«Академик Е.А. Бөкетов атындағы Қарағанды университеті» ҚЕАҚ

«Академик Е.А. Бөкетов атындағы
Қарағанды университеті» ҚЕАҚ
Директорлар кеңесінің шешімімен
(№3 Хаттама 19.03.2021 жылғы)
БЕКІТІЛДІ

«АКАДЕМИК Е.А. БӨКЕТОВ АТЫНДАҒЫ ҚАРАҒАНДЫ УНИВЕРСИТЕТІ» КЕАҚ АҚПАРАТТЫҚ ҚАУІПСІЗДІК ЖӨНІНДЕГІ ЕРЕЖЕСІ

2021 ж.

МАЗМҰНЫ

1.	Терминдер олардың анықтамалары, қысқартулары және нормативтік сілтемелер	3
2.	Негізгі мақсаттары	4
3.	Қолдану саласы	5
4.	АҚ ережесі	5
5.	АҚ қамтамасыз етуді ұйымдастыру	5
6.	АЖ пайдаланушылар санаттары	5
7.	АҚ объектілері	6
8.	Қорғауға жататын АР санаттары	6
9.	АҚ ережесін іске асыру жөніндегі шаралар	6
10.	АҚ және ЖӘ үшін жауапты тұлғаның ұйымдық-құқықтық мәртебесі	7
11.	Құпиялылықтың жалпы талаптары	7
12.	Жүйеде пайдаланушыларды аутентификациялау бойынша талаптар	8
13.	Байланыс желілері бойынша ақпарат беру кезіндегі құпиялылық талаптары	8
14.	Жалпыға қолжетімді ресурстарды қорғауды ұйымдастыру жөніндегі талаптар	8
15.	Тұтастықтың жалпы талаптары	9
16.	АЖ әзірлеу, жетілдіру және қызмет көрсету кезіндегі қауіпсіздік талаптары	9
17.	АҚ желісін қамтамасыз ету компоненттеріне қойылатын талаптар	9
18.	Қауіпсіздік инциденттерін басқаруға қойылатын талаптар	10
19.	Ақпаратты рұқсатсыз қолжетімділіктен қорғауға қойылатын талаптар	10
20.	Электрондық поштаны және интернетті қолдануға қойылатын талаптар	10
21.	Резервтік көшіруге және қалпына келтіруге қойылатын талаптар	11
22.	Вирусқа қарсы қауіпсіздікке қойылатын талаптар	11
23.	Қолжетімділіктің жалпы талаптары	11
24.	Істен шығуды болдырмауға қойылатын талаптар	11
25.	Тәуекелдерді талдау мен бағалауға қойылатын талаптар	11
26.	Қолданылатын қорғау шараларының тиімділігін бақылау	12
27.	АҚ ережесін қайта қарау	12
28.	Жауапкершілік	13

1. Терминдер олардың анықтамалары, қысқартулары және нормативтік сілтемелер

Осы Ақпараттық қауіпсіздік жөніндегі ережеде (бұдан әрі – АҚ ережесі) мынадай терминдер, олардың анықтамалары мен қысқартулары қолданылды:

1.1. **аутентификация** – жүйеде іске асырылған қолжетімділіктің ұсынылған деректемелерінің сәйкестігін айқындау арқылы қол жеткізу субъектісінің немесе объектісінің түпнұсқалығын растау;

1.2. **деректер базасы (ДБ)** – осы деректердің сипаттамаларын, сондай-ақ олардың объектілері арасындағы өзара байланысты сипаттайтын тұжырымдамалық құрылымға сәйкес ұйымдастырылған деректер жиынтығы;

1.3. **ақпараттық қауіпсіздік деңгейлері бойынша ақпараттық жүйені градациялау** – ақпараттық қауіпсіздікті қамтамасыз ету бойынша оларға қойылатын талаптар деңгейі бойынша ақпараттық жүйені сыныптарға бөлу;

1.4. **Ақпараттық ресурстар (АР)** – ақпараттық жүйелерде сақталатын мәтін, рафика; аудио-; бейне- және т.б. деректердің жиынтығы;

1.5. **ақпараттық жүйе (АЖ)** – аппараттық-бағдарламалық кешенді қолдана отырып, ақпаратты сақтауға, өңдеуге, іздеуге, таратуға, беруге және ұсынуға арналған жүйе;

1.6. **ақпараттық қауіпсіздік (АҚ)** – ақпараттың немесе оны өңдеу құралының құпиялылығын, тұтастығын, қолжетімділігін, істен шығуына тұрақтылығын, есептілігін, түпнұсқалығы мен анықтығын айқындауға, оған қол жеткізуге және қолдауға байланысты барлық аспектілер;

1.7. **электрондық ақпараттық ресурстар (ЭАР)** – тиісті бағдарламалық қамтылыммен біріктірілген және ақпаратты пайдаланушылар үшін қызығушылық тудыратын АЖ-да қамтылған электрондық жүйелендірілген ақпарат массивтері (ақпараттық ДБ);

1.8. **ақпараттық-коммуникациялық инфрақұрылым (АКИ)** – есептеу техникасы құралдарының, телекоммуникациялық жабдықтардың, деректерді беру арналары мен АЖ, коммутация және ақпараттық ағындарды басқару құралдарының жиынтығы;

1.9. **жергілікті-есептеу желісі (ЖЕЖ)** – шағын аумақ шегінде орналасқан абоненттерді біріктіретін желі;

1.10. **ақпаратқа рұқсатсыз қолжетімділік (АРҚ)** – есептеу техникасы құралдары немесе автоматтандырылған жүйелер ұсынатын штаттық құралдарды пайдалана отырып, қолжетімділікті шектеу қағидаларын бұзатын ақпаратқа қол жеткізу;

1.11. **нормативтік құқықтық актілер (НҚА)** – лауазымды адам(дар) қабылдаған, құқықтық нормаларды белгілейтін, олардың қолданылуын өзгертетін, тоқтататын немесе тоқтата тұратын белгіленген нысандағы жазбаша ресми құжат, сондай-ақ жазбаша ресми құжатқа ұқсас және электрондық цифрлық қолтаңба арқылы куәландырылған электрондық-цифрлық нысандағы құжат;

1.12. **АЖ пайдаланушы** – өзіне қажетті электрондық АР алу үшін АЖ-ға жүгінетін және оларды пайдаланатын субъект;

1.13. **бағдарламалық қамтылым (БҚ)** – осы бағдарламаларды пайдалану үшін қажетті ақпаратты және бағдарламалық құжаттарды өңдеу жүйесінің компьютерлік бағдарламаларының жиынтығы;

1.14. **қолданбалы БҚ (ҚБҚ)** – қолданбалы міндетті шешуге арналған БҚ (немесе бағдарлама);

1.15. «Е.А. Бөкетов атындағы Қарағанды университеті» КЕАҚ (бұдан әрі – Университет);

1.16. **Ақпараттық технологиялар және телекоммуникациялар орталығы (АТжТО)** – байланыс арналарын техникалық сүйемелдеуді және оларға қызмет көрсетуді, компьютерлік жабдық пен базалық БҚ-ның жұмыс істеуін қамтамасыз етеді;

1.17. **серверлік бөлме** – серверлік, белсенді және пассивті желілік (телекоммуникациялық) жабдықты және құрылымдалған кабельдік жүйелердің жабдығын орналастыруға арналған үй-жай;

1.18. **деректер базасын басқару жүйесі (ДББЖ)** – деректер базасын басқаруды қамтамасыз ететін бағдарламалық және тілдік құралдар жиынтығы;

1.19. **жүйелік БҚ** – есептеу жабдықтарының жұмысын қамтамасыз етуге арналған компьютерлік бағдарламалар жиынтығы;

1.20. **жүйелік әкімші (ЖӘ)** – сервердің дұрыс жұмыс істеуі және сервердегі БҚ параметрлері

үшін жауапты тұлға;

1.21. **мамандандырылған БҚ** – қосалқы және сервистік міндеттерді шешу үшін қолданылатын компьютерлік бағдарламалар;

1.22. **есептеу техникасы құралдары (ЕТҚ)** – дербес немесе басқа жүйелердің құрамында жұмыс істеуге қабілетті ақпаратты өңдеу, оның ішінде енгізу немесе шығару жүйелерінің бағдарламалық және техникалық элементтерінің жиынтығы;

1.23. **интернет желісі** – халықаралық ресурстарға қол жеткізуді қамтамасыз ететін желілер жүйесі;

1.24. Осы АҚ ережесін әзірлеу кезінде пайдаланылған негізгі НҚА, мемлекеттік және халықаралық стандарттар:

1) «Ақпараттық-коммуникациялық технологиялар және ақпараттық қауіпсіздікті қамтамасыз ету саласындағы бірыңғай талаптарды бекіту туралы» Қазақстан Республикасы Үкіметінің 2016 жылғы 20 желтоқсандағы № 832 қаулысы;

2) «Ғимараттар мен құрылыстардың өрт қауіпсіздігі» ҚР ҚНжЕ 2.02-05-2009;

3) «Құрылымдық кабельдік желілер. Жобалау нормалары» ҚР ҚН 3.02-17-2011;

4) «Ақпараттық технология. Негізгі терминдер мен анықтамалар» ҚР СТ 34.005-2002;

5) «Ақпараттық технология. Деректер базасы. Негізгі терминдер мен анықтамалар» ҚР СТ 34.006-2002;

6) «Ақпараттық технология. Телекоммуникациялық желілер. Негізгі терминдер мен анықтамалар» ҚР СТ 34.007-2002;

7) «Ақпараттық технология. Қорғауды қамтамасыз ету әдістері. Ақпаратты қорғауды басқару жөніндегі қағидалар жиынтығы» ҚР СТ ИСО/МЭК 17799-2006;

8) «Ақпараттық технология. Қамту құралдары. Ақпаратты қорғауды басқару жөніндегі қағидалар жиынтығы» ҚР СТ ИСО/МЭК 27002-2009;

9) «Ақпараттық технология. Қамту құралдары. Ақпаратты қорғауды басқару жөніндегі қағидалар жиынтығы» ҚР СТ ИСО/МЭК 27002-2015.

2. Негізгі мақсаттары

2.1. Осы АҚ ережесі Университеттің ақпараттық-коммуникациялық инфрақұрылымының (бұдан әрі – АКИ) қазіргі жай-күйін және оны дамытудың таяу перспективаларын, пайдалану мақсаттарын, міндеттері мен құқықтық негіздерін, жұмыс істеу режимдерін, сондай-ақ оның ресурстары үшін қауіпсіздік қатерлерін талдауды ескереді.

2.2.АҚ ережесінің негізгі мақсаттары:

1) өңделетін ақпараттың қолжетімділігі;

2) Университеттің АКИ-нің тұрақты жұмыс істеуі;

3)ЕТҚ сақтайтын, өңдейтін және байланыс арналары арқылы берілетін ақпараттың құпиялылығын қамтамасыз ету;

4) Университеттің АЖ-да сақталатын және өңделетін және байланыс арналары арқылы берілетін ақпараттың тұтастығы мен тұтынушылығы.

2.3.Мақсаттарға жету үшін келесі міндеттер қойылған:

1) Университетте АҚ қамтамасыз ету саласында бірыңғай саясатты қалыптастыру және жүргізу;

2) университеттің үздіксіз жұмысын қамтамасыз ету және олардың алдын алу, болдырмау және/немесе салдарын барынша азайту арқылы АҚ қатерлерін іске асырудан экономикалық залалды барынша азайту;

3) ақпарат қауіпсіздігіне әртүрлі қауіп-қатерлерді іске асыру салдарларын анықтауға, көрсетуге және жоюға бағытталған рәсімдерді айқындау;

4) АҚ қамтамасыз ету міндеттерін шешу қажеттілігін ескере отырып, Университет шеңберінде ақпараттандыруды басқару рәсімдерінің мазмұнына қойылатын талаптарды айқындау;

5) АҚ қамтамасыз ету стандарттарының талаптарын сақтай отырып, АКИ-де жұмыс жүргізу кезінде Университеттің қызметін үйлестіру;

6) Университет АКИ-інің қорғалу деңгейін арттыру;
7) АҚ-ны басқару АҚ ережесі негізінде құрылады.

3. Қолдану саласы

3.1.Осы АҚ ережесі ақпаратты, оның ішінде әкімшілік деректерді, таралуы шектеулі ақпаратты (қызметтік ақпарат) қамтитын автоматтандырылған ақпаратты немесе дербес деректерді өңдеу жүзеге асырылатын Университеттің құрылымдық бөлімшелеріне, сондай-ақ Университеттің АЖ-сын әзірлеуді, сүйемелдеуді, оның жұмыс істеуіне қызмет көрсетуді жүзеге асыратын ұйымдарға қолданылады.

3.2. Басқа АЖ АҚ-ның қолданылу саласын олардың иелері айқындайды. Егер АЖ деректері университеттің АКИ-на енгізілген жағдайда, АҚ талаптары АҚ шарттары немесе АЖ иесі мен университет арасындағы өзара іс-қимылдың бірлескен қағидалары шеңберінде келісіледі.

4. АҚ ережесі

4.1.Осы АҚ ережесі Қазақстан Республикасының АҚ саласындағы заңнамасының қағидаттары мен талаптарына және ұсынымдарына сәйкес, оның ішінде осы АҚ ережесінің 1-бөлімінің 1.24-тармағында санамаланған құжаттарға негізделе отырып әзірленді.

4.2.АҚ қамтамасыз ету деп ақпараттың құпиялылығын, тұтастығын және қолжетімділігін сақтау түсініледі. Ақпараттың құпиялылығы ақпаратқа тек авторландырылған адамдарға қол жеткізуді ұсыну жолымен, тұтастығы – деректерге тек авторландырылған өзгерістерді енгізу жолымен, қолжетімділік –авторландырылған адамдарға олардың қызметтік міндеттерін орындау үшін деректерге қол жеткізуді ұсыну жолымен қамтамасыз етіледі.

4.3.Университеттің АҚ ережесі мыналар үшін әдістемелік база болып табылады:

1) ақпаратты қорғауға бағытталған келісілген нормативтік, құқықтық, технологиялық және ұйымдастырушылық шаралар кешенін әзірлеу және жетілдіру үшін;

2) АҚ қамтамасыз ету үшін;

3) АҚ қамтамасыз ету талаптарын сақтау бойынша жұмыстарды жүргізу кезінде Университеттің құрылымдық бөлімшелерінің қызметін үйлестіру үшін.

4.4. Осы АҚ ережесінің талаптары мен шарттары Университеттің барлық АЖ-не қатысты қолданылады.

5. АҚ қамтамасыз етуді ұйымдастыру

5.1.Ақпаратты қорғау жүйесін тікелей ұйымдастыру (құру) және оның тиімді жұмыс істеуін қамтамасыз ету үшін мыналар жауап береді:

1) АТжТО – АКИ, ЕТҚ, АЖ, АҚ жұмыс істеуін іске асыратын құрылымдық бөлімше.

2) АТжТО Университеттің Басқарма мүшесі, жетекшілік ететін проректормен келісім бойынша ақпаратты АРҚ-тан қорғауға бағытталған шараларды дамытудың негізгі бағыттарын анықтайды.

6. АЖ пайдаланушылар санаттары

6.1. АЖ пайдаланушыларының санаттарына мыналар жатады:

1) ішкі пайдаланушылар – Қазақстан Республикасының заңнамасына сәйкес өз қызметін жүзеге асыратын және негізгі құқықтар мен міндеттерге ие, АР-ға авторландырылған қолжетімділігі бар Университет қызметкерлері;

2) сыртқы пайдаланушылар – Университет қызметтерін тұтынушылар, оның ішінде Университет АР-ын пайдаланатын тұлғалар;

3) көмекші қызметкерлер – қызмет көрсетуші, техникалық персонал және Университетте өзара іс-қимылды жүзеге асыратын басқа АЖ иелері,

оның ішінде:

- телекоммуникациялық жабдықты сүйемелдеуге жауапты ЖЕЖ әкімшілері;
- ЖӘ;

– ҚБҚ әзірлеушілер;

– инженер-жүйе техниктері, техникалық мамандар (жүйелік-техникалық қызмет көрсету) және т.б.

7. АҚ объектілері

7.1.Университеттің АҚ қорғаудың негізгі объектілері:

1) Құпияны құрайтын, рұқсат етілмеген әсерлерге және олардың қауіпсіздігінің бұзылуына қатысты сезімтал, қолжетімділігі шектеулі АР, оның ішінде ұсыну нысаны мен түріне қарамастан ашық (жалпыға қолжетімді) ақпарат;

2) АЖ-да ақпаратты өңдеу процестері мен адами ресурстар – ақпараттық технологиялар, ақпаратты жинау, өңдеу, сақтау және беру регламенттері мен рәсімдері, әзірлеушілер персоналы, жүйенің ішкі пайдаланушылары және оған қызмет көрсетуші персонал;

3) ақпаратты өңдеу және талдау, беру және бейнелеу жүйелерін, оның ішінде ақпарат алмасу арналарын, АР және АЖ компоненттері орналасқан объектілер мен үй-жайларды қамтитын ақпараттық инфрақұрылым.

7.2.Ақпараттық инфрақұрылым объектілері мыналарды қамтиды:

1) технологиялық жабдық (ЕТҚ, желілік және кабельдік жабдық);

2) Қолжетімділігі шектеулі мәліметтері бар АР;

3) бағдарламалық құралдар (операциялық жүйе (бұдан әрі – ОЖ), ДББЖ, басқа да жалпы жүйелік және ҚБҚ);

4) Автоматтандырылған байланыс және деректер беру жүйелері (телекоммуникация құралдары);

5) ақпарат берілетін байланыс арналары (оның ішінде таратылуы шектелген);

6) таратылуы шектеулі ақпарат айналатын қызметтік үй-жайлар;

7) қызметтік ақпарат өңделетін (айналатын) үй-жайларда орналастырылған ақпаратты өңдемейтін техникалық құралдар мен жүйелер.

7.3.АҚ-ның барлық құралдары университеттің АКИ-де қолданылғанға дейін АТжТО-ның АҚ үшін жауапты тұлғасымен келісіліп, Университет Басқармасының мүшесі, жетекшілік ететін проректоры тарапынан мақұлдануы тиіс. Аппараттық құралдар мен БҚ-ны қолданалар алдында жүйенің басқа компоненттерімен үйлесімділігін тексеру керек.

8. Қорғауға жататын АР санаттары

8.1.Университеттің АЖ кіші жүйелерінде таратылуы шектеулі мәліметтерді (дербес деректер, қызметтік, қаржылық ақпарат) және ашық мәліметтерді қамтитын ақпарат таратылады.

9. АҚ ережесін іске асыру жөніндегі шаралар

9.1.Университеттің АКИ-де жұмыс істейтін ішкі пайдаланушылар Университеттің АҚ ережесінің белгіленген талаптарын қатаң сақтауға міндетті.

9.2.АҚ бойынша қызметкерлердің, мамандардың функционалдық міндеттері Университеттің ішкі регламенттеуші құжаттарымен, қызметкерлердің лауазымдық нұсқаулықтарымен анықталады және АҚ ережесі мен «Ақпараттық технология. Қамту құралдары. Ақпаратты қорғауды басқару жөніндегі қағидалар жиынтығы» ҚР СТ ИСО/МЭК 27002-2015 Қазақстан Республикасы Мемлекеттік стандартының 8.1.1-т. талаптарына сәйкес құжатталады.

9.3.Қызметтік, коммерциялық және заңмен қорғалатын өзге де құпияны құрайтын «Академик Е.А. Бөкетов атындағы Қарағанды университеті» КЕАҚ туралы ақпараттың сақталуын қамтамасыз ету жөніндегі нұсқаулық.

9.4.АҚ үшін жауапты тұлға «Ақпараттық технология. Қамту құралдары. Ақпаратты қорғауды басқару жөніндегі қағидалар жиынтығы» ҚР СТ ИСО/МЭК 27002-2009 Қазақстан Республикасы Мемлекеттік стандартының 6.1.2-6.1.7-тармақтарының талаптарына сәйкес ақпаратты қорғауға байланысты мәселелер мен жұмыстарды ұйымдастырады, орындайды, бақылайды және үйлестіреді.

9.5.АҚ үшін жауапты тұлға АҚ-ны қамтамасыз ету шеңберінде мынадай жұмыс түрлерін

жүргізеді:

1) тиісті қызметтерді көрсету кезінде Университеттің ішкі пайдаланушыларына АҚ негіздері бойынша кеңес беру/таныстыру;

2)қорғау жүйесінің жұмыс істеу сенімділігін қамтамасыз ету;

3) техникалық ерекшеліктерді дайындауға, құрастыруға және бағдарламалық-аппараттық кешендерді сатып алу процесіне қатысу;

4) Университет шеңберінде АҚ-ны қамтамасыз етудің аппараттық және бағдарламалық құралдарын практикалық енгізу;

5) АЖ құру, дамыту және қолдану процесінде АҚ-ға қойылатын талаптарды қалыптастыруға;

6) қорғау жүйесін жобалауға, оны сынауға және пайдалануға қабылдауға қатысу;

7) авторландырылған ішкі пайдаланушылар арасында қажетті қорғау деректемелерін бөлу;

8) қорғау жүйесінің және оның элементтерінің жұмыс істеуін бақылау;

9) АЖ-ның ішкі пайдаланушыларына ақпаратты қауіпсіз өңдеу талаптары жөнінде кеңес беру;

10) АЖ ішкі пайдаланушыларының қорғалатын ақпаратты автоматтандырылған өңдеу процесінде онымен жұмыс істеудің белгіленген қағидаларын сақтауын бақылау;

11) АРҚ әрекеттерін анықтау кезінде және қорғау жүйесінің жұмыс істеу қағидаларын бұзу кезінде қажетті шаралар қабылдау;

12) ішкі аудит және ақпараттық қауіпсіздік мониторингін жүргізуге қатысу;

13) ақпаратты қорғаудың криптографиялық құралдарын пайдалану бойынша ұсыныстарды қарауға енгізеді;

14) Университеттің ақпараттық жүйелеріне қол жеткізу құқықтарының аражігін ажыратуды қамтамасыз етеді.

9.6. АҚ үшін жауапты тұлға және АТжТО қызметкерлері АҚ саласындағы біліктілікті арттыру бойынша оқуға мерзімді түрде жіберілуі тиіс.

9.7.Университеттің АКИ-де жұмыс істейтін ішкі және сыртқы пайдаланушылар қажеттілігіне қарай (не құпия ақпаратты қамтитын немесе өңдейтін жабдыққа қол жеткізу деңгейі болған кезде) АҚ саласында оқытуды жүргізуге уәкілетті ұйымдар ұйымдастыратын оқытудан өтеді.

10. АҚ және ЖӘ үшін жауапты тұлғаның ұйымдық-құқықтық мәртебесі

10.1.АҚ үшін жауапты адамның қажетті құқықтары бар:

1) Университеттің ақпараттық инфрақұрылымын мониторингілеу және бақылау үшін;

2) Университеттің АЖ, ЕТҚ және ЖЕЖ орнатылған университеттің барлық үй-жайларына кіру үшін;

3) қорғалатын ақпаратқа тікелей қауіп төнген кезде ақпаратты автоматтандырылған өңдеуді тоқтатуға.

10.2.Жүйелік әкімшілер АҚ үшін жауапты тұлғамен келісу бойынша мыналарға құқылы:

1)Университеттің АЖ, ЕТҚ және ЖЕЖ орнатылған барлық үй-жайларына кіруге;

2)қорғалатын ақпаратқа тікелей қауіп төнген кезде ақпаратты автоматтандырылған өңдеуді тоқтатуға.

11. Құпиялылықтың жалпы талаптары

11.1. Құпиялылықтың басты талаптары қандай да бір құпия ақпараттың таралып кетуін (жария етілуін) болдырмау және ақпаратты тек авторландырылған тұлғаларға беруді қамтамасыз ету болып табылады.

11.2. Университеттің АЖ-не ішкі пайдаланушыларды қосу осы ақпаратты 1 жылдан кем емес мерзімге сақтай отырып (бағдарлама жұмысы туралы деректерді жазу), толық және мұқият түрде тіркелуі тиіс.

11.3. Университеттің АЖ-де өңделетін және сақталатын қызметтік және өзге де қорғалатын ақпарат Басқарманың жетекшілік ететін мүшесінің ресми рұқсатымен ғана көшіруге және үшінші тұлғаға беруге жатады.

11.4. Университеттің АЖ-мен жұмыс істеу кезінде ішкі пайдаланушының монитор экранында көрсетілетін ақпаратты бөгде адамдардың бақылау мүмкіндігін болдырмауы тиіс.

11.5. Университеттің АЖ жұмысы кезінде зиянды бағдарламалардан, вирустардан және желілік шабуылдардан қорғауды қамтамасыз ететін арнайы лицензиялық бағдарламалық немесе аппараттық құралдар пайдаланылуы тиіс. Физикалық қорғауды қамтитын іс-шаралардан басқа, Университетке есепке алынбаған бағдарламаларды заңсыз енгізуден және пайдаланудан қорғау үшін жүйелік журналдарға мониторинг жүргізілуі тиіс, ішкі пайдаланушылардың жұмыс станцияларында БҚ-ның базалық кешені орнатылуы тиіс. БҚ базалық кешеніне ЕТҚ жұмыс қабілеттілігін қамтамасыз ету үшін қажетті лицензиялық БҚ кіреді.

11.6. Университеттің АЖ-мен жұмыс істеу кезінде ішкі пайдаланушылар мен қосалқы персоналдың құпиялылық талаптарын сақтауы құпиялылық туралы келісіммен қамтамасыз етілуі тиіс.

12. Жүйеде пайдаланушыларды аутентификациялау бойынша талаптар

12.1.Университеттің АЖ-да жұмыс істейтін барлық ішкі пайдаланушылар авторландырылған деректердің таралып кетуін және ұстап алу мүмкіндігін болдырмайтын қауіпсіз аутентификациядан өтуі тиіс.

12.2.АЖ-да ішкі пайдаланушыларды анықтап тану үшін бірегей сәйкестендіру есептік жазбалары (логин, құпиясөз) жасалады.

12.3.Есептік жазба туралы мәліметтердің сақталуына және жария етілмеуіне жауапкершілік АЖ-ның ішкі пайдаланушыларына жүктеледі.

12.4.Ішкі пайдаланушылардың есептік жазбалары тиісті құжаттар немесе жазбалар болған кезде ғана жасалуы және жойылуы тиіс.

12.5.Құпиясөзбен жұмыс істеу кезінде ішкі пайдаланушылардың және АЖ қызмет көрсетуші персоналының іс-қимылдарына құпиясөзді қорғауды ұйымдастыруға қойылатын талаптар: жеке құпиясөз кемінде 8 таңбадан тұрып, жалпы сөздіктегі сөздерді қамтымауы керек, кем дегенде келесі үш таңба жиынтығынан тұруы керек:¶

а) бас әріптер: A, B, C;¶

ә) кіші әріптер: a, b, c; ¶

б) сандар: 0, 1, 2, 3, 4, 5, 6, 7, 8, 9;¶

в)таңбалар`'~! @ # $ % ^ & * ( ) _ + - = { } | [ ] \ : " ; ' < > ? , . /.

13. Байланыс желілері бойынша ақпарат беру кезіндегі құпиялылық талаптары

13.1. Университеттің ақпаратын беру жеке немесе жалға алынған талшықты-оптикалық арналар арқылы, үлкен қашықтықта жүзеге асырылуы керек.

13.2. Серверлік, телекоммуникациялық жабдық пен құрылымдалған кабельдік жүйенің техникалық реттеу саласындағы талаптарға сәйкестігі туралы құжаттамалық дәлелдемелері және АҚ талаптарына сәйкестігі туралы сертификаты болуы тиіс.

13.3. Университеттің электрондық поштасының пошта мекенжайларын сайттарда тіркелген кезде және форумдарға немесе интернет-конференцияларға қатысқан кезде (қызметкердің кәсіби қызметіне байланысты іс-шараларға қатысты жағдайларды қоспағанда) пайдалануға тыйым салынады.

13.4. Құпия ақпаратпен жұмыс істейтін қызметкерлерге Интернеттің жалпыға қолжетімді пошта сервистерін және жедел қарым-қатынас Интернет-жүйесін пайдалануға тыйым салынады.

14. Жалпыға қолжетімді ресурстарды қорғауды ұйымдастыру жөніндегі талаптар

14.1. Жалпыға қолжетімді ресурстар (пошта серверлері, web-серверлер, web-порталдар және басқа ресурстар) университеттің ЖЕЖ жеке сегментінде (сегменттерінде) орналасуы тиіс. Көрсетілген ресурстарды Интернетке қосу Интернетке қолжетімділіктің бірыңғай шлюзі (ИҚБШ) арқылы жүзеге асырылады. Бұл ретте желіаралық экрандар мен басып кіруді анықтау және

болдырмау жүйелері (IDP, IPS, Anti-DDoS) қолданылуы тиіс.

14.2. Ресми интернет-ресурс интернет-ресурстардың бірыңғай платформасында орналастырылады және edu.kz (buketov.edu.kz) домендік аймағында тіркеледі.

14.3. Интернет-ресурс Интернет желісіне ИҚБШ арқылы қосылады.

14.4. Интернет-ресурстардың АҚ қамтамасыз ету үшін мазмұнды (контентті) басқару жүйесін қолдану қажет, ол:

1) ақпараттық контентті орналастыру, өзгерту және жою операцияларын санкциялауды;

2) ақпараттық контентті орналастыру, өзгерту және жою кезінде авторлықты тіркеуді;

3) жүктелетін контентті зиянды кодқа тексеруді;

4) орналастырылған ақпараттық контенттің тұтастығын бақылауды;

5) пайдаланушылар мен бағдарламалық роботтардың қалыптан тыс белсенділігін бақылауды жүзеге асырады.

Құпиялылықты қамтамасыз етуді бақылау мақсатында мынадай іс-шаралар жүзеге асырылуы тиіс:

1) ресми тіркелген пайдаланушылар мен АЖ-да жұмыс істейтін пайдаланушылардың тізімін жыл сайын салыстырып тексеру;

2) осы АҚ ережесі талаптарының сақталуына АҚ-ның жыл сайынғы аудиті;

3)Университеттің АКИ АҚ-ын аспаптық, бағдарламалық құралдармен тұрақты мониторингілеу.

15. Тұтастықтың жалпы талаптары

15.1. Тұтастықтың басты талабы – ақпараттың өзгеруін тек авторландырылған адамдар ғана қамтамасыз етеді.

15.2. Жаңа/әзірленген БҚ орнату, сондай-ақ қолда бар БҚ жаңарту алдында Университеттің АЖ тұтастығы мен қауіпсіздігін қамтамасыз ету үшін мұқият тестілеу және АҚ талаптарына сәйкестігін тексеру рәсімдері енгізілуі тиіс.

16. АЖ әзірлеу, жетілдіру және қызмет көрсету кезіндегі қауіпсіздік талаптары

16.1. АЖ әзірлегенге дейін АҚ қамтамасыз ету элементтеріне қойылатын талаптарды сәйкестендіріп, АҚ үшін жауапты тұлғамен келісу керек және Университет Басқармасының жетекшілік ететін мүшесіне бекітуге ұсыну қажет.

16.2. Бағдарламалық құралдарды әзірлеу немесе бағдарламалық құралдарды сүйемелдеу шеңберінде бастапқы кодты өзгерту әзірлеу ортасында жүзеге асырылуы тиіс.

16.3. Өзгертілген бағдарламалық құрал АҚ-ның белгіленген талаптарына сәйкестігі және басқа бағдарламалық құралдармен үйлесімділігі тұрғысынан тестілеуден өтуге тиіс. Тестілеуді әзірлеушілер АҚ-ға жауапты тұлғамен бірлесіп өткізеді, тестілеу нәтижелері тестілеу хаттамасында көрсетілуі тиіс.

16.4. Бағдарламалық құралды пайдалану ортасына қосу оң қорытындысы бар тестілеу хаттамасы болған кезде ғана жүзеге асырылуы тиіс.

16.5. Қауіпсіздік талаптары ақпараттық активтердің құндылығын, бизнес-процестің ықтимал залалын ескеруі керек.

17. АҚ желісін қамтамасыз ету компоненттеріне қойылатын талаптар

17.1. Университет ақпараттық жүйесінің қауіпсіз жұмыс істеуін қамтамасыз ету үшін әртүрлі бөлімшелердің ақпараттық ағындарын бөлуді және оқшаулауды қамтамасыз ететін техникалық шешімдерді, басып кіруді анықтау және алдын алу жүйелеріне кіруді бақылау және шектеу үшін желіаралық экрандарды пайдалану қажет.

17.2. Санкцияланған электрондық және нақты қол жеткізу құралдарынан басқа коммуникацияларды заңсыз қосудан қорғау бағдарламалық, техникалық құралдармен және ұйымдастыру шараларымен жүзеге асырылады. Коммуникацияларға кіруге рұқсат алу бойынша тұлғалардың заңсыз іс-әрекеттерін уақтылы анықтау, алдын алу және жолын кесу үшін қажетті іс-шараларды жүргізу.

17.3. Ақпараттың таралып кетуін анықтау үшін жария болу арналарының пайда болу мүмкіндігін жүйелі бақылау және бақыланатын аймақ шегінде олардың қауіптілігін бағалау қажет. Ақпараттың жария болу арналарын жабу және оқшаулау ұйымдастырушылық-техникалық шаралармен, сондай-ақ бар болған жағдайда сертификатталған DLP технологияларымен қамтамасыз етіледі.

18. Қауіпсіздік инциденттерін басқаруға қойылатын талаптар

18.1. АҚ-ны бұзу жағдайлары туралы АҚ-ға жауапты адамға дереу хабарлау керек.

18.2. Ақпаратты қорғау жүйесіндегі оқиғаларға тез, тиімді және реттелген жауап беру үшін жауапкершілік аймақтары мен рәсімдері белгіленуі керек.

18.3. Ақпаратты қорғау жүйесінде инциденттерге мониторинг жүргізу және оларды үнемі бақылау үшін тетіктер қабылдануға тиіс.

19. Ақпаратты рұқсатсыз қолжетімділіктен қорғауға қойылатын талаптар

19.1. АРҚ-тан қорғау мыналарды қамтамасыз етуі тиіс:

1) ашық кілттер инфрақұрылымының цифрлық сертификаттарында сәйкестендіру мүмкіндігін;

2) тиісті рұқсаттардың болуын талап ететін жүйенің ақпараттық-есептеу ресурстарына қол жеткізу үшін пайдаланушыларды авторландыруды;

3) деректерді енгізу, түзету, қарау құқықтарын дербес анықтауды;

4) жүйелік ресурстарға қол жеткізу құқығын дербес анықтауды;

5) пайдаланушыларды сәйкестендіру бойынша оқиғалардың аудитін;

6) АЖ-да пайдаланушыларды топтар бойынша бөлу функцияларының іске асырылуын және ақпаратты рұқсатсыз жоюды, көшіруді, түрлендіруді болдырмау үшін оларға тиісті қол жеткізу құқықтарын беруді;

7) физикалық деңгейде қорғалған байланыс арналарын;

8) АЖ-ның сыни функциялары мен қосымшалары бар пайдаланушылардың жұмысын хаттамалауды.

19.2. Негізгі ақпарат жеткізгіштерге (жинақтауыштарға, дискілерге, серверлік жабдыққа және т.б.) физикалық қол жеткізу Өңдеу құралдарын физикалық қорғауды және ақпараттық ресурстардың қауіпсіз жұмыс істеу ортасын ұйымдастыру қағидаларына сәйкес шектеледі.

20. Электрондық поштаны және интернетті қолдануға қойылатын талаптар

20.1. Электрондық поштаны пайдаланумен байланысты өндірістік процестер мен қауіпсіздік жүйесі ұшырайтын тәуекелді азайту үшін тиісті бақылау құралдарын қолдану керек (қажеттілігіне қарай), олар мыналарды ескеруі тиіс:

1) рұқсат етілмеген ұстап алу мен модификацияға қатысты электрондық хабарламалардың осалдығын;

2) қателіктерге қатысты электрондық пошта арқылы жіберілген деректердің осалдығын, мысалы, хабарламаларды бұрыс бағыттау немесе басқа адреске жіберу, сондай-ақ қызметтің сенімділігі мен қол жетімділігін;

3) өндірістік үдерістерге коммуникациялық орта сипаттамаларының өзгеруінің әсерін, мысалы, деректерді беру жылдамдығының жоғарылауының әсерін немесе ұйымдар мен жеке тұлғалар арасындағы адрестеу жүйесінің өзгеруін;

4) хабарлама көзін тексеру қажеттілігі және т.б. сияқты заңды пайымдамаларды;

5) каталог мазмұнын ашумен байланысты қауіпсіздік жүйесінің салдарын;

6) пайдаланушылардың электрондық поштаға қашықтан қол жеткізуін бақылау үшін қорғаныс шараларын қабылдау қажеттілігін.

20.2. Интернет желісіне қосылу Университеттің ақпараттық-коммуникациялық және жергілікті желісімен түйіндеспейтін Интернет желісіне қол жеткізудің бірыңғай шлюзі арқылы ғана жүзеге асырылуы тиіс.

21. Резервтік көшіруге және қалпына келтіруге қойылатын талаптар

21.1. Университеттің АКИ-де өңделетін барлық ақпарат резервтік көшіруге жатады.

21.2. Резервтік көшіруге қойылатын талаптар АҚ ережесіне Ақпаратты резервтік көшіру және қалпына келтіру регламентінде сипатталған.

21.3. ҚБҚ мен жүйелік БҚ-ны резервтік көшіру жауапты тұлғалармен резервтік көшіру кестесіне сәйкес жүргізілуі тиіс. Барлық ҚБҚ және Университет бойынша жүйелік БҚ жарамдылық, қауіпсіздік, басқа жүйелерге әсер ету және пайдалану қолайлылығы тұрғысынан жеке аспаптық ортада көлемді және ойдағыдай тестілеуден кейін іске асырылуы тиіс.

21.4. ҚБҚ нұсқасы өзгерген сайын (қателерді түзету, функционалдылықты қосу) ҚБҚ-ның ескі нұсқасы 3 ай бойы сақталуы тиіс.

22. Вирусқа қарсы қауіпсіздікке қойылатын талаптар

22.1. Вирустарды анықтаудың вирусқа қарсы бағдарламалық құралдарын АЖ серверлерін, жұмыс станцияларын және тасымалданатын ақпарат тасымалдағыштарын вирустардың болуына тексеру үшін қолданған жөн. Вирусқа қарсы бағдарламалық құралдар үнемі жаңартылып, вирусқа қарсы бақылауды ұйымдастыру қағидаларына сәйкес пайдаланылуы тиіс.

23. Қолжетімділіктің жалпы талаптары

23.1. Қолжетімділіктің басты талабы пайдаланушылардың ақпаратқа уақтылы және заңды қол жеткізуін қамтамасыз ету болып табылады.

23.2. Апат, дүлей зілзалалар және өзге де төтенше жағдайлар туындаған кезде тиісті қорғау, үздіксіз жұмыс істеу және қалпына келтіру шаралары ескерілуі тиіс.

23.3. Апат, дүлей зілзалалар және өзге де төтенше жағдайлар осы ақпаратты кем дегенде 1 жыл сақтай отырып, толық және мұқият түрде тіркелуі тиіс.

24. Істен шығуды болдырмауға қойылатын талаптар

24.1.Аппараттық-бағдарламалық қамтамасыз ету университет АЖ міндеттерінің орындалуын бір реттік бос тұрып қалу уақыты 10 сағаттан аспайтын және жалпы бос тұрып қалу уақыты жылына 48 сағаттан аспайтындай етіп қамтамасыз етуі тиіс.

24.2.АЖ өндірістік серверінде штаттан тыс жағдай туындаған жағдайда ҚБҚ, жүйелік БҚ және ОЖ 9 сағаттан аспайтын уақыт ішінде қалпына келтірілуі тиіс.

24.3.Университеттің АЖ жұмыс қабілеттілігін қалпына келтіру және үздіксіз жұмыс істеуін қамтамасыз ету Қазақстан Республикасы Үкіметінің 2016 жылғы 20 желтоқсандағы № 832 «Ақпараттық-коммуникациялық технологиялар және ақпараттық қауіпсіздікті қамтамасыз ету саласындағы бірыңғай талаптарды бекіту туралы» қаулысының «Техникалық құралдардың үздіксіз жұмыс істеу жүйелеріне және ақпараттық қауіпсіздікке қойылатын талаптар» атты 8-параграфына сәйкес жүргізіледі.

24.4.Деректерді сақтау жүйесі дискілердің тұтастығын автоматты түрде мезгіл-мезгіл бақылауды, нашар секторларды талдауды, әкімшінің араласуынсыз және пайдаланушылардың жұмысына әсер етпестен резервтік батареялардың күйін тексеруді қамтуы керек.

24.5.Деректерді сақтау жүйесі дискілерді жедел ауыстыру мүмкіндігін қамтамасыз етуі тиіс.

24.6.Үздіксіз қуат көзі қажетті қуаты бар үздіксіз қуат көзімен (ҮҚК) қамтамасыз етіледі, ол сыртқы қуат көзі өшірілген кезде қосымшалар мен ОЖ жұмысының кем дегенде дұрыс аяқталуын қамтамасыз етуі керек.

25. Тәуекелдерді талдау мен бағалауға қойылатын талаптар

25.1. АҚ ережесі бастапқыда АҚ тәуекелдерін талдау және бағалау нәтижесінде алынған деректерге негізделуі тиіс.

25.2. АҚ ережесін жетілдіру мақсатында АҚ тәуекелдерін жыл сайынғы талдау және бағалау

жүргізілуі тиіс. Бұл талдау АҚ-ның жыл сайынғы аудитінің деректеріне негізделеді және одан әрі ұйымдастырушылық-өкімдік шаралар қабылдау мақсатында Университет Басқармасының жетекшілік ететін мүшесіне ұсынылады.

25.3. Тәуекелдерді талдау және бағалау ҚР СТ ИСО/МЭК 17799-2006 «Ақпараттық технология. Қорғауды қамтамасыз ету әдістері. Ақпаратты қорғауды басқару жөніндегі қағидалар жиынтығы» Мемлекеттік стандартты іске асыру жөніндегі нұсқаулыққа сәйкес жүргізілуі тиіс.

25.4. АҚ үшін жауапты тұлға шығындар мен тәуекелдердің пайдасын талдау нәтижелерінің негізінде тәуекелді азайту үшін неғұрлым экономикалық тиімді шараларды анықтайды. Таңдалған шаралар университеттің АКИ үшін тиісті қауіпсіздікті қамтамасыз ету үшін техникалық, пайдалану және басқару шараларын біріктіруі тиіс.

26. Қолданылатын қорғау шараларының тиімділігін бақылау

26.1. АҚ-ның талап етілетін деңгейін ұстап тұру үшін Университетте АҚ үшін жауапты тұлға қорғау шараларының тиімділігін тұрақты бақылауды жүзеге асырады. Бұл ретте негізгі критерий – қорғалатын ресурстардың тәуекелдері Университет үшін қолайлы шектерде болуы тиіс.

26.2. Қабылданып жатқан қорғау шараларының тиімділігін бақылаудың негізгі тетіктері Университеттің АҚ мониторингі мен аудиті болып табылады.

26.3. Университеттің АҚ аудиті Университеттің ақпараттық қауіпсіздігіне ішкі аудит және мониторинг жүргізу қағидаларына сәйкес жүзеге асырылады.

26.4. Аудит нәтижелері АҚ ережесінің кейбір тармақтарын қайта қарау және оған қажетті түзетулер енгізу үшін негіз бола алады.

26.5. Осы АҚ ережесінің талаптарын АҚ талаптарына сәйкестігіне бақылауды АҚ жөніндегі қызметкерлер жүзеге асырады.

27. АҚ ережесін қайта қарау

27.1.АҚ ережесін дамытуды, қайта қарауды және бағалауды АҚ тәуекелдерін жыл сайынғы талдау және бағалау негізінде АҚ үшін жауапты адам жүзеге асырады.

27.2.АҚ ережесін қайта қарау мынадай мақсаттарда жүргізіледі:

1) АҚ мақсаттары мен бақылау шараларын жетілдіру;

2)Университеттің ақпараттық қауіпсіздігі мен бизнес-процестерін басқару тәсілін жетілдіру;

3) ресурстарды және/немесе міндеттерді бөлуді жақсарту.

27.3.АҚ ережесі АҚ бұзылуының елеулі инциденттерін, жаңа осалдықтардың пайда болуын немесе ұйымдық/технологиялық инфрақұрылымның өзгеруін, Университеттің бизнес-процестерінің негізгі сипаттамаларының өзгеруін анықтау жолымен тәуекелді бастапқы бағалау негізіне әсер ететін өзгерістерге сәйкес қайта қаралуы тиіс.

27.4.АҚ қамтамасыз ететін технологияларда елеулі өзгерістер пайда болған жағдайда, ақпараттың құпиялылығын, тұтастығын, қолжетімділігін, сондай-ақ АҚ қолданылатын шараларының барабарлығы мен тиімділігін қамтамасыз ету мақсатында.

27.5.АҚ ережесі нормаларының өзгерістеріне ішкі және сыртқы пайдаланушылар тарапынан қосымша ескертулер мен ұсыныстар туындаған жағдайда, осы ұсыныстарды АҚ үшін жауапты тұлға талдайды және қажет болған кезде бекіту үшін ұсынады.

27.6.Университет басшылығы АҚ ережесін тәуелсіз қайта қарауды бастауы мүмкін. Мұндай қайта қарауды қайта қаралатын қауіпсіздік саласына тікелей қатысы жоқ адам жүргізеді, мысалы, ішкі аудит функциясын тәуелсіз менеджер немесе осындай қайта қарауға маманданған үшінші тарап ұйымы жүзеге асырады. Тәуелсіз қайта қарау нәтижелері есеп түрінде құжатталады және Университеттің Басқарма төрағасының назарына ұсынылады.

27.7.АҚ ережесі Университет үшін АҚ тәуекелдерін талдау және бағалау жүргізілгеннен кейін қайта қаралуы тиіс, оның қорытындысы бойынша анықталған кемшіліктерді түзетуді ескере отырып, оны өзектендіру қажет.

27.8.АҚ ережесінің жаңа редакциясы бекітілген кезде редакцияның нөмірі титулдық парақта

құжат атауының астында көрсетіледі, мысалы: 1-ред..

27.9.АҚ ережесін қайта қарау ҚР СТ ИСО/МЭК 17799-2006 «Ақпараттық технология. Қорғауды қамтамасыз ету әдістері. Ақпаратты қорғауды басқару жөніндегі қағидалар жиынтығы» Қазақстан Республикасының мемлекеттік стандартын іске асыру жөніндегі нұсқаулыққа сәйкес жүзеге асырылуы тиіс.

28. Жауапкершілік

28.1.АҚ үшін жауапты тұлға Университет Басқармасының жетекшілік ететін мүшесімен бірлесіп мыналарды қамтамасыз етеді:

1)Университеттің ұйымдастырушылық талаптарына және бизнес-үдерістеріне кірігуіне сәйкес АҚ мақсаттарын анықтау;

2) осы АҚ ережесінің барлық тармақтарының орындалуын бақылау;

3)Университеттің АҚ қолдау саласындағы бастамаларды нақты басқару және айқын қолдау;

4)АҚ қамтамасыз ету үшін ресурстар ұсыну;

5)Бекітілген құжаттарды жариялауды және оларды Университеттің АКИ пайдаланушыларына жеткізуді бақылау.

28.2.АҚ үшін жауапты тұлғаның ұсынуы бойынша Университет Басқармасының жетекшілік ететін мүшесі:

1) Университеттің АҚ бойынша әзірленетін, қайта қаралатын құқықтық құжаттарды бекітуге;

2) АҚ ережесін іске асырудың тиімділігіне бақылау жүргізуге тиіс;

3) АҚ бойынша айрықша рөлдер мен міндеттерді бөлуді бекітуге;

4) АҚ туралы хабардар болу жөніндегі жоспарлар мен бағдарламаларды бастауы тиіс;

28.3. Университеттің құрылымдық бөлімшелерінің басшылары Ереже талаптарының орындалуына, сондай-ақ осы Ережемен танысуға жауапты болады.

28.4. Қол астындағылардың ақ, оның ішінде жаңадан қабылданған қызметкерлер.

28.5.Университет үшін моральдық және материалдық залалға әкеп соққан АҚ ережесінің талаптары бұзылған кезде, оған қатысы бар қызметкерлер Қазақстан Республикасының заңнамасына сәйкес жауапкершілікке тартылады.

28.6.АҚ ережесі талаптарының бұзылуы еңбек міндеттерін орындамаудан немесе тиісінше орындамаудан тұратын тәртіптік теріс қылық ретінде сараланады. АҚ ережесі талаптарының бұзылуына жол берген қызметкер Қазақстан Республикасының Еңбек кодексіне және ҚР СТ ИСО/МЭК 27002-2009 «Ақпараттық технологиялар. Қамту құралдары. Ақпаратты қорғауды басқару жөніндегі қағидалар жиынтығы» Мемлекетік стандартының 8.2.3 және 13.2.3-тармақтарының талаптарына сәйкес тәртіптік жауапкершілікке тартылады.