной ситуации обнаруживший пользователь должен поставить в известность сотрудника ОИ, и срочном порядке средствами телефонной связи оповещаются: ответственные руководители структурных подразделений за данный участок работ, руководство ОИ. Событие в обязательном порядке регистрируется в журнале, с указанием точного времени инцидента, краткого описания событий, с указанием Ф.И.О. оповещенных руководителей структурных подразделений, описания действий, направленных на устранение кризисной ситуации.

1) частичное восстановление работоспособности и возобновление обработки;

2) полное восстановление системы и возобновление обработки в полном объеме;

3) расследование причин возникновения кризисной ситуации и установление виновных;

4) выработка решений по устранению причин и недопущения в последующем подобных фактов нарушений.

14. Контроль за организацией работ в кризисных ситуациях осуществляет ДЦ.

Мероприятия по ведению регистрации и описанию внештатных ситуаций

1. Сотрудники ОИ, совместно с СА заводят журнал учета и регистрации внештатных ситуаций. В данном журнале обязательно регистрируются: причины ситуации, ее продолжительность и значение параметров во время внештатной ситуации. При необходимости составляется акт и разрабатывается план необходимых корректирующих мер по исправлению критической ситуации.