«Ахмет Байтұрсынұлы атындағы Қостанай өңірлік университеті» КЕАҚ

BU
BAITURSYNULY UNIVERSITY

Бекітемін
Басқарма Төрағасы –
Ректор
_____ С. Куанышбаев
16.06. 2026 ж.

ҚАҒИДАЛАР

АҚПАРАТТЫҚ ҚАУІПСІЗДІКТІҢ ІШКІ АУДИТІН ЖҮРГІЗУ

Қ 015-2026

Қостанай

Алғы сөз

1 Бағдарламалық қамтамасыз етуді әзірлеу және сүйемелдеу бөлімімен **ӘЗІРЛЕНДІ**

2 Бағдарламалық қамтамасыз етуді әзірлеу және сүйемелдеу бөлімімен **ЕНГІЗІЛДІ**

3 Басқарма Төрағасы - Ректордың 16.06.2026 жылғы №213 НҚ бұйрығымен **БЕКІТІЛДІ ЖӘНЕ ҚОЛДАНЫСҚА ЕНГІЗІЛДІ**

4 ӘЗІРЛЕУШІ:
В. Гриднева – бағдарламалық қамтамасыз етуді әзірлеу және сүйемелдеу бөлімінің бастығы

5 САРАПШЫЛАР:
Ж. Жарлығасов – зерттеулер, инновациялар және цифрландыру жөніндегі проректор, ауыл шаруашылығы ғылымдарының кандидаты;
А. Шмит – техникалық қамтамасыз ету бөлімінің бастығы

6 ТЕКСЕРУ КЕЗЕҢДІЛІГІ 3 жыл

7 АЛҒАШ РЕТ ЕНГІЗІЛДІ

Мазмұны

1 тарау. Қолдану саласы

1. Осы Ақпараттық қауіпсіздіктің ішкі аудитін жүргізу қағидалары (бұдан әрі – Қағидалар) «Ахмет Байтұрсынұлы атындағы Қостанай өңірлік университеті» КЕАҚ-та (бұдан әрі – Университет) ақпараттық қауіпсіздіктің ішкі аудитін ұйымдастыру және жүргізу тәртібін айқындайды.

2. Қағидалар ақпараттық қауіпсіздіктің жай-күйіне ішкі бақылауды жүзеге асыру, Университеттің жергілікті нормативтік құжаттарының талаптарын сақтау, осалдықтарды, ақпаратты қорғаудың ұйымдастырушылық және техникалық шараларындағы кемшіліктерді анықтау, сондай-ақ Университеттің электрондық ақпараттық ресурстарының, ақпараттық жүйелерінің және активтерінің қорғалу деңгейін арттыру жөнінде ұсынымдар әзірлеу мақсатында әзірленді.

3. Ақпараттық қауіпсіздіктің ішкі аудитін Университет қызметкерлері жүргізеді және ол электрондық ақпараттық ресурстарға, ақпараттық жүйелерге, серверлік жабдыққа, жұмыс станцияларына, желілік инфрақұрылымға, бағдарламалық қамтамасыз етуге, корпоративтік сервистерге және ақпаратты өңдеу құралдарымен байланысты өзге де активтерге қолданылады.

4. Ақпараттық қауіпсіздіктің ішкі аудиті мыналарды қамтиды:

1) АҚ бойынша жергілікті нормативтік құжаттар талаптарының сақталуын тексеруді;

2) ақпаратты қорғаудың ұйымдастырушылық және техникалық шараларының жай-күйін талдауды;

3) АҚ осалдықтары мен ықтимал қатерлерін анықтауды;

4) қолжетімділік құқықтарының дұрыс ажыратылуын тексеруді;

5) ақпараттың резервтік көшірмесін жасау және оны қалпына келтіру жай-күйін тексеруді;

6) вирусқа қарсы қорғанысты тексеруді;

7) оқиғалар және АҚ инциденттері журналдарын талдауды;

8) Интернет желісін және корпоративтік электрондық поштаны пайдалану қағидаларының сақталуын бағалауды;

9) анықталған бұзушылықтарды жою жөнінде ұсынымдар әзірлеуді.

5. Қағидалар Университеттің нормативтік-анықтамалық құжаттамасының құрамына кіреді, Университеттің барлық қызметкерлері үшін орындауға міндетті болып табылады, сондай-ақ Университеттің ақпаратты өңдеу құралдарын пайдалану мен қызмет көрсетуге қатысатын өзге де үшінші тұлғалардың назарына жеткізіледі.

2 тарау. Нормативтік сілтемелер

6. Осы Қағидаларда мынадай нормативтік құжаттарға сілтемелер пайдаланылды:

1) «Ақпараттандыру туралы» Қазақстан Республикасының 2015 жылғы 24 қарашадағы № 418-V Заңы;

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

3) Қазақстан Республикасы Қаржы министрлігі Мемлекеттік мүлік және жекешелендіру комитеті төрағасының 2020 жылғы 05 маусымдағы № 350 бұйрығымен бекітілген, 03.10.2023 жылғы өзгерістерімен «Ахмет Байтұрсынұлы атындағы Қостанай өңірлік университеті» КЕАҚ Жарғысы;

4) ҰС 002-2025 Ұйым стандарты. Іс қағаздарын жүргізу;

5) ҚП 001-2025 Құжатталған процедура. Құжаттаманы басқару;

6) Е 054-2024 «Ахмет Байтұрсынұлы атындағы Қостанай өңірлік университеті» КЕАҚ ақпараттық қауіпсіздік саясаты;

3 тарау. Анықтамалар

7. Осы Қағидаларда мынадай анықтамалар қолданылады:

1) ақпараттық қауіпсіздіктің ішкі аудиті – жергілікті нормативтік құжаттар талаптарының сақталуын және ақпаратты қорғау шараларының тиімділігін бағалауға бағытталған Университеттің ақпараттық қауіпсіздік жай-күйін ішкі тексеру процесі;

2) ақпаратты өңдеу құралдарымен байланысты актив (бұдан әрі – АҚ активі) – ақпарат болып табылатын, ақпаратты қамтитын не ақпаратты өңдеу, сақтау немесе беру үшін пайдаланылатын және Университет үшін құндылығы бар материалдық немесе материалдық емес объект;

3) ақпараттық қауіпсіздік – Университеттің электрондық ақпараттық ресурстарының, ақпараттық жүйелерінің және АҚ активтерінің ішкі және сыртқы қатерлерден қорғалу жай-күйі;

4) ақпараттық жүйе – осы Қағидаларда ақпаратты өңдеу, сақтау және беру үшін пайдаланылатын Университеттің барлық ақпараттық жүйелері, корпоративтік сервистері және веб-ресурстары ақпараттық жүйелер деп түсініледі;

5) ақпараттық қауіпсіздік инциденті – ақпараттың құпиялылығына, тұтастығына немесе қолжетімділігіне қатер төндіретін оқиға немесе әрекет;

6) осалдық – АҚ қатерін іске асыру үшін пайдаланылуы мүмкін ұйымдастырушылық, бағдарламалық, техникалық немесе физикалық қорғау шараларының кемшілігі;

7) аудиторлық топ – ақпараттық қауіпсіздіктің ішкі аудитін жүргізу үшін тағайындалған Университет қызметкерлері.

4 тарау. Белгілер мен қысқартулар

8. Осы Қағидаларда мынадай қысқартулар қолданылады:

1) ҚП – құжатталған процедура;

2) КЕАҚ – коммерциялық емес акционерлік қоғам;
3) ҚҚБ – құжаттамалық қамтамасыз ету бөлімі;
4) ҰС – ұйым стандарты;
5) АҚ – ақпараттық қауіпсіздік;
6) АЖ – ақпараттық жүйе;
7) Е – ереже;
8) Қ – қағидалар;
9) LMS – оқытуды басқару жүйесі (Learning Management System);
10) CMS – контентті басқару жүйесі (Content Management System).

5 тарау. Негізгі мақсаттар мен міндеттер

9. АҚ ішкі аудитінің негізгі мақсаттары:
1) Университет АҚ-ның ағымдағы жай-күйін бағалау;
2) АҚ бойынша жергілікті нормативтік құжаттар талаптарының сақталуын бақылау;
3) ақпаратты қорғау жүйесінің осалдықтары мен кемшіліктерін анықтау;
4) АЖ ресурстарына қатысты қауіпсіздік қатерлерінің іске асу мүмкіндігімен байланысты тәуекелдерді талдау;
5) Университеттің ақпараттық жүйелері мен корпоративтік сервистерінің орнықтылығын арттыру.

10. Ішкі аудиттің негізгі міндеттері:
1) қолжетімділік құқықтарын ажырату талаптарының сақталуын тексеру;
2) вирусқа қарсы бақылау талаптарының сақталуын тексеру;
3) ақпараттың резервтік көшірмесін жасау және қалпына келтіру жай-күйін тексеру;
4) оқиғалар және АҚ инциденттері журналдарын талдауды;
5) бағдарламалық қамтамасыз ету жаңартуларының өзектілігін тексеру;
6) Интернет желісін және корпоративтік электрондық поштаны пайдалану қағидаларының сақталуын тексеру;
7) серверлік және желілік жабдықты физикалық қорғау талаптарының сақталуын тексеру;
8) ақпараттық қауіпсіздік тәуекелдерін төмендету жөніндегі іс-шаралардың орындалуын бағалау;
9) анықталған бұзушылықтарды жою жөнінде ұсынымдар дайындау.

6 тарау. Ақпараттық қауіпсіздіктің ішкі аудиті түрлері

11. Ақпараттық қауіпсіздіктің ішкі аудиті мынадай түрлерге бөлінеді:
1) жоспарлы аудит;
2) жоспардан тыс аудит.

12. Жоспарлы аудит Университеттің АҚ-ны қамтамасыз етуге жауапты қызметкерлері жасайтын және Университет басшылығы бекітетін ақпараттық

қауіпсіздіктің ішкі аудитінің жыл сайынғы жоспар-кестесіне сәйкес жүргізіледі. АҚ ішкі аудитінің жоспар-кестесінің нысаны осы Қағидаларға А қосымшасында келтірілген.

13. Жоспардан тыс аудит мынадай жағдайларда жүргізіледі:

1) АҚ инциденттері туындаған кезде;
2) АҚ талаптарының бұзылу белгілері анықталған кезде;
3) жаңа АЖ, сервистер немесе техникалық құралдар енгізілгеннен кейін;
4) Университет басшылығының тапсырмасы бойынша.

14. Мақсаттары мен міндеттеріне қарай ақпараттық қауіпсіздіктің ішкі аудиті мыналарды қамтуы мүмкін:

1) АҚ жай-күйін бағалау және ақпаратты қорғау шараларын жетілдіру жөнінде ұсынымдар дайындау мақсатында АЖ, корпоративтік есептеу желісінің, серверлік, желілік және өзге де жабдықтың аудиті;

2) АҚ жүйесінің Қазақстан Республикасы заңнамасының талаптарына және Университеттің ішкі нормативтік құжаттарына сәйкестігін қамтамасыз етуге бағытталған профилактикалық аудит;

3) ақпараттық қауіпсіздік инциденттерінің себептері мен мән-жайларын анықтау мақсатында жүргізілетін аудит (қызметтік тергеп-тексеру);

4) Университеттің құрылымдық бөлімшелері қызметкерлерінің, қызмет көрсетуші ұйымдар өкілдерінің не тартылған мамандардың құзыреті шегінде және шарттық міндеттемелер негізінде қатысуымен жүргізілетін аудит.

7 тарау. Ақпараттық қауіпсіздіктің ішкі аудитін ұйымдастыру және жүргізу тәртібі

15. Ішкі аудитті бағдарламалық қамтамасыз етуді әзірлеу және сүйемелдеу бөлімінің, техникалық қамтамасыз ету бөлімінің қызметкерлері және ақпараттық қауіпсіздікті қамтамасыз етуге жауапты қызметкерлер жүргізеді.

16. Аудит жүргізу үшін аудиторлық топ және оның жетекшісі тағайындалады.

17. Аудит жүргізу кезінде мыналар ескеріледі:

1) аудиттің мақсаттары мен саласы;
2) тексерілетін ақпараттық жүйелер мен АҚ активтерінің тізбесі;
3) аудит жүргізу мерзімдері;
4) қолданылатын нормативтік құжаттардың тізбесі;
5) алдыңғы тексерулердің және АҚ инциденттерінің нәтижелері.

18. Осы Қағидаларға А қосымшасына сәйкес нысан бойынша жасалған, бекітілген АҚ ішкі аудитінің жоспар-кестесі негізінде нақты аудитті жүргізу бағдарламасы қалыптастырылады. АҚ ішкі аудиті бағдарламасының нысаны осы Қағидаларға Б қосымшасында келтірілген.

19. Аудит жүргізуге дайындық мыналарды қамтиды:

1) жергілікті нормативтік құжаттарды зерделеу;
2) оқиғалар мен инциденттер журналдарын талдау;

3) аудит критерийлерін айқындау;

4) тексерілетін АҚ активтерінің тізбесін айқындау;

5) осы Қағидаларға Б қосымшасына сәйкес нысан бойынша ақпараттық қауіпсіздіктің ішкі аудиті бағдарламасына енгізілетін тексерілетін мәселелерді дайындау.

20. Аудиторлық топтың жетекшісі аудиторлық топтың барлық мүшелерін аудит бағдарламасымен таныстырады. Осыдан кейін аудит жүргізілгенге дейін кемінде 7 күнтізбелік күн бұрын аудит бағдарламасы аудит жүргізу шарттары мен уақытын келісу үшін тексерілетін құрылымдық бөлімшелердің басшыларына беріледі. Келісілген аудит бағдарламасы Университет басшылығының бекітуіне беріледі.

21. Аудит жүргізу процесінде мынадай әдістер қолданылады:

1) ұйымдастыру-өкімдік құжаттаманы талдау;

2) ақпараттық жүйелер мен серверлік жабдық баптауларын тексеру;

3) оқиғалар журналдарын талдау;

4) қызметкерлермен әңгімелесу;

5) жергілікті нормативтік құжаттар талаптарының сақталуын тексеру;

6) мониторинг пен талдаудың мамандандырылған бағдарламалық құралдарын пайдалану.

22. Ішкі аудит жүргізу кезінде мыналар тексерілуі мүмкін:

1) серверлік жабдық;

2) жұмыс станциялары;

3) жергілікті есептеу желісі;

4) резервтік көшірме жасау жүйелері;

5) вирусқа қарсы қорғаныс жүйелері;

6) корпоративтік электрондық пошта;

7) LMS, CMS, деректер базалары және өзге де ақпараттық жүйелер;

8) АҚ инциденттерін тіркеу журналдары;

9) пайдаланушылардың қолжетімділік құқықтары.

23. АҚ ішкі аудитін жүргізу кезінде аудиторлық топ мүшелерінің мынадай құқықтары бар:

1) аудит жүргізу үшін қажетті АҚ активтері орналасқан не байланыс желілері мен желілік коммуникацияларды орналастыру және өткізу үшін пайдаланылатын Университеттің қызметтік, серверлік, коммутациялық, аппараттық және өзге де үй-жайларына кіруге;

2) берілген өкілеттіктер шегінде аудит нысанасына қатысты ақпараттық жүйелерге, корпоративтік есептеу желісіне, серверлерге, желілік жабдыққа, бейнебақылау жүйелеріне, интернет-ресурстарға және құжаттамаға қол жеткізуге;

3) аудит нысанасына қатысты қажетті құжаттарды, мәліметтерді, есепке алу журналдарын, есептерді, логтарды және өзге де материалдарды сұратуға және алуға;

4) Қазақстан Республикасының заңнамасында және Университеттің ішкі құжаттарында белгіленген шектерде АЖ-да, оқиғаларды тіркеу журналдарында, мониторинг құралдарында және өзге де бақылау жүйелерінде қамтылған оқиғалар мен жазбалар туралы ақпарат алуға;

5) аудит жүргізу барысында туындайтын мәселелер бойынша құрылымдық бөлімшелер қызметкерлерінен ауызша және жазбаша түсініктемелер алуға;

6) қажет болған жағдайда Университет басшылығымен келісу бойынша құрылымдық бөлімшелердің қызметкерлерін, сондай-ақ қызмет көрсетуші ұйымдар мен АЖ жеткізушілерінің өкілдерін тартуға.

24. Аудит нәтижелері бойынша осы Қағидаларға В қосымшасына сәйкес нысан бойынша АҚ ішкі аудиті туралы есеп жасалады.

25. АҚ ішкі аудиті туралы есеп мыналарды қамтиды:

1) аудит объектісі;
2) аудит жүргізілген күн;
3) анықталған бұзушылықтардың тізбесі;
4) анықталған осалдықтар;
5) қорғалу деңгейін бағалау;
6) бұзушылықтарды жою жөніндегі ұсынымдар;
7) анықталған кемшіліктерді жою мерзімдері;
8) аудиторлық топтың құрамы;
9) жауапты орындаушылар;
10) аудит нәтижелері бойынша қорытынды.

8 тарау. Түзету іс-шаралары

26. Ішкі аудит нәтижелері бойынша анықталған бұзушылықтарды жою және АҚ тәуекелдерін төмендету жөніндегі түзету іс-шаралары әзірленеді.

27. Түзету іс-шаралары мыналарды қамтуы мүмкін:

1) пайдаланушылардың қолжетімділік құқықтарын өзгерту;
2) бағдарламалық қамтамасыз етуді жаңарту;
3) вирусқа қарсы қорғанысты күшейту;
4) қауіпсіздік параметрлерін түзету;
5) серверлер мен желілік жабдық конфигурациясын жаңарту;
6) резервтік көшірмелерді қалпына келтіру немесе олардың жұмысқа қабілеттілігін тексеру;
7) белгіленген тәртіппен серверлік, желілік, компьютерлік жабдықты, бағдарламалық қамтамасыз етуді және ақпаратты қорғау құралдарын жөндеу, ауыстыру, жаңғырту немесе сатып алу;
8) қызметкерлерге қосымша оқыту жүргізу.

28. Түзету іс-шаралары, оларды орындау мерзімдері және жауапты орындаушылар осы Қағидаларға В қосымшасына сәйкес нысан бойынша АҚ ішкі аудиті туралы есепте көрсетіледі.

29. АҚ ішкі аудиті туралы есептің түзету іс-шараларында көрсетілген жауапты орындаушылар іс-шаралардың белгіленген мерзімдерде орындалуын қамтамасыз етеді. Түзету іс-шараларын орындау нәтижелері бойынша жауапты орындаушылар АҚ-ны қамтамасыз етуге жауапты қызметкерлерге іс-шаралардың орындалғаны туралы қызметтік жазба ұсынады.

30. АҚ-ны қамтамасыз етуге жауапты қызметкерлер түзету іс-шараларының орындалуын бақылауды жүзеге асырады. Қажет болған жағдайда бақылау тексеруі не анықталған сәйкессіздіктердің жойылуы бойынша қайталама ішкі аудит жүргізіледі.

9 тарау. Жауапкершілік

31. Университет қызметкерлері өздерінің лауазымдық міндеттері шегінде ақпарат беруге және АҚ ішкі аудитін жүргізуге жәрдемдесуге міндетті.

32. Аудиторлық топтың жетекшісі мыналар үшін жауапты болады:

1) ішкі аудитті жүргізуді ұйымдастыру;
2) тексеру нәтижелерінің объективтілігі;
3) ресімделетін материалдардың дұрыстығы;
4) есептердің уақтылы ұсынылуы.

33. Құрылымдық бөлімшелердің басшылары анықталған бұзушылықтарды белгіленген мерзімдерде жою үшін жауапты болады.

34. АҚ-ны қамтамасыз етуге жауапты қызметкерлер бұзушылықтарды жою және ақпараттық қауіпсіздік тәуекелдерін төмендету жөніндегі іс-шаралардың орындалуын бақылауды жүзеге асырады.

10 тарау. Өзгерістер енгізу тәртібі

35. Осы Қағидаларға өзгерістер енгізу бағдарламалық қамтамасыз етуді әзірлеу және сүйемелдеу бөлімі бастығының, техникалық қамтамасыз ету бөлімі бастығының, зерттеулер, инновациялар және цифрландыру жөніндегі проректордың бастамасы бойынша ҚП 001-2025 Құжатталған процедура. Құжаттаманы басқару құжатына сәйкес жүзеге асырылады.

11 тарау. Келісу, сақтау және тарату

36. Қағидаларды келісу және тарату ҚП 001-2025 Құжатталған процедура. Құжаттаманы басқару құжатына сәйкес жүргізіледі.

37. Осы Қағидалар зерттеулер, инновациялар және цифрландыру жөніндегі проректормен, құқықтық қамтамасыз ету және мемлекеттік сатып алу бөлімінің бастығымен, персоналды басқару бөлімінің бастығымен және құжаттамалық қамтамасыз ету бөлімінің бастығымен келісіледі.

38. Осы Қағидалардың түпнұсқасы «Келісу парағымен» бірге қабылдау-беру актісі бойынша ҚҚБ-ға сақтауға беріледі.

39. Осы Қағидалардың жұмыс данасы ішкі корпоративтік желіден қолжетімділікпен Университеттің сайтында орналастырылады.

А қосымшасы

Ақпараттық қауіпсіздік бойынша ішкі аудиттердің жоспар-кестесінің үлгісі

Ақпараттық қауіпсіздік бойынша ішкі аудиттердің жоспар-кестесі
_____ жылға

№	Аудит объектісі (мысалдар)	Алдыңғы ішкі аудит күні	Аудит жүргізудің жоспарлы мерзімі	Аудит жүргізудің нақты күні
1	Серверлік жабдық			
2	Жұмыс станциялары			
3	Жергілікті есептеу желісі			
4	Университеттің ақпараттық жүйелері			
5	Корпоративтік электрондық пошта			
6	Резервтік көшірме жасау жүйесі			
7	Вирусқа қарсы қорғаныс			
8	Пайдаланушылардың қолжетімділік құқықтары			
9	Серверлік үй-жайлар			
10	АҚ инциденттері және штаттан тыс жағдайлар журналдары			

Ескертпе: ақпараттық қауіпсіздік инциденттері туындаған, АҚ талаптарының бұзылу белгілері анықталған, жаңа ақпараттық жүйелер, сервистер немесе техникалық құралдар енгізілген жағдайда жоспардан тыс аудит жүргізіледі.

Аудиторлық топтың жетекшісі

Лауазымы _____ А. Тегі
(қолы)

Жасалған күні: «____» _____ 20__ жыл

Б қосымшасы

Ішкі аудит бағдарламасының үлгісі

«Ахмет Байтұрсынұлы атындағы Қостанай өңірлік университеті» КЕАҚ

Бекітемін
Лауазымы
_____Т.А.Ә.
_____202 __ж.

АҚ ІШКІ АУДИТІНІҢ № _____ БАҒДАРЛАМАСЫ

1. Тексерілетін құрылымдық бөлімше
2. Аудит объектісі
3. Аудит жүргізу негізі
4. Аудит мақсаты
5. Аудит міндеттері
6. Аудит жүргізу мерзімдері
7. Аудит саласы
8. Аудиторлық топтың құрамы
9. Сәйкестігіне аудит жүргізілетін нормативтік құжаттардың тізбесі:
10. Аудит критерийлері:

Аудит критерийлері аудит объектісіне қолданылатын Қазақстан Республикасы заңнамасының, Университеттің ақпараттық қауіпсіздік саясатының және ақпараттық қауіпсіздік саласындағы Университеттің жергілікті нормативтік құжаттарының талаптары болып табылады.

Ішкі аудит жүргізу кезінде аудиттің мақсаты мен саласына қарай мынадай бағыттар бойынша талаптардың сақталуы тексеріледі:

1) АҚ бойынша нормативтік-анықтамалық құжаттаманың болуы және өзектілігі;
2) Ақпараттық қауіпсіздік саясаты талаптарының сақталуы;
3) активтерді сәйкестендіру, сыныптау және таңбалау талаптарының сақталуы;
4) ақпараттық қауіпсіздік тәуекелдерін бағалау талаптарының сақталуы;
5) аутентификация және қолжетімділік құқықтарын ажырату талаптарының сақталуы;
6) вирусқа қарсы бақылау талаптарының сақталуы;
7) Интернет желісін және корпоративтік электрондық поштаны пайдалану талаптарының сақталуы;
8) ақпараттың резервтік көшірмесін жасау және қалпына келтіру талаптарының сақталуы;
9) АҚ инциденттеріне және штаттан тыс жағдайларға ден қою тәртібінің сақталуы;
10) серверлік және желілік жабдықты физикалық қорғау талаптарының сақталуы.

11. Аудит шеңберінде тексерілетін мәселелер:

Тексерілетін мәселелерді аудиторлық топ аудиттің мақсатын, міндеттерін, объектісін, тексерілетін құрылымдық бөлімшені, пайдаланылатын ақпараттық жүйелерді, жабдықты және Университеттің қолданыстағы жергілікті нормативтік құжаттарын ескере отырып айқындайды.

Осы аудит шеңберінде мынадай мәселелер тексерілуі мүмкін:

1) ақпараттық қауіпсіздік бойынша бекітілген және өзекті құжаттардың болуы;
2) ақпаратты өңдеу құралдарымен байланысты активтердің өзекті тізілімінің болуы;
3) ақпараттық жүйелерді, сервистерді және жабдықты пайдалануға жауапты тұлғалардың болуы;

Б қосымшасының жалғасы

4) пайдаланушылардың қолжетімділік құқықтарын беру, өзгерту және жою тәртібі;
5) есептік жазбалар мен парольдерге қойылатын талаптардың сақталуы;
6) жұмыстан босатылған қызметкерлердің есептік жазбаларын уақтылы бұғаттау;
7) жұмыс станциялары мен серверлерде вирусқа қарсы қорғаныстың болуы және өзектілігі;
8) операциялық жүйелердің, қолданбалы бағдарламалық қамтамасыз етудің және вирусқа қарсы базалардың тұрақты жаңартылуы;
9) белгіленген кесте бойынша резервтік көшірме жасаудың орындалуы;
10) ақпараттың резервтік көшірмесін жасау және қалпына келтіру журналдарының болуы;
11) деректерді тестілік қалпына келтіруді жүргізу;
12) АҚ инциденттерін тіркеу және штаттан тыс жағдайларды есепке алу журналын жүргізу;
13) Интернет желісін пайдалану қағидаларының сақталуы;
14) корпоративтік электрондық поштаны пайдалану қағидаларының сақталуы;
15) серверлік және желілік жабдыққа физикалық қолжетімділік шектеулерінің болуы;
16) серверлік жабдықты қауіпсіз пайдалану үшін жағдайлардың болуы;
17) жергілікті есептеу желісі схемасының болуы;
18) АҚ рәсімдерінің орындалуын растайтын журналдардың, есептердің, өтінімдердің және өзге де жұмыс құжаттарының болуы.
19) нақты ішкі аудиттің мақсаты мен саласына қатысты өзге де мәселелер.

12. Аудит жүргізу әдістері:

Аудит жүргізу кезінде мынадай әдістер қолданылады:
1) құжаттарды талдау;
2) журналдар мен есептерді талдау;
3) жабдықтар мен үй-жайларды қарап-тексеру;
4) ақпараттық жүйелер мен сервистердің баптауларын тексеру;
5) қызметкерлермен әңгімелесу;
6) ақпараттық қауіпсіздік оқиғаларын талдау;
7) мониторинг және әкімшілендіру құралдарын пайдалану.

13. Есепті ұсыну күні_____

Аудиторлық топтың жетекшісі:

Лауазымы _____ А. Тегі
(қолы)

Аудиторлар:

Лауазымы _____ А. Тегі
(қолы)

Лауазымы _____ А. Тегі
(қолы)

Келісілді
Тексерілетін құрылымдық бөлімшенің басшысы

Лауазымы _____ А. Тегі
(қолы)

В қосымшасы

Ішкі аудит туралы есептің үлгісі

«Ахмет Байтұрсынұлы атындағы Қостанай өңірлік университеті» КЕАҚ

Бекітемін
Лауазымы
_____Т.А.Ә.
_____202 __ж.

АҚ ІШКІ АУДИТІ ТУРАЛЫ № _____ ЕСЕП

1. Жалпы мәліметтер

№	Көрсеткіш	Мәліметтер
1.	Тексерілетін құрылымдық бөлімше	
2.	Аудит объектісі	
3.	Құрылымдық бөлімшенің басшысы	
4.	Аудиторлық топтың жетекшісі	
5.	Аудиторлар	
6.	Аудит жүргізілген күн	
7.	Аудит жүргізу негізі	
8.	Сәйкестігіне аудит жүргізілген құжаттар	

2. Аудит нәтижелері

№	Көрсеткіш	Саны / белгісі	Ескертпе
1	Анықталған сәйкессіздіктер		
2	Анықталған осалдықтар		
3	Ұсыныстар мен ұсынымдар		

3. Аудит нәтижелері бойынша анықталған сәйкессіздіктер/осалдықтар және түзету іс-шаралары

1. № 1 сәйкессіздік/осалдық
АҚ ішкі аудитін жүргізу барысында мынадай сәйкессіздік/осалдық анықталды:

_____

_____

Негіздеме / бұзылған талап:

_____

В қосымшасының жалғасы

Жою жөніндегі ұсыным:

---

4. Аудит нәтижелері бойынша қорытынды

_____ қызметі
бөлімшенің атауы
белгіленген талаптарға сәйкес келеді / сәйкес келмейді_____

Түзету іс-шаралары (жоспар):

№	Түзету іс-шарасы	Жауапты орындаушы	Орындау мерзімі
1			
2			
3			

Қайталама ішкі аудит жүргізу қажеттілігі: ИӘ / ЖОҚ.

Ұсыныстар мен ұсынымдар

Құрастырған:

Аудиторлық топтың жетекшісі:

Лауазымы _____ А. Тегі
(қолы)

Аудиторлар:

Лауазымы _____ А. Тегі
(қолы)

Лауазымы _____ А. Тегі
(қолы)

Есеппен таныстым:

Тексерілетін құрылымдық бөлімшенің басшысы

Лауазымы _____ А. Тегі
(қолы)