Бекітемін
«Әбілқас Сағынов атындағы Қарағанды техникалық университеті» КеАҚ
Басқарма төрағасы – Ректоры
_____ Сагинтаева С.С.
Басқраманың «14» қаңтар 2026 ж.
№ 23 шешімі

ІШКІ НОРМАТИВТІК ҚҰЖАТ

АҚПАРАТТЫҚ ҚАУІПСІЗДІК ОҚИҒАЛАРЫНА ЖӘНЕ ШТАТТАН ТЫС (ДАҒДАРЫСТЫҚ) ЖАҒДАЙЛАРҒА ӘРЕКЕТ ЕТУ БОЙЫНША ПАЙДАЛАНУШЫЛАРДЫҢ ІС-ҚИМЫЛ ТӘРТІБІ ТУРАЛЫ НҰСҚАУЛЫҚ

ІНҚ ІІ-10-2026

Әзірлеген: Ақпараттық қауіпсіздік жөніндегі инженер
Д.К. Читян _____

Қарағанды

Құжатты рұқсатсыз көшіруге тыйым салынады

Мазмұны

1 Қолдану саласы 3

2 Нормативтік сілтемелер 3

3 Терминдер, анықтамалар және қысқартулар 4

4 Жауапкершілік және өкілеттіктер 4

5 Жалпы қағидалар 5

6 Штаттан тыс жағдай туындаған кездегі әрекеттердің жалпы тәртібі 6

7 Ең көп таралған штаттан тыс жағдайлар туындаған кездегі іс-әрекеттің ерекшеліктері 8

8 Үздіксіз жұмыс пен қалпына келтіруді қамтамасыз ету құралдары 10

9 Ақпараттық жүйелердің үздіксіз жұмысын қамтамасыз ету және қалпына келтіру жөніндегі қызметкерлердің міндеттері мен іс-әрекеттері 10

10 Штаттан тыс немесе дағдарыстық жағдайлардың туындауын және олар бойынша түзету әрекеттерін бақылау 11

11 Келісу, бекіту және қолданысқа енгізу 11

12 Сақтау 12

13 Қайта қарау және өзектендіру тәртібі 12

1-қосымша 14

Құжатты рұқсатсыз көшіруге тыйым салынады

1 Қолдану саласы

1.1 Осы Нұсқаулық ақпараттық қауіпсіздік оқиғалары анықталған және штаттан тыс (дағдарыстық) жағдайлар туындаған кезде «Әбілқас Сағынов атындағы Қарағанды техникалық университеті» КеАҚ Ақпараттық технологиялар департаменті мен Ақпараттық қауіпсіздік қызметі пайдаланушыларының, қызметкерлерінің іс-әрекеттерінің бірыңғай және орындалуы міндетті тәртібін белгілейді.

1.2 Нұсқаулық Университет қызметінде пайдаланылатын барлық автоматтандырылған ақпараттық жүйелерге, корпоративтік сервистерге, серверлік және желілік жабдыққа, деректерді сақтау жүйелеріне, жұмыс станцияларына, мобильді құрылғыларға, бағдарламалық қамтамасыз етуге және ақпарат тасымалдаушыларға қолданылады.

1.3 Нұсқаулықтың талаптары Университеттің ақпараттық ресурстарын пайдаланушылар, АТД және СИБ қызметкерлері үшін міндетті, сондай-ақ сыртқы провайдерлермен, мердігерлік ұйымдармен және өзге де үшінші тұлғалармен өзара іс-қимыл жасау кезінде қолданылады, егер оқиғалар Университеттің ақпараттық ресурстарына әсер етсе.

1.4 Нұсқаулық ақпараттың қолжетімділігіне, тұтастығына және құпиялылығына әсер ететін кез келген жағдайларда демалыс және мереке күндерін қоса алғанда, жұмыс уақытында да, жұмыстан тыс уақытта да қолданылады.

2 Нормативтік сілтемелер

2.1 Ережені әзірлеу кезінде пайдаланылған нормативтік құжаттар:

1) «Ақпараттандыру туралы» Қазақстан Республикасының 2015 жылғы 24 қарашадағы № 418-V Заңы.
2) ҚР СТ ИСО/МЭК 27002-2023 «Ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Ақпараттық қауіпсіздікті басқару шаралары».
3) ҚР СТ ИСО/МЭК 27001-2023 «Ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Ақпараттық қауіпсіздікті басқару жүйелері. Талаптар».
4) Қазақстан Республикасы Үкіметінің «Ақпараттық-коммуникациялық технологиялар және ақпараттық қауіпсіздікті қамтамасыз ету саласындағы бірыңғай талаптарды бекіту туралы» 2016 жылғы 20 желтоқсандағы № 832 Қаулысы.

2.2 Ереже Университеттің ішкі нормативтік құжаты болып табылады және Университеттің ақпараттық қауіпсіздік саясатына сәйкес келеді.

Құжатты рұқсатсыз көшіруге тыйым салынады

3 Терминдер, анықтамалар және қысқартулар

1) Университет – «Әбілқас Сағынов атындағы Қарағанды техникалық университеті» КеАҚ;

2) Нұсқаулық - ақпараттық қауіпсіздік оқиғаларына және Университеттің штаттан тыс (дағдарыстық) жағдайларына әрекет ету бойынша пайдаланушылардың іс-қимыл тәртібі туралы Нұсқаулық

3) Құпиясөзді бұзу – құпиясөздің ағуы немесе жария етілуі.

4) Ақпаратқа рұқсатсыз қол жеткізу (бұдан әрі – АРҚ) – есептеу техникасы құралдарымен немесе автоматтандырылған жүйелермен берілетін штаттық құралдарды пайдалана отырып, қол жеткізуді саралау қағидаларын бұзатын ақпаратқа қол жеткізу.

5) Прокси – қашықтағы пайдаланушылардың серверге қосылуын және сұраныстарын жүзеге асыратын бағдарламалық қамтамасыз ету.

6) Провайдер – **м**амандандырылған ақпараттық жүйелердің жабдықтарын орналастыру, Интернет желісіне қосу және жүйелерді сүйемелдеуге байланысты өзге де қызметтер көрсететін заңды тұлға (тұлғалар).

7) АТД – Ақпараттық технологиялар департаменті.

8) АҚҚ – Ақпараттық қауіпсіздік қызметі.

9) Қауіп - жүйеге немесе Серіктестікке зиян келтіруі мүмкін жағымсыз оқиғаның ықтимал себебі.

10) АЖ – ақпараттық жүйе (соның ішінде Университеттің жергілікті есептеу желісі);

11) БҚ – бағдарламалық қамтамасыз ету.

12) Жүйелік әкімші (бұдан әрі – ЖӘ) – әкімшілендіруге жауапты корпоративтік ақпараттық желінің серверлері мен қолданбалы белсенді жабдықтарын әкімшілендіру функцияларын орындайтын қызметкер:

- Университеттің ақпараттық жүйелерін;
- деректер базасының серверлерін (далее – ДБ);
- корпоративтік электрондық поштаны;
- proxy-серверді.

4 Жауапкершілік және өкілеттіктер

4.1 Ақпараттық технологиялар департаменті жедел техникалық ден қоюға, оқиғалардың салдарын оқшаулауға және жоюға, ақпараттық жүйелердің жұмысқа қабілеттілігін қалпына келтіруге және провайдерлермен өзара іс-қимылға жауап береді.

4.2 Ақпараттық қауіпсіздік қызметі оқиғаларды жіктеуді, себептерін талдауды, ақпараттық қауіпсіздік талаптарының сақталуын бақылауды, тергеуге

қатысуды және қайталама оқиғалардың алдын алу бойынша ұсыныстар дайындауды жүзеге асырады.

4.3 Жүйелік әкімшілер жүйелерді оқшаулау, қалпына келтіру және тестілеу бойынша техникалық іс-шараларды орындайды, іс-қимыл журналдарын жүргізеді және АТД және АҚҚ нұсқауларын орындауға міндетті.

4.4 Пайдаланушылар анықталған оқиғалар немесе күдікті белгілер туралы дереу хабарлауға, зардап шеккен ресурстармен жұмысты тоқтата тұруға және уәкілетті қызметкерлердің нұсқауынсыз салдарларды жою бойынша дербес іс-қимыл жасамауға міндетті.

4.5 Нұсқаулықтың талаптарын бұзуға жол берген адамдар Қазақстан Республикасының заңнамасына және Университеттің ішкі актілеріне сәйкес тәртіптік, әкімшілік немесе өзге де жауаптылықта болады.

5 Жалпы қағидалар

5.1 Ақпараттық қауіпсіздік инциденттеріне және штаттан тыс (дағдарыстық) жағдайларға ден қою Ақпараттық технологиялар департаменті мен Ақпараттық қауіпсіздік қызметінің басқаруымен орталықтандырылған түрде жүзеге асырылады. Барлық оқиғалар мен әрекеттер белгіленген тәртіппен міндетті түрде тіркелуге жатады.

5.2 Оқиға анықталған кезде пайдаланушы зардап шеккен ақпараттық ресурстармен жұмысты дереу тоқтата тұруға міндетті. Пайдаланушы оқиға белгілерін тіркейді, мүмкіндігінше скриншоттарды, қателер туралы хабарламаларды және басқа да қолжетімді деректерді сақтайды, содан кейін белгіленген байланыс арналары арқылы АТД пен АҚҚ-ні дереу хабардар етеді.

5.3 АТД қызметкерлері алынған ақпаратқа бастапқы талдау жүргізеді. Оқиға уақытты, хабарлама көзін және оқиғаның қысқаша сипаттамасын көрсете отырып, штаттан тыс жағдайларды тіркеу журналында тіркеледі.

5.4 Ақпараттық жүйелердің жұмысқа қабілеттілігіне елеулі әсер ету белгілері немесе ақпараттық қауіпсіздікті бұзу тәуекелдері болған кезде оқиғаның өршуі басталады. Туындаған жағдай туралы Университет басшылығы мен ақпараттық қауіпсіздік жөніндегі инженер хабардар етіледі.

5.5 Оқиғаның сипаты мен сыни деңгейіне байланысты салдарды оқшаулау және азайту бойынша іс-шаралар орындалады. Мұндай іс-шараларға зардап шеккен компоненттерді оқшаулау, кіруді шектеу, қызметтерді уақытша өшіру немесе резервтік ресурстарға көшу жатады.

5.6 АТД қызметкерлері жабдықтар мен бағдарламалық қамтамасыз етуді қалпына келтіру бойынша жұмыстарды орындайды. Қажет болған жағдайда деректерді резервтік көшірмелерден қалпына келтіру олардың тұтастығын және ақпараттық жүйелердің дұрыс жұмыс істеуін кейіннен тексере отырып жүзеге асырылады.

Құжатты рұқсатсыз көшіруге тыйым салынады

5.7 Оқиға жойылғаннан кейін барлық тәуелді сервистердің жұмысқа қабілеттілігін тексеру жүргізіледі. Ақпараттық жүйелерді одан әрі пайдалануға әсер ететін қалдық салдардың жоқтығы расталады.

5.8 Әрекет ету барысында орындалған барлық іс-әрекеттер құжатталуға жатады. Жұмыстар аяқталғаннан кейін оқиғаның сипаттамасын, оның пайда болу себептерін талдауды, орындалған іс-шаралар тізбесін және болашақта осындай жағдайлардың алдын алу бойынша ұсыныстарды қамтитын есеп жасалады.

5.9 Қызметкерлердің ақпараттық қауіпсіздік оқиғасына және штаттан тыс жағдайларға әрекет ету дайындығын арттыру үшін оқыту іс-шаралары өткізіледі. Әрекет ету сценарийлерін оқыту және жаттығу пысықтау жылына кемінде бір рет ұйымдастырылады.

5.10 Осы Нұсқаулықтың шеңберінде штаттан тыс (дағдарыстық) жағдайлар деп ақпараттың қолжетімділігін, тұтастығын немесе құпиялылығын бұзуға әкеп соғатын немесе ықтимал әкеп соғуы мүмкін оқиғалар түсініледі.

5.11 Мұндай жағдайларға сервермен немесе сервистермен байланыстың ұзақ уақыт болмауы, бағдарламалық жасақтаманың істен шығуы, құпиясөздердің бұзылуы, серверлік немесе желілік жабдықтың істен шығуы, ақпараттың жоғалуы немесе ағуы, рұқсатсыз кіру әрекеттері, зиянды немесе зиянды кодты анықтау жатады.

5.12 Сондай-ақ штаттан тыс жағдайларға байланыс арналарының істен шығуы, ақпаратты өңдеуге кедергі келтіретін электр энергиясын берудің бұзылуы, сондай-ақ өрттер, су тасқыны, дауылдар мен жер сілкіністерін қоса алғанда, табиғи-климаттық әсерлер жатады.

5.13 Штаттан тыс жағдайлардың туындауы туралы ақпарат көздеріне ДИТ-ке берілетін пайдаланушылардың хабарламалары және ақпараттық жүйелерді пайдалануды жүзеге асыратын қызметкерлердің хабарламалары жатады.

5.14 Қосымша көздер мониторинг пен хабарлаудың автоматтандырылған жүйелері, сондай-ақ бұзушылықтар, іркілістер немесе күдікті белсенділік туралы мәліметтерді қамтитын жүйелік журналдар мен оқиғалар журналдары болып табылады.

5.15 Барлық анықталған ақпарат көздері оқиғаны жедел сәйкестендіру, оны жіктеу және ден қою және қалпына келтіру бойынша негізделген шешімдер қабылдау үшін пайдаланылады.

6 Штаттан тыс жағдай туындаған кездегі іс қимылдардың жалпы тәртібі

6.1 Пайдаланушы, штаттан тыс жағдай туындаған жағдайда:

1) жұмысын тоқтатады;
2) АТД мен АҚҚ дереу хабардар етеді;
3) басшылықты хабардар етеді;

4) штаттан тыс жағдайлар бойынша АТД қызметкерлерінің рұқсатынан кейін және (немесе) ақпараттық қауіпсіздік жөніндегі инженердің рұқсатынан кейін ғана жұмысты қайта бастайды.

6.2 АТД қызметкерлері, ақауды жедел түрде жояды, егер мүмкін болса, АТД басшысын, ақпараттық қауіпсіздік жөніндегі инженерді хабардар етеді және штаттан тыс жағдайлардың пайда болу фактісін штаттан тыс жағдайларды тіркеу журналында тіркейді (оның нысаны осы Нұсқаулықтың 1-қосымшасында келтірілген).

6.3 Университеттің бизнес-процестерін жүзеге асыруға елеулі әсер етуі мүмкін штаттан тыс жағдай туындаған жағдайда АТД қызметкері:

1) штаттан тыс жағдайлардың туындағаны туралы Университет басшылығына, сондай-ақ ақпараттық қауіпсіздік жөніндегі инженерге хабарлайды;

2) штаттан тыс жағдайдың ауқымын, ықтимал зақымдану көлемін және аймағын анықтайды;

3) зардап шеккен компоненттерді өшіреді немесе резервтік ресурстарды пайдалануға ауысады;

4) зақымдалған сыни аппараттық құралдар мен басқа да жабдықтардың жұмысқа қабілеттілігін қалпына келтіреді, қажет болған жағдайда істен шыққан тораптар мен блоктарды резервтік қондырғылармен ауыстыруды жүргізеді;

5) эталондық көшірмелерді қолдана отырып, бүлінген бағдарламалық жасақтаманы қалпына келтіреді;

6) сақтық көшірмелерді пайдалана отырып, қажетті ақпаратты қалпына келтіреді;

7) қалпына келтірілген жүйенің жұмыс қабілеттілігін тексереді, штаттан тыс жағдайдың салдары жүйенің одан әрі жұмысына әсер етпейтініне көз жеткізеді;

8) АТД басшысын штаттан тыс жағдайды жою туралы хабардар етеді;

9) штаттан тыс жағдайды штаттан тыс жағдайларды тіркеу журналына тіркейді.

10) ақпараттық қауіпсіздік жөніндегі инженерге штаттан тыс жағдай туралы есеп береді.

6.4 Бағдарламалық қамтамасыз етуді орнату және баптау немесе желілік жабдықты ауыстыру үшін есептеу техникасының құралдарына функционалдық міндеттеріне сәйкес АТД қызметкерлері ғана қол жеткізе алады.

6.5 Штаттан тыс жағдайды жойған АТД қызметкерлері жағдайды сипаттайтын акт жасайды. Актіге түсіндірме материалдар (скриншоттар, оқиғалар журналын басып шығару және т.б.) қоса беріледі.

6.6 Әрбір штаттан тыс жағдайды ақпараттық қауіпсіздік инженері талдайды. Осы талдау нәтижелері бойынша басшылыққа болашақта штаттан тыс жағдайлардың алдын алуға бағытталған ықтимал ұйымдастырушылық және техникалық іс-шаралар бойынша ұсыныстар әзірленеді және ұсынылады.

Құжатты рұқсатсыз көшіруге тыйым салынады

6.7 Қажет болған жағдайда Университет басшылығының шешімі бойынша оның себептерін анықтау, келтірілген залалды бағалау, кінәлі адамдарды анықтау және тиісті ықпал ету шараларын қабылдау мақсатында штаттан тыс жағдайдың туындау фактісі бойынша қызметтік тергеу жүргізілуі мүмкін.

7 Ең көп таралған штаттан тыс жағдайлар туындаған кездегі іс-әрекеттің ерекшеліктері

7.1 Провайдерде орналасқан бір немесе бірнеше серверлермен байланыс болмаған кезде жүйелік әкімші байланыстың болмау себептерін дереу анықтайды және қажет болған жағдайда осы Нұсқаулыққа сәйкес іс-шаралар жүргізіледі.

7.2 Бағдарламалық жасақтама істен шыққан кезде АТД қызметкерлері ақаулықтың себебін анықтайды. Егер қатені өз бетімен, соның ішінде бағдарламалық жасақтама жасаушымен кеңескеннен кейін түзету мүмкін болмаса, акт пен ілеспе материалдардың (сондай-ақ қажет болған жағдайда файлдардың) көшірмесі бағдарламалық жасақтама жасаушыға жіберіледі.

7.3 Құпиясөз бұзылған кезде Университеттің құпиясөзді қорғауды ұйымдастыру Ережесін сақтау қажет.

7.4 Компьютерлік вирус анықталған кезде вирусқа қарсы бақылауды ұйымдастыру Ережелерін басшылыққа алу қажет.

7.5 Сервер немесе желілік жабдық істен шыққан кезде жүйелік әкімші:

1) сервердің немесе желілік жабдықтың істен шыққан компоненттерін өшіруге;

2) үздіксіз жұмысты қамтамасыз ету үшін резервтік серверді немесе желілік жабдықты олар болған кезде дереу іске қосу жөнінде шаралар қабылдауға;

3) деректер мен бағдарламалық қамтамасыз етудің жоғалуына және/немесе тұтастығының бұзылуына талдау жүргізуге;

4) зақымдалған жабдықтың жұмыс қабілеттілігін тексеруге;

5) серверлік немесе желілік жабдықтың бүлінген компоненттерінің немесе сервистерінің жұмыс қабілеттілігін қалпына келтіруге (қажет болған жағдайда бағдарламалық қамтамасыз етуді және актіні жасай отырып, резервтік көшірмелерден деректерді қалпына келтіру) міндетті.

7.6 Пайдаланушылардың серверлерінде немесе дербес компьютерлерінде ақпараттың жоғалғаны немесе ағып кеткені анықталған жағдайда, АТД қызметкері ақпараттық қауіпсіздік жөніндегі инженердің қатысуымен ақпараттың жоғалу себептерін іздеу және жою бойынша іс-шаралар жүргізеді (БҚ мен есептеу техникасы құралдарының тұтастығы мен жұмысқа қабілеттілігін тексеру), қажет болған жағдайда резервтік көшірмелерден ақпарат қалпына келтіріледі. Егер ақпараттың ағуы техникалық себептер бойынша орын

алса, ақпараттың қорғалуына талдау жүргізіледі, осалдықтардың туындауын жою және алдын алу бойынша шаралар қабылданады.

7.7 Тіркеу құралдарымен тіркелген РК әрекеті кезінде ақпараттық қауіпсіздік жөніндегі инженер тіркеу журналдарында ақпаратқа талдау жүргізеді және талдау нәтижелері бойынша РК-ге нақты қауіп төнген жағдайда РК-ні болдырмау бойынша мынадай шаралар қабылданады:

1) құпиясөздерді жоспардан тыс толық ауыстыру жүргізіледі;

2) қауіпсіздік жүйесінің осалдығын жоятын бағдарламалық қамтамасыз етудің қолда бар жаңартуы қолданылады.

7.8 РК немесе АЖ бұзу анықталған жағдайда мынадай іс-шаралар жүргізіледі:

1) жүйелік әкімшілер және ақпараттық қауіпсіздік жөніндегі инженер РК мән-жайларына жедел талдау жүргізеді, оның нәтижелері бойынша инцидентті тексеру аяқталғанға дейін АЖ пайдалануды жалғастыру мүмкіндігі туралы шешім қабылданады.

2) қажет болған жағдайда АЖ және БҚ-ны зиянды кодтың бар-жоғын тексеру үшін серверді желіден ажырату немесе серверді тоқтату жүргізіледі. Резервтік серверге уақытша көшу мүмкін.

3) кейіннен талдау үшін резервтік көшіру құралдарымен жүйенің көшірмесі жасалады.

4) ақпараттық қауіпсіздік жөніндегі инженер серверді тіркеу журналдарына және ақпаратты қорғау құралдарын тіркеу журналдарына талдау жүргізеді.

5) серверлерге қатысы бар құпиясөздерді жоспардан тыс ауыстыру жүргізіледі.

7.9 Байланыс арналары істен шыққан кезде жүйелік әкімші байланыс қызметтерін жеткізушіні хабардар етеді, байланыс арнасын қалпына келтіру мәселесін пысықтайды, олар болған жағдайда қосалқы байланыс арналарына көшу жөнінде шаралар қабылдайды.

7.10 Электр энергиясы 10 минуттан артық ажыратылған жағдайда және үздіксіз қоректендіру көздерін пайдалану мүмкін болмаған жағдайда, АТҚ қызметкеріне барлық серверлер мен желілік жабдықтарды дұрыс ажырату қажет. Университет ғимаратында электр энергиясын беру кезінде ақпараттық қауіпсіздік жөніндегі инженер АТД қызметкерлерімен бірлесіп сервердегі деректер мен БҚ шығындарының және (немесе) бұзылуының бар-жоғына талдау жүргізеді, сондай-ақ жабдықтың жұмысқа қабілеттілігін тексереді. Қажет болған жағдайда актіні жасай отырып, соңғы резервтік көшірмеден БҚ мен деректерді қалпына келтіру жүргізіледі.

7.11 Кеңседе немесе провайдердің аумағында орналасқан жабдықты электрмен қоректендірудің істен шығуы анықталған жағдайда, АТД қызметкері уәкілетті қызметкерлерді дереу хабардар етеді. Егер электр қуатының істен шығуын жоюдың болжамды уақыты 30 минуттан асса, АТД қызметкері Университет басшылығына хабарлайды. Электр қуатын беруді қайта бастаған

кезде жүйелік әкімші жабдықтың тұтастығын тексеру бойынша іс-шаралар жүргізеді.

7.12 Апаттың табиғи-климаттық әсер (жер сілкінісі, су тасқыны, дауыл, өрт және т.б.) туындаған кезде резервтік көшірмелерге жауапты жүйелік әкімшілер мен ақпараттық қауіпсіздік жөніндегі инженер мүмкіндігінше жүйенің соңғы толық көшірмесін сақтауды қамтамасыз етуі тиіс.

7.13 Табиғи апаттар кезінде қызметкерлердің нақты іс-қимылдарын әзірлеу үшін ақпараттық қауіпсіздік жөніндегі инженер жылына кемінде бір рет арнайы оқыту жаттығуларын ұйымдастыруы тиіс.

8 Үздіксіз жұмыс пен қалпына келтіруді қамтамасыз ету құралдары

8.1 Осы Нұсқаулық шеңберінде техникалық сипаттағы штаттан тыс жағдайлардың туындау тәуекелдері қарастырылады.

8.2 Техногендік әсер етудің және табиғи апаттардың штаттан тыс жағдайларының туындау тәуекелдері Төтенше жағдайларға жатады және «Ақпаратты өңдеу құралдарымен байланысты активтердің үздіксіз жұмысын қамтамасыз ету жөніндегі ереже» құжатында қаралады.

8.3 Үздіксіз жұмыс пен қалпына келтіруді қамтамасыз ету құралдары:

1) БҚ және Университеттің ақпараттық ресурстарының резервтік көшірмесі;

2) кластерлік шешімді қолдану (кластерлерді пайдалану);

3) үздіксіз қоректендіру көздері.

8.4 Резервтік көшірме ақпарат жоғалған жағдайда ақпаратты қалпына келтіруді қамтамасыз етеді. Резервтік көшіру ақпараттың Резервтік көшірмесін жасау және қалпына келтіру регламентінің талаптарына сәйкес орындалады.

8.5 Кластерлерді қолдану пайдаланылатын жабдықтың сенімділігін арттыруды қамтамасыз етеді. Кластерлік шешімді қолданудың орындылығы ақпараттық жүйенің аппараттық архитектурасын анықтау немесе өзгерту кезеңінде анықталады.

8.6 Үздіксіз қуат көздері электр тогының параметрлері рұқсат етілген параметрлерден ажыратылған немесе шыққан жағдайда, қосылған жабдықты аккумуляторлардан біраз уақыт жұмыс істеумен қамтамасыз етеді.

9 Ақпараттық жүйелердің үздіксіз жұмысын қамтамасыз ету және қалпына келтіру жөніндегі қызметкерлердің міндеттері мен іс-әрекеттері

9.1 Дағдарыс жағдайындағы қызметкерлердің әрекеттері оның ауырлығына байланысты.

9.2 Қауіпті немесе ауыр дағдарыс жағдай туындаған жағдайда персоналдың іс-әрекеттері мынадай кезеңдерді қамтиды:

1) жауапты қызметкерлердің жедел реакциясы;

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

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

4) дағдарыс жағдайының туындау себептерін тергеу және кінәлілерді анықтау;

5) тәуліктің күндізгі уақытында штаттан тыс (дағдарыстық) жағдайды анықтаған қызметкер өзінің тікелей басшысын, АТД қызметкерлерін және ақпараттық қауіпсіздік жөніндегі инженерді ауызша, қажет болған жағдайда жазбаша хабардар етуге тиіс;

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

9.3 Университет ғимаратты күзететін қызметті келесі қажеттілікке жеткізеді: түнгі уақытта штаттан тыс жағдай туындаған кезде қауіпсіздікке жауапты күзетші АТД немесе АҚҚ жауапты қызметкеріне хабарлауы керек.

9.4 АЖ пайдалануды жүзеге асыратын қызметкерлер ақпараттық қауіпсіздік жөніндегі инженерге штаттан тыс жағдайлардың туындауының барлық байқалған алғышарттары туралы хабарлауға міндетті.

9.5 Дағдарыс жағдайларында жұмыстарды ұйымдастыруды оларға жүктелген міндеттер шеңберінде АТД және АҚҚ қызметкерлері жүзеге асырады.

9.6 Дағдарыс жағдайларында жұмыстарды ұйымдастыруды бақылауды университет басшылығы жүзеге асырады.

10 Штаттан тыс немесе дағдарыстық жағдайлардың туындауын және олар бойынша түзету әрекеттерін бақылау

10.1 Штаттан тыс жағдайлардың пайда болуын бақылау келесі функциялардың көмегімен жүзеге асырылады:

1) штаттан тыс жағдайлардың туындауын штаттан тыс жағдайларды тіркеу журналында тіркеу;

2) штаттан тыс жағдайды және түзету әрекеттерін сипаттай отырып, олардың түпнұсқалығын растайтын құжаттамада тіркелген түсіндірме материалдарды (скриншоттар, оқиғалар журналының басып шығарулары және т. б.) қоса бере отырып, актілер жасау.

11 Келісу, бекіту және қолданысқа енгізу

11.1 Осы Нұсқаулық қызметі ақпараттық жүйелерді пайдаланумен, ақпаратты өңдеумен және ақпараттық қауіпсіздікті қамтамасыз етумен байланысты университеттің құрылымдық бөлімшелерінің басшыларымен міндетті түрде келісуге жатады. Егер Нұсқаулықтың ережелері материалдық жауапкершілік, шарттық міндеттемелер не қаржылық есепке алу мәселелерін

қозғаған жағдайда, келісу қосымша бухгалтерлік және қаржылық есепке алуды жүзеге асыратын бөлімшемен жүзеге асырылады.

11.2 Нұсқаулықты келісу талап етілетін лауазымды тұлғалар мен құрылымдық бөлімшелердің тізбесін құжатты әзірлеуші оның мазмұнын, қолдану саласын және университет қызметіне ықтимал ықпалын ескере отырып айқындайды.

11.3 Нұсқаулықтың жобасын қарау мерзімі оны келісуші тұлғалар алған сәттен бастап бес жұмыс күнінен аспауға тиіс. Ескертулер мен ұсыныстар жазбаша нысанда ресімделеді, дәлелді болуға және құжаттың ережелерін түзету бойынша нақты ұсыныстарды қамтуға тиіс.

11.4 Ескертулер болмаған кезде не олар есепке алынғаннан кейін нұсқаулыққа келісуші тұлғалар қол қояды және атқарушы органға Басқармаға бекітуге беріледі.

11.5 Нұсқаулықтың қолданысқа енгізілген күні оның бекітілген күні болып есептеледі. Бекітілген сәттен бастап Нұсқаулық оның қолданысы қолданылатын барлық пайдаланушылар мен қызметкерлер үшін міндетті болып табылады.

11.6 Нұсқаулықтың жаңа редакциясын бекіту немесе өзгерістер енгізу кезінде құжаттың алдыңғы нұсқасы күшін жояды және жарамсыз деп есептеледі.

12 Сақтау

12.1 Осы Нұсқаулықтың бекітілген түпнұсқасы Университеттің Ақпараттық қауіпсіздік қызметінде сақталады.

12.2 Нұсқаулықтың электрондық нұсқасы мүдделі құрылымдық бөлімшелер мен уәкілетті қызметкерлер үшін қолжетімділікті қамтамасыз ете отырып, университеттің корпоративтік ақпараттық ресурстарында орналастырылады.

12.3 Университет қызметкерлерін осы Нұсқаулықпен таныстыру ішкі нормативтік құжаттар үшін белгіленген тәртіппен танысу парағын ресімдеумен жүзеге асырылады.

12.4 Көшірмелерді есепке алу, рұқсатсыз пайдаланудың алдын алу және құжаттың құрылымдық бөлімшелерде сақталуына олардың басшылары жауапты болады.

13 Қайта қарау және өзектендіру тәртібі

13.1 Осы Нұсқаулықты қайта қарауды ақпараттық қауіпсіздік қызметі кемінде екі жылда бір рет жүзеге асырады және құжат талаптарын ақпараттық жүйелерді пайдаланудың ағымдағы шарттарына, АТ-инфрақұрылымын дамытуға және Университеттің Ақпараттық қауіпсіздікті басқару жүйесінің талаптарына сәйкес келтіруге бағытталған.

13.2 Нұсқаулықты жоспардан тыс өзектендіру Ақпараттық қауіпсіздікті басқару жүйесінің АҚБЖ-нің қолданылу саласы өзгерген кезде, Қазақстан

Республикасы заңнамасының және ақпараттық қауіпсіздік саласындағы стандарттардың талаптары өзгерген кезде, криптографиялық қорғаудың жаңа құралдары енгізілген кезде, сондай-ақ инциденттердің, ішкі тексерулер мен ақпараттық қауіпсіздік аудиттерінің нәтижелері бойынша жүргізіледі.

13.3 Осы Нұсқаулыққа өзгерістер мен толықтырулар жаңа редакция не жекелеген өкімдік құжат түрінде ресімделеді және осы Нұсқаулықты бекіту үшін белгіленген тәртіппен бекітіледі.

Құжатты рұқсатсыз көшіруге тыйым салынады

Ақпараттық қауіпсіздік оқиғаларына және штаттан тыс (дағдарыстық) жағдайларға әрекет ету бойынша пайдаланушылардың іс-қимыл тәртібі туралы нұсқаулыққа **1-қосымша**
«__» _____ 20__ ж. № __

Штаттан тыс жағдайларды тіркеу журналы

№	Күні	Штаттан тыс жағдайдың қысқаша сипаттамасы	Басталу уақыты	Аяқталу уақыты	Іркіліс	Себебі	Жою әдісі	Жауапты

Ф.01-2022

Келісу парағы

Лауазымы	Аты-жөні	Күні	Қолы
Басқарма мүшесі – Цифрландыру жөніндегі проректор	Амиров А.Ж.	9.12.25	
Заң қызметінің басшысы	Аязбаева Г.С.	9.12.25	
Software-орталығының басшысы	Штефан К.Б.	9.12.25	

Ф.02-2022

Танысу парағы

Лауазымы	Аты-жөні	Күні	Қолы

Құжатты рұқсатсыз көшіруге тыйым салынады