БЕКІТЕМІН
Ө.Жәнібеков атындағы ОҚПУ
Басқарма төрағасы-Ректордың
уақытша міндетін атқарушы
_____Г.Д. Сугирбаева
«16» 10 2025 ж.

САПА МЕНДЖМЕНТІ ЖҮЙЕСІ

АҚПАРАТТЫҚ ҚАУІПСІЗДІК ТУРАЛЫ

ЕРЕЖЕ

СМЖ ОҚПУ Е 6.12-2025

қызметі	*қолы*	*А.Ж.Т.*
Келісілді:		
Басқарма мүшесі – Ғылыми жұмыстар және инновациялар жөніндегі проректор		Керімбеков Е.Р.
Стратегиялық жоспарлау және менеджмент бөлімінің басшысының у.м.а.		Иманбердиева М.Н.
Заң бөлімінің басшысы		Амирхан М.А.

қызметі	*қолы*	*А.Ж.Т.*
Әзірлеген:		
IT департаментінің директоры		Инкарбеков С.А.
Бағдарламалық және техникалық қызмет көрсету бөлімінің басшысы		Байырбекова Л.М.

Құжаттың жарамдылық мерзімі: «16» 10 2025 ж. «13» 10 2028 ж. дейін ұзартылды: «___» _____ 20__ г.	Енгізілді: № 3 бұйрық Енгізілген күні: «16» 10 2025 ж.	**СМЖ ОҚПУ Е 6.12-2025** Басылым 1 Тіркеу №___ Көшірме №___

Мазмұны

1 Қолдану саласы

1.1 Осы Ақпараттық қауіпсіздік туралы ереже (АҚ ережесі) «Өзбекәлі Жәнібеков атындағы Оңтүстік Қазақстан педагогикалық университетінің» ақпараттық-коммуникациялық инфрақұрылымының (бұдан әрі – АҚИ) қазіргі жай-күйі мен даму болашағын ескере отырып әзірленді. Ережеде пайдалану мақсаттары, міндеттері мен құқықтық негіздері, жұмыс істеу режимдері, сондай-ақ қауіпсіздік қатерлерінің талдауы сипатталған.

1.2 Қазіргі Ақпараттық қауіпсіздік ережесі университеттің құрылымдық бөлімшелеріне қолданылады, онда әкімшілік деректерді, шектеулі таралымдағы ақпаратты (қызметтік ақпаратты) немесе жеке деректерді, соның ішінде автоматтандырылған өңдеуді жүзеге асыратын ақпарат өңделеді. Сондай-ақ, университеттің ақпараттық жүйелерінің жұмыс істеуін әзірлеу, қолдау және қызмет көрсету жұмыстарын жүзеге асыратын ұйымдарға да қатысты.

1.3 Басқа ақпараттық жүйелердің ақпараттық қауіпсіздік талаптарының қолдану ауқымы олардың иелерімен анықталады. Егер осы ақпараттық жүйелер университеттің ақпараттық-коммуникациялық инфрақұрылымының құрамына кіретін болса, ақпараттық қауіпсіздік шарттары ақпараттық жүйенің иесі мен университет арасындағы келісімшарттар немесе өзара әрекеттесу ережелері шеңберінде реттеледі.

1.4 Осы Ереже университеттің барлық бөлімдеріне міндетті тәртіпте ұсынылуы тиіс.

1.5 Ереже авторлық құқық болып табылады және оны Басқарма төрағасы - ректор рұқсатынсыз бөгде ұйымдарға беруге жол берілмейді.

2 Нормативті сілтемелер

2.1 Осы Ережеде келесі нормативті құжаттарға сілтемелер пайдаланылды:

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

ҚР ҚН 202-05-2009 «Ғимараттар мен құрылыстардың өрт қауіпсіздігі»;

ҚР ҚН 3.02-17-2011 «Құрылымдық кабельдік жүйелер. Жобалау нормалары»;

ҚР СТ 34.005-2002 «Ақпараттық технологиялар. Негізгі терминдер мен анықтамалар»;

ҚР СТ 34.006-2002 «Ақпараттық технологиялар. Деректер қоры. Негізгі терминдер мен анықтамалар»;

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

ҚР СТ ISO/IEC 17799-2006 «Ақпараттық технологиялар. Қорғау әдістері. Ақпараттық қауіпсіздік басқармасының ережелер жинағы»;

ҚР СТ ISO/IEC 27002-2015 «Қауіпсіздік құралдары. Ақпараттық қауіпсіздікті басқару ережелер жинағы».

СМЖ ОҚПУ ПР 4.01-2023 Сапа менеджменті жүйесі. Құжатталған ақпаратты басқару.

3 Терминдер мен анықтамалар

Ережеде келесі терминдер мен анықтамалар

Аутентификация – ұсынылған қолжетімділік деректері жүйеде іске асырылған рұқсаттармен сәйкестігін анықтау арқылы субъектінің немесе объектінің шынайылығын растау.

Деректер қоры (ДҚ) – осы деректердің сипаттамаларын және олардың объектілері арасындағы байланыстарды сипаттайтын тұжырымдамалық құрылымға сәйкес ұйымдастырылған деректер жиынтығы.

Ақпараттық жүйенің ақпараттық қауіпсіздік деңгейлері бойынша жіктелуі – ақпараттық қауіпсіздік талаптарының деңгейі бойынша ақпараттық жүйелерді кластарға бөлу.

Ақпараттық ресурстар (АР) – ақпараттық жүйелерде сақталатын мәтіндік, графикалық, аудио, бейне және т.б. деректер жиынтығы.

Ақпараттық жүйе (АЖ) – ақпаратты сақтау, өңдеу, іздеу, тарату, беру және ұсынуға арналған аппараттық-бағдарламалық кешенді қолданатын жүйе.

Ақпараттық қауіпсіздік (АҚ) – ақпараттың немесе оны өңдеу құралдарының құпиялылығын, тұтастығын, қолжетімділігін, орнықтылығын, есептілігін, аутенттілігін және шынайылығын анықтау, қамтамасыз ету және сақтау аспектілері.

Электрондық ақпараттық ресурстар (ЭАР) – ақпараттық жүйелерде сақталған, тиісті бағдарламалық қамтамасыз етумен біріктірілген және ақпарат пайдаланушылары үшін қызығушылық тудыратын электронды жүйеленген ақпарат жиынтықтары (ақпараттық деректер қоры).

Ақпараттық-коммуникациялық инфрақұрылым (АҚИ) – есептеу техникасы құралдары, телекоммуникациялық жабдықтар, деректерді беру арналары, АЖ, коммутация және ақпарат ағындарын басқару құралдары жиынтығы.

Локалды-есептеу желісі (ЛЕЖ) – шағын аумақта орналасқан абоненттерді біріктіретін желі.

Ақпаратқа рұқсат етілмеген қолжетімділік (РҚҚ) – есептеу техникасы немесе автоматтандырылған жүйелер арқылы ұсынылған қалыпты құралдарды пайдалана отырып, қолжетімділікті шектеу ережелерін бұзатын ақпаратқа қол жеткізу.

Нормативтік құқықтық актілер (НҚА) – белгіленген нысанда қабылданған және заңдық нормаларды белгілейтін, өзгертетін, тоқтататын

немесе тоқтата тұратын жазбаша ресми құжат, сондай-ақ электрондық цифрлық қолтаңбамен куәландырылған электронды нұсқасы.

АЖ пайдаланушысы – қажетті электрондық АР алу үшін АЖ-ға жүгінетін және оларды пайдаланатын субъект.

Бағдарламалық қамтамасыз ету (БҚ) – ақпаратты өңдеу жүйесінің компьютерлік бағдарламалары мен осы бағдарламаларды пайдалануға қажетті құжаттар жиынтығы.

Қолданбалы БҚ (ҚБҚ) – нақты қолданбалы міндеттерді шешуге арналған бағдарламалар.

IT департаменті (ИТД) – байланыс арналарының жұмыс істеуін, компьютерлік жабдықтар мен базалық БҚ-ның қызметін техникалық сүйемелдеу және қолдауды жүзеге асырады.

Серверлік бөлме – серверлік, белсенді және пассивті желілік (телекоммуникациялық) жабдықтар мен құрылымдық кабельдік жүйе жабдықтарын орналастыруға арналған бөлме.

Деректер қорын басқару жүйесі (ДҚБЖ) – ДҚ басқаруды қамтамасыз ететін бағдарламалық және тілдік құралдар жиынтығы.

Жүйелік БҚ – есептеу құрылғыларының жұмыс істеуін қамтамасыз етуге арналған компьютерлік бағдарламалар жиынтығы.

Жүйелік әкімші (ЖӘ) – сервердің дұрыс жұмыс істеуі мен сервердегі БҚ баптауға жауапты тұлға.

Инженер-бағдарламашы – компьютерлік бағдарламаларды жасау арқылы бағдарламалау жұмысымен айналысатын маман.

Техникалық қолдау қызметі – пайдаланушылардың компьютерлік жабдықтарымен (аппараттық және бағдарламалық) және кеңсе техникасымен байланысты мәселелерін шешетін сервистік құрылым.

Арнайы БҚ – көмекші және қызметтік міндеттерді шешуге арналған компьютерлік бағдарламалар.

Есептеу техникасы құралдары (ЕТҚ) – ақпаратты өңдеу жүйелерінің, соның ішінде енгізу немесе шығару элементтерінің, жеке немесе басқа жүйелер құрамында жұмыс істей алатын техникалық және бағдарламалық элементтер жиынтығы.

Интернет желісі – халықаралық ресурстарға қолжетімділікті қамтамасыз ететін желілер жүйесі.

4 Белгілер мен қысқартулар

Ережеде келесі белгілер мен қысқартулар пайдаланылған:

ҚР – Қазақстан Республикасы;

СМЖ-сапа менеджменті жүйесі;

КЕАҚ - коммерциялық емес акционерлік қоғам;

ОҚПУ - Оңтүстік Қазақстан педагогикалық университеті;

СМЖ – сапа менеджменті жүйесі;

Е – ереже;
ОПҚ – профессор-оқытушылар құрамы;
ДҚ – Деректер қоры
АР – Ақпараттық ресурстар
АЖ - Ақпараттық жүйе
АҚ - Ақпараттық қауіпсіздік
ЭАР - Электрондық ақпараттық ресурстар
АҚИ- Ақпараттық-коммуникациялық инфрақұрылым
ЛЕЖ - Локалды-есептеу желісі
РҚҚ - Ақпаратқа рұқсат етілмеген қолжетімділік
НҚА - Нормативтік құқықтық актілер
БҚ - Бағдарламалық қамтамасыз ету
ҚБҚ - Қолданбалы бағдарламалық қамтамасыз ету
ИТД - IT департаменті
ДҚБЖ - Деректер қорын басқару жүйесі
ЖӘ - Жүйелік әкімші
ЕТҚ - Есептеу техникасы құралдары

5 Жауапкершілігі мен өкілеттілігі

5.1 Ережені университеттің Басқарма төрағасы - ректоры бекітеді.

5.2 Осы Ережелерде көрсетілген талаптарды енгізілуін және орындалуы жөніндегі жауапкершілік Ғылыми жұмыстар және инновациялар жөніндегі проректорға, IT департаментінің директорына жүктеледі.

5.3 Университеттің құрылымдық бөлімшелерінің басшылары өз бағынысты қызметкерлерін, соның ішінде жаңа қабылданған қызметкерлерді, осы ақпараттық қауіпсіздік ережесімен таныстыруға жауапты.

5.4 Ақпараттық қауіпсіздік ережесінің талаптарының бұзылуы нәтижесінде университетке моральдық және материалдық зиян келтірілген жағдайда, кінәлі қызметкерлер Қазақстан Республикасының заңнамасына сәйкес жауапкершілікке тартылады.

5.5 Ақпараттық қауіпсіздік ережесінің талаптарының бұзылуы еңбек міндеттерін орындамау немесе дұрыс орындамау түрінде тәртіптік құқық бұзушылық болып саналады. Ақпараттық қауіпсіздік ережесін бұзған қызметкер Қазақстан Республикасының Еңбек кодексіне сәйкес тәртіптік жауапкершілікке тартылады.

5.6 Ережеге өзгерістерді **(А Қосымшасы)** "Өзгерістерді тіркеу парағына" міндетті түрде белгілей отырып, IT департаментінің директоры енгізеді.

6 Жалпы ереже

6.1 АҚ ережесінің негізгі мақсаттары:

1. өңделетін ақпараттың қолжетімділігі;
2. университеттің АҚИ-ның тұрақты жұмыс істеуі;

3. есептеу техникасында (ЕТҚ) сақталатын және байланыс арналары арқылы берілетін ақпараттың құпиялылығын қамтамасыз ету;

4. университеттің ақпараттық жүйелерінде (АЖ) сақталатын және өңделетін, сондай-ақ байланыс арналары арқылы берілетін ақпараттың тұтастығы мен аутенттілігін қамтамасыз ету.

6.2 Мақсаттарға қол жеткізу үшін келесі міндеттер қойылады:

- университетте АҚ-ні қамтамасыз ету бойынша бірыңғай саясатты қалыптастыру және жүргізу;
- университеттің үздіксіз жұмыс істеуін қамтамасыз ету және АҚ қатерлерінің алдын алу, оларды болдырмау арқылы экономикалық залалды барынша азайту;
- ақпараттық қауіпсіздік қатерлерін анықтау, оларды тойтару және олардың салдарын жоюға бағытталған рәсімдерді айқындау;
- университет аясындағы ақпараттандыруды басқару рәсімдерінің мазмұнына қойылатын талаптарды анықтау, олар арқылы АҚ міндеттерін шешу қамтамасыз етіледі;
- АҚИ шеңберінде жұмыстарды жүргізу кезінде АҚ стандарттарының талаптарын сақтау бойынша университет қызметін үйлестіру;
- университеттің АҚИ-ның қорғалу деңгейін арттыру;
- АҚ ережесінің негізінде АҚ басқару жүйесі құрылады.

6.3 Ақпараттық қауіпсіздік ережесі

6.3.1 Қазіргі Ақпараттық қауіпсіздік ережесі Қазақстан Республикасының ақпараттық қауіпсіздік саласындағы заңнамасының принциптері мен талаптарына және ұсыныстарына негізделіп, соның ішінде осы Ақпараттық қауіпсіздік ережесінің 1-бөлімінің 1.26 тармағында көрсетілген құжаттарға сүйене отырып әзірленген.

6.3.2 Ақпараттық қауіпсіздікті қамтамасыз ету дегеніміз — ақпараттың құпиялылығын, тұтастығын және қолжетімділігін сақтау. Ақпараттың құпиялылығы — ақпаратқа тек уәкілетті тұлғаларға ғана қолжетімділік беру арқылы қамтамасыз етіледі; тұтастығы — деректерге тек уәкілетті өзгерістер енгізу арқылы қамтамасыз етіледі; қолжетімділігі — қызметтік міндеттерді орындау үшін деректерге уәкілетті тұлғаларға қолжетімділік беру арқылы қамтамасыз етіледі.

6.3.3 Университеттің Ақпараттық қауіпсіздік ережесі әдістемелік база болып табылады:

- ақпаратты қорғауға бағытталған нормативтік, құқықтық, технологиялық және ұйымдастырушылық шаралардың кешенін әзірлеу және жетілдіру үшін;
- ақпараттық қауіпсіздікті қамтамасыз ету үшін;
- ақпараттық қауіпсіздік талаптарын орындау бойынша жұмыстарды жүргізген кезде университеттің құрылымдық бөлімшелерінің қызметін үйлестіру үшін.

6.3.4 Осы Ақпараттық қауіпсіздік ережесінің талаптары мен шарттары университеттің барлық ақпараттық жүйелеріне қолданылады.

6.4 Ақпараттық қауіпсіздікті қамтамасыз ету ұйымдастыруы

6.4.1 Ақпаратты қорғау жүйесінің тікелей ұйымдастырылуы (құрылуы) және тиімді жұмысын қамтамасыз етуге жауапты:

- ДИТ — ақпараттық-коммуникациялық инфрақұрылымды (ИКИ), СВТ, ақпараттық жүйелерді (ИС) және ақпараттық қауіпсіздікті (АҚ) жүзеге асыратын құрылымдық бөлімше;
- ДИТ курирлейтін проректормен және университет басқарма мүшесімен келісіп, ақпаратты рұқсатсыз қолжетімділіктен қорғауға бағытталған шараларды дамыту негізгі бағыттарын анықтайды.

6.5 Ақпараттық жүйелердің пайдаланушы категориялары

6.5.1 Ақпараттық жүйелердің пайдаланушы категорияларына мыналар жатады:

1. ішкі пайдаланушылар — университет қызметкерлері, ақпараттық ресурстарға (АР) уәкілетті қолжетімділігі бар, өз қызметін атқаратын және Қазақстан Республикасының заңнамасына сәйкес негізгі құқықтары мен міндеттеріне ие тұлғалар;
2. сыртқы пайдаланушылар — университет қызметтерін тұтынушылар, соның ішінде университеттің ақпараттық ресурстарын пайдаланатын тұлғалар;
3. көмекші персонал — қызмет көрсету, техникалық персонал және университетте өзара әрекеттесетін басқа ақпараттық жүйелердің иелері, оның ішінде:

- жергілікті желілер әкімшілері, телекоммуникациялық жабдықты қолдауға жауапты тұлғалар;
- қауіпсіздік қызметі (ҚҚ);
- бағдарламалық қамтамасыз етуді әзірлеушілер;
- техникалық мамандар (жүйелік-техникалық қызмет көрсету) және басқалар.

6.6 Ақпараттық қауіпсіздік объектілері

6.6.1 Университеттің ақпараттық қауіпсіздігінің негізгі қорғау объектілері:

- шектеулі қолжетімді ақпараттық ресурстар (АР), олардың құпиялығы сақталуы тиіс, рұқсатсыз әсерлер мен қауіпсіздіктің бұзылуына сезімтал, соның ішінде ашық (қоғамға қолжетімді) ақпарат, оның берілу формасы мен түріне қарамастан;
- ақпараттық жүйелердегі (АЖ) ақпаратты өңдеу процестері мен адами ресурстар — ақпараттық технологиялар, ақпаратты жинау, өңдеу, сақтау және беру ережелері мен процедуралары, әзірлеушілер персоналы, жүйенің ішкі пайдаланушылары және оның қызмет көрсетуші персоналы;

- ақпараттық инфрақұрылым, оған ақпаратты өңдеу және талдау жүйелері, беру және көрсету жүйелері, соның ішінде ақпарат алмасу арналары, ақпараттық ресурстар мен АЖ құрамдастары орналасқан нысандар мен бөлмелер кіреді.

6.6.2 Ақпараттық инфрақұрылым объектілері мыналарды қамтиды:

- технологиялық жабдықтар (СВТ, желілік және кабельдік жабдықтар);
- шектеулі қолжетімді ақпараттық ресурстар;
- бағдарламалық қамтамасыз ету (операциялық жүйе (бұдан әрі — ОЖ), дерекқорды басқару жүйелері (ДББЖ), басқа жүйелік және бағдарламалық қамтамасыз ету);
- автоматтандырылған байланыс және деректерді беру жүйелері (телекоммуникациялық құралдар);
- ақпарат берілетін байланыс арналары (соның ішінде шектеулі таралымдағы ақпарат үшін);
- шектеулі таралымдағы ақпарат айналатын қызметтік бөлмелер;
- ақпаратты өңдемейтін, бірақ қызметтік ақпарат айналатын бөлмелерде орналасқан техникалық құралдар мен жүйелер.

6.7 Қорғалуы тиіс ақпараттық ресурстар категориялары

6.7.1 Университеттің ақпараттық жүйелерінің (АЖ) подсистемаларында шектеулі таралымдағы ақпарат (жеке деректер, қызметтік, қаржылық ақпарат) және ашық ақпарат айналады.

6.8 Ақпараттық қауіпсіздік ережесін жүзеге асыру шаралары

6.8.1 Университеттің ақпараттық-коммуникациялық инфрақұрылымында (ИКИ) жұмыс істейтін ішкі пайдаланушылар университеттің Ақпараттық қауіпсіздік ережесінде белгіленген талаптарды қатаң сақтауға міндетті.

6.8.2 Ақпараттық қауіпсіздік мамандары мен қызметкерлерінің функционалдық міндеттері университеттің ішкі реттеуші құжаттарымен және лауазымдық нұсқаулықтарымен белгіленеді және Ақпараттық қауіпсіздік ережесі мен Қазақстан Республикасының мемлекеттік стандарты СТ РК ИСО/МЭК 27002-2015 «Қамтамасыз ету құралдары. Ақпаратты қорғауды басқару ережелер жинағы» 8.1.1 тармағы талаптарына сәйкес құжатталады.

6.8.3 «Оңтүстік Қазақстан педагогикалық университеті Өзбекәлі Жәнібеков атындағы» жауапкершілігі шектеулі акционерлік қоғамы туралы, қызметтік, коммерциялық және заңмен қорғалатын басқа құпия ақпараттың сақталуын қамтамасыз ету жөніндегі нұсқаулық.

6.8.4 Ақпараттық қауіпсіздік үшін жауапты тұлға ақпаратты қорғау мәселелері мен жұмыстарын ұйымдастырып, бақылайды және үйлестіреді, бұл Қазақстан Республикасының мемлекеттік стандарты СТ РК ИСО/МЭК 27002-2009 «Қамтамасыз ету құралдары. Ақпаратты қорғауды басқару ережелер жинағы» 6.1.2-6.1.7 тармақтарының талаптарына сәйкес жүзеге асырылады.

6.8.5 Ақпараттық қауіпсіздік үшін жауапты тұлға ақпараттық қауіпсіздікті қамтамасыз ету аясында келесі жұмыстарды атқарады:

1. техникалық спецификацияларды әзірлеуге, бағдарламалық-жабдықтық кешендерді жобалауға және сатып алу процесіне қатысу;
2. университет аясында ақпараттық қауіпсіздікті қамтамасыз ететін аппараттық және бағдарламалық құралдарды практикалық енгізу;
3. ақпараттық жүйелерді құру, дамыту және қолдану кезінде ақпараттық қауіпсіздік талаптарын қалыптастыруға қатысу;
4. қорғаныс жүйесін жобалау, сынау және оны пайдалану қабылдау жұмыстарында қатысу;
5. уәкілетті ішкі пайдаланушыларға қажетті қорғаныс реквизиттерін бөлу;
6. қорғаныс жүйесінің және оның элементтерінің жұмысын бақылау;
7. ішкі пайдаланушыларды ақпаратты қауіпсіз өңдеу талаптары туралы хабардар ету;
8. ішкі пайдаланушылардың автоматтандырылған өңдеу кезінде қорғалатын ақпаратпен жұмыс істеу ережелерін сақтауын бақылау;
9. ақпаратқа рұқсатсыз қолжетімділік әрекеттері анықталғанда және қорғаныс жүйесінің жұмыс істеу ережелері бұзылғанда қажетті шараларды қабылдау;
10. ақпараттық қауіпсіздіктің ішкі аудиті мен мониторингіне қатысу;
11. ақпаратты қорғау үшін криптографиялық құралдарды қолдану жөнінде ұсыныстар енгізу;
12. университеттің ақпараттық жүйелеріне қолжетімді құқықтарды шектеуді қамтамасыз ету.

6.8.6 Ақпараттық қауіпсіздік үшін жауапты тұлға мен ДИТ қызметкерлері ақпараттық қауіпсіздік саласында біліктілігін арттыру курстарына үнемі жіберілуі тиіс.

6.8.7 Университеттің ақпараттық-коммуникациялық инфрақұрылымында жұмыс істейтін ішкі және сыртқы пайдаланушылар қажет болған жағдайда (немесе құпия ақпаратты қамтитын немесе өңдейтін жабдыққа қолжетімділік деңгейі болған кезде) оқудан өтеді.

6.9 Ақпараттық қауіпсіздік және қауіпсіздік қызметі үшін жауапты тұлғаның ұйымдастырушылық-құқықтық мәртебесі

6.9.1 Ақпараттық қауіпсіздік үшін жауапты тұлға келесі құқықтарға ие:

- университеттің ақпараттық инфрақұрылымын бақылау және мониторинг жүргізу;
- университеттегі ақпараттық жүйелер (АЖ), есептеу техникасы (СВТ) және жергілікті желілер (ЖЖ) орнатылған барлық бөлмелерге қол жеткізу;
- қорғалатын ақпаратқа тікелей қауіп төніп тұрған жағдайда автоматтандырылған ақпарат өңдеуді тоқтату.

6.9.2 Қауіпсіздік қызметі (ҚҚ) ақпараттық қауіпсіздік үшін жауапты тұлғамен келісім бойынша:

- университеттегі ақпараттық жүйелер, есептеу техникасы және жергілікті желілер орнатылған барлық бөлмелерге қол жеткізу құқығына ие;
- қорғалатын ақпаратқа тікелей қауіп төніп тұрған жағдайда автоматтандырылған ақпарат өңдеуді тоқтату құқығына ие.

6.1.10 Құпиялылықтың жалпы талаптары

6.10.1 Құпиялылықтың негізгі талаптары — кез келген құпия ақпараттың ағып кетуін (ашылуын) болдырмау және ақпаратты тек уәкілетті тұлғаларға беруін қамтамасыз ету.

6.10.2 Университеттің ақпараттық жүйелеріне ішкі пайдаланушылардың қосылуы толық және мұқият тіркелуі тиіс, бұл ақпарат кемінде 1 жыл бойы сақталуы керек (логирование).

6.10.3 Университеттің ақпараттық жүйелерінде өңделетін және сақталатын қызметтік және басқа да қорғалатын ақпаратты көшіріп алу және үшінші тұлғаға беру тек университеттің курирлейтін проректоры — басқарма мүшесінің ресми рұқсатымен жүзеге асырылады.

6.10.4 Университеттің ақпараттық жүйесімен жұмыс істегенде, ішкі пайдаланушының монитор экранында көрсетілген ақпаратқа бөтен адамдардың қарауы мүмкіндігі болмауы тиіс.

6.10.5 Университеттің ақпараттық жүйесімен жұмыс істегенде, зиянды бағдарламалардан, вирустардан және желілік шабуылдардан қорғауды қамтамасыз ететін арнайы лицензияланған бағдарламалық немесе аппараттық құралдар қолданылуы тиіс. Негізгі бағдарламалық қамтамасыз ету кешеніне есептеу техникасының жұмыс қабілеттілігін қамтамасыз ететін лицензияланған бағдарламалық қамтамасыз ету кіреді.

6.10.6 Университеттің ақпараттық жүйесімен жұмыс істегенде ішкі пайдаланушылар мен көмекші персоналдың құпиялылық талаптарын сақтауы құпиялылық туралы келісім арқылы қамтамасыз етіледі.

6.11 **Жүйедегі пайдаланушыларды аутентификациялау талаптары**

6.11.1 Университеттің ақпараттық жүйесінде жұмыс істейтін барлық ішкі пайдаланушылар авторизацияланған деректердің ағып кетуін және ұрлануын болдырмайтын қауіпсіз аутентификациядан өтуі тиіс.

6.11.2 Ішкі пайдаланушыларды аутентификациялау үшін ақпараттық жүйеде бірегей идентификациялық есептік жазбалар (логин, пароль) құрылады.

6.11.3 Есептік жазба туралы мәліметтердің сақталуы мен құпиялылығына жауапкершілік ішкі пайдаланушыларға жүктеледі.

6.11.4 Ішкі пайдаланушылардың есептік жазбалары тиісті құжаттар немесе жазбалар болған жағдайда ғана құрылып, жойылуы тиіс.

6.11.5 Ішкі пайдаланушылар мен қызмет көрсетуші персоналдың пароль қорғауын ұйымдастыру талаптары: жеке пароль кемінде 8 таңбадан тұруы, жалпы сөздіктегі сөздерді қамтымауы және келесі таңбалар жиынтығынан кем дегенде үшеуін қамтуы тиіс:

а) бас әріптер: A, B, C;

ә) кіші әріптер: a, b, c;

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

6.12 Ақпаратты байланыс желілері арқылы беру кезіндегі құпиялылық талаптары

6.12.1 Университеттің ақпаратын беру өздерінің немесе жалға алынған талшықты-оптикалық арналары арқылы, үлкен қашықтықтарға жүзеге асырылуы тиіс.

6.12.2 Серверлік, телекоммуникациялық жабдықтар және құрылымдық кабельдік жүйелер техникалық реттеу талаптарына сәйкес келетіні туралы құжаттық растамалары болуы және ақпараттық қауіпсіздік талаптарына сәйкестігін растайтын сертификатқа ие болуы қажет.

6.12.3 Университеттің электрондық пошта мекенжайларын сайттарға тіркелу кезінде немесе форумдар мен интернет-конференцияларға қатысу кезінде пайдалану тыйым салынады (тек қызметкердің кәсіби қызметіне қатысты іс-шараларда қолданылатын жағдайларды қоспағанда).

6.12.4 Құпия ақпаратпен жұмыс істейтін қызметкерлерге жалпыға қолжетімді интернет пошта сервистерін және жедел хабар алмасу жүйелерін қолдануға тыйым салынады.

6.13 Қоғамға қолжетімді ресурстарды қорғау талаптары

6.13.1 Ресми интернет-ресурс біріккен Интернет-ресурстар платформасында орналастырылады және edu.kz домендік аймағында тіркеледі (zhanibekov.edu.kz).

6.13.2 Интернет-ресурстардың ақпараттық қауіпсіздігін қамтамасыз ету үшін келесі міндеттерді орындайтын мазмұнды басқару жүйесін (контентті басқару) қолдану қажет:

- ақпараттық контентті орналастыру, өзгерту және жою операцияларын санкциялау;
- ақпараттық контентті орналастыру, өзгерту және жою кезінде авторлықты тіркеу;
- жүктелетін контентті зиянды кодқа тексеру;
- орналастырылған ақпараттық контенттің тұтастығын бақылау;
- пайдаланушылар мен бағдарламалық роботтардың аномальды белсенділігін бақылау.

6.13.2 Құпиялылықты қамтамасыз ету мақсатында келесі іс-шаралар ұйымдастырылуы тиіс:

- жыл сайын ресми тіркелген пайдаланушылар мен ақпараттық жүйеде жұмыс істейтін пайдаланушылар тізімін сәйкестендіру;
- ақпараттық қауіпсіздік бойынша жыл сайын аудит жүргізу, осы Құжаттың талаптарына сәйкес;
- университеттің ИКИ ақпараттық қауіпсіздік құралдарымен тұрақты мониторинг жүргізу.

6.14 Тұтастыққа қойылатын жалпы талаптар

6.14.1 Тұтастыққа қойылатын негізгі талап — ақпаратқа тек авторизацияланған тұлғалардың ғана өзгерістер енгізуін қамтамасыз ету.

6.14.2 Университеттің ақпараттық жүйесінің тұтастығы мен қауіпсіздігін қамтамасыз ету үшін жаңа немесе әзірленген бағдарламалық қамтамасыз етуді орнатудан және қолданыстағы бағдарламалық қамтамасыз етуді жаңартудан бұрын ақпараттық қауіпсіздік талаптарына сәйкестігін мұқият тексеру және сынау процедуралары енгізілуі тиіс.

6.15 **Ақпараттық жүйенің қауіпсіздігіне қойылатын талаптар — әзірлеу, жетілдіру және қызмет көрсету кезінде**

6.15.1 Ақпараттық қауіпсіздікті қамтамасыз ету элементтеріне қойылатын талаптар ақпараттық жүйені әзірлеуден бұрын анықталып, ақпараттық қауіпсіздік үшін жауапты тұлғамен келісіліп, университеттің курирлейтін проректорына — Басқарма мүшесіне бекітуге ұсынылуы тиіс.

6.15.2 Бағдарламалық қамтамасыз етуді әзірлеу немесе бастапқы кодты өзгерту қызмет көрсету аясында әзірлеу ортасында жүзеге асырылуы қажет.

6.15.3 Өзгертілген бағдарламалық құрал ақпараттық қауіпсіздік талаптарына сәйкестігі және басқа бағдарламалармен үйлесімділігін тексеру үшін тестілеуден өтуі керек. Тестілеуді әзірлеушілер ақпараттық қауіпсіздік үшін жауапты тұлғамен бірге жүргізеді, тестілеу нәтижелері тестілеу хаттамасында көрсетілуі тиіс.

6.15.4 Бағдарламалық қамтамасыз етуді эксплуатациялық ортаға іске қосу тек оң қорытындысы бар тестілеу хаттамасы болған жағдайда жүзеге асырылады.

6.15.5 Қауіпсіздік талаптары ақпараттық активтердің құндылығын және бизнес-процесске келетін ықтимал залалды ескеруі тиіс.

6.16 Ақпараттық қауіпсіздікті қамтамасыз ететін деректерді беру желісінің құрамдас бөліктеріне қойылатын талаптар

6.16.1 Университеттің ақпараттық жүйелерінің қауіпсіз жұмысын қамтамасыз ету үшін әртүрлі бөлімшелердің ақпарат ағындарының бөлінуі мен оқшауланuын қамтамасыз ететін техникалық шешімдерді, жүйеге кіруді бақылау және шектеу үшін желілік экрандарды (фаерволдарды), сондай-ақ басып кіруді анықтау және болдырмау жүйелерін пайдалану қажет.

6.16.2 Құқықсыз қосылудан коммуникацияларды қорғау авторизацияланған электрондық және физикалық қолжетімділік құралдарынан басқа бағдарламалық, техникалық және ұйымдастырушылық шаралармен жүзеге асырылады. Қажетті шаралар уақтылы анықтау, ескерту және заңсыз әрекеттерді тоқтату үшін қабылдануы тиіс.

6.17 Қауіпсіздік оқиғаларын басқару талаптары

6.17.1 Ақпараттық қауіпсіздік бұзылған жағдайда дереу ақпараттық қауіпсіздік үшін жауапты тұлғаға хабарлануы тиіс.

6.17.2 Ақпараттық қауіпсіздік жүйесіндегі оқиғаларға жылдам, нәтижелі және тәртіпті әрекет етуді қамтамасыз ету үшін жауапкершілік аймақтары мен процедуралары анықталуы қажет.

6.17.3 Ақпараттық қауіпсіздік жүйесіндегі оқиғаларды мониторинг жүргізу және оларды үнемі бақылау үшін механизмдер қабылдануы тиіс.

6.18 Ақпаратты рұқсатсыз қол жеткіруден қорғау талаптары

6.18.1 Рұқсатсыз қол жеткіруден қорғау келесі мүмкіндіктерді қамтамасыз етуі тиіс:

1. ашық кілт инфрақұрылымының цифрлық сертификаттарында идентификациялау мүмкіндігі;
2. тиісті рұқсаттардың болуын талап ететін ақпараттық есептеу ресурстарына қол жеткізу үшін пайдаланушыларды авторизациялау;
3. деректерді енгізу, түзету, қарау құқықтарын жекелей анықтау;
4. жүйелік ресурстарға қол жеткізу құқықтарын жекелей анықтау;
5. пайдаланушылардың идентификациясына қатысты оқиғаларды аудит жүргізу;
6. рұқсатсыз ақпаратты өшіру, көшіру, өзгерту әрекеттерін болдырмау үшін пайдаланушыларды топтарға бөлу және оларға сәйкес қол жеткізу құқықтарын тағайындау функцияларын ақпараттық жүйеде жүзеге асыру.

6.18.1 Ақпараттың негізгі тасымалдаушыларына (жинағыштар, дискілер, сервер жабдықтары және т.б.) физикалық қол жеткізу ақпараттық ресурстарды өңдеу құралдары мен қауіпсіз жұмыс ортасын ұйымдастыру ережелеріне сәйкес шектеледі.

6.19 Электрондық пошта мен Интернетті қолдануға қойылатын талаптар

6.19.1 Өндірістік процестер мен қауіпсіздік жүйесіне электрондық поштаны пайдалану кезінде туындайтын тәуекелдерді азайту үшін қажеттілік туындаған жағдайда тиісті бақылау құралдарын қолдану қажет, олар:

1. электрондық хабарламалардың рұқсатсыз ұстап алу және өзгертуге осал екенін ескеруі тиіс;
2. электрондық пошта арқылы жіберілетін деректердің, мысалы, хабарламалардың дұрыс емес бағытталуы немесе тағайындалмаған жерге жіберілуі сияқты қателіктерге осал болуы, сондай-ақ қызметтің сенімділігі мен қолжетімділігі;
3. пайдаланушылардың электрондық поштаға қашықтан қол жеткізуін бақылау үшін қорғаныс шараларын қабылдау қажеттілігі.

6.20 Антивирустық қауіпсіздік талаптары

6.20.1 Вирустарды анықтайтын антивирус бағдарламалық құралдары серверлерде, ИС жұмыс станцияларында және ақпараттың тасымалданатын құралдарында вирустардың бар-жоғын тексеру үшін қолданылуы тиіс. Антивирус бағдарламалық құралдары тұрақты түрде жаңартылып,

антивирустық бақылауды ұйымдастыру ережелеріне сәйкес пайдаланылуы қажет.

6.21 Қолжетімділікке қойылатын жалпы талаптар

6.21.1 Қолжетімділікке қойылатын басты талап — пайдаланушылардың ақпаратқа уақтылы және заңды түрде қол жеткізуін қамтамасыз ету.

6.21.2 Апаттар, табиғи апаттар және басқа да төтенше жағдайлар туындаған кезде үздіксіз жұмыс істеу және қалпына келтіру шаралары қарастырылуы тиіс.

6.21.3 Апаттар, табиғи апаттар және басқа да төтенше жағдайлар туралы ақпарат кем дегенде 1 жыл бойы толық және мұқият түрде тіркелуі қажет.

6.22 Сенімділікке қойылатын талаптар

6.22.1 Аппараттық және бағдарламалық қамтамасыз ету университеттің ақпараттық жүйесінің тапсырмаларын орындауды қамтамасыз етіп, бір реттік тоқтау уақыты 48 сағаттан аспауы және жылдық жалпы тоқтау уақыты 120 сағаттан аспауы тиіс.

6.22.2 Ақпараттық жүйенің өндірістік серверінде төтенше жағдай туындаған жағдайда, бағдарламалық өнімді, жүйелік бағдарламалық қамтамасыз етуді және операциялық жүйені қалпына келтіру 48 сағат ішінде жүргізілуі тиіс.

6.22.3 Университет ақпараттық жүйесінің жұмыс қабілеттілігін қалпына келтіру және үздіксіз жұмыс істеуді қамтамасыз ету Қазақстан Республикасы Үкіметінің 2016 жылғы 20 желтоқсандағы №832 «Ақпараттық-коммуникациялық технологиялар және ақпараттық қауіпсіздікті қамтамасыз ету саласындағы бірыңғай талаптарды бекіту туралы» қаулысының 8-тармағына сәйкес жүзеге асырылады.

6.22.4 Деректерді сақтау жүйесі дискілердің тұтастығын автоматты түрде мерзімді бақылауды, нашар секторларды талдауды, резервтік батареялардың жағдайын тексеруді әкімшіге араласусыз және пайдаланушылардың жұмысына әсер етпей қамтамасыз етуі тиіс.

6.22.5 Деректерді сақтау жүйесі дискілерді «ыстық» ауыстыру мүмкіндігін қамтамасыз етуі қажет.

6.22.6 Үздіксіз электрмен жабдықтау қажетті қуаттағы үздіксіз электр көзінен (UPS) қамтамасыз етіліп, сыртқы электр қуатының өшуі кезінде бағдарламалар мен операциялық жүйенің дұрыс жабылуын қамтамасыз етуі тиіс.

6.23 Тәуекелдерді талдау және бағалауға қойылатын талаптар

6.23.1 Ақпараттық қауіпсіздік (АҚ) туралы Ереже бастапқыда АҚ тәуекелдерін талдау және бағалау нәтижелеріне негізделуі тиіс.

6.23.2 Ережені жетілдіру мақсатында жыл сайын АҚ тәуекелдерін талдау және бағалау жүргізіледі. Бұл талдау жыл сайынғы АҚ аудитінің деректеріне негізделіп, университеттің құқықтық мәселелерді ұйымдастыру және реттеу мақсатында жауапты Правление мүшесіне ұсынылады.

6.23.3 Тәуекелдерді талдау және бағалау Қазақстан Республикасы Мемлекеттік стандарты СТ РК ИСО/МЭК 17799-2006 «Ақпараттық технологиялар. Қорғаныс әдістері. Ақпараттық қауіпсіздікті басқару бойынша нұсқаулықтар жинағы» нұсқаулығына сәйкес жүзеге асырылуы тиіс.

6.23.4 Талдау нәтижелері мен шығындар мен пайда арасындағы байланыс негізінде ақпараттық қауіпсіздік үшін жауапты тұлға тәуекелдерді төмендетудің ең тиімді экономикалық шараларын анықтайды. Таңдалған шаралар техникалық, эксплуатациялық және басқарушылық шараларды біріктіріп, университеттің ақпараттық-коммуникациялық инфрақұрылымының қауіпсіздігін қамтамасыз етуі тиіс.

6.24 **Қабылданған қорғаныс шараларының тиімділігін бақылау**

6.24.1 Университетте қажетті ақпараттық қауіпсіздік деңгейін сақтау үшін ақпараттық қауіпсіздік бойынша жауапты тұлға қабылданған қорғаныс шараларының тиімділігін тұрақты түрде бақылайды. Негізгі критерий — қорғауға алынған ресурстардың тәуекелдерінің университет үшін қабылданатын шектерде болуы.

6.24.2 Қабылданған қорғаныс шараларының тиімділігін бақылаудың негізгі механизмдері — университеттің ақпараттық қауіпсіздік мониторингі және аудиті.

6.24.3 Осы Ақпараттық қауіпсіздік Ережесінің талаптарының ақпараттық қауіпсіздік талаптарына сәйкестігін бақылау ақпараттық қауіпсіздік қызметкерлерімен жүзеге асырылады.

6.25 **Ақпараттық қауіпсіздік ережесін қайта қарау**

6.25.1 Ақпараттық қауіпсіздік ережесін дамыту, қайта қарау және бағалау ақпараттық қауіпсіздік бойынша жауапты тұлға арқылы жыл сайынғы ақпараттық қауіпсіздік тәуекелдерін талдау және бағалау негізінде жүзеге асырылады.

6.25.2 Ақпараттық қауіпсіздік ережесін қайта қараудың мақсаттары:

1. Ақпараттық қауіпсіздіктің мақсаттары мен бақылау шараларын жетілдіру;

2. Ақпараттық қауіпсіздік пен университеттің бизнес-процестерін басқару тәсілдерін жетілдіру;

3. Ресурстар мен міндеттерді тиімді бөлу.

6.25.3 Ақпараттық қауіпсіздік ережесі бастапқы тәуекел бағалауының негізіне әсер ететін өзгерістерге сәйкес қайта қаралуы тиіс, мысалы: маңызды ақпараттық қауіпсіздік бұзушылық оқиғаларының пайда болуы, жаңа осалдықтардың анықталуы, ұйымдық/технологиялық инфрақұрылымның өзгеруі немесе университеттің бизнес-процестерінің негізгі сипаттамаларының өзгеруі.

6.25.4 Ақпараттық қауіпсіздікті қамтамасыз ететін технологияларда маңызды өзгерістер болған жағдайда, ақпараттың құпиялылығы, бүтіндігі,

қолжетімділігі және қолданылып жатқан ақпараттық қауіпсіздік шараларының адекваттылығы мен тиімділігін қамтамасыз ету үшін қайта қарау қажет.

6.25.5 Ішкі және сыртқы пайдаланушылар тарапынан ережеге енгізілетін өзгерістерге қатысты қосымша ескертулер мен ұсыныстар пайда болған жағдайда, олар ақпараттық қауіпсіздік бойынша жауапты тұлға тарапынан талданып, қажет болған жағдайда бекітуге ұсынылады.

6.25.6 Университет басшылығы ақпараттық қауіпсіздік ережесін тәуелсіз қайта қарауды бастамақ мүмкін. Мұндай қайта қарау қауіпсіздік саласына тікелей қатысы жоқ тұлға немесе тәуелсіз менеджер, сондай-ақ осы қызметтерге маманданған үшінші тарап ұйымы арқылы жүзеге асырылады. Тәуелсіз қайта қарау нәтижелері есеп түрінде құжатталып, университеттің Правление төрағасына хабарланады.

6.25.7 Ақпараттық қауіпсіздік ережесі университет үшін тәуекелдерді талдау және бағалау жүргізілгеннен кейін қайта қаралуы тиіс, оның нәтижесінде анықталған кемшіліктерді түзету негізінде өзектілендіріледі.

6.25.8 Ақпараттық қауіпсіздік ережесін қайта қарау Қазақстан Республикасының СТ РК ИСО/МЭК 17799-2006 мемлекеттік стандартының «Ақпараттық технология. Қорғаныс әдістері. Ақпараттық қауіпсіздікті басқару бойынша нұсқаулық» бойынша жүргізілуі тиіс.

А Қосымшасы
(міндетті)

Өзгерістерді тіркеу парағы

№	Өзгеріс жөніндегі хабарландыру нөмірі	Өзгерісті тіркеу мерзімі	Бұл құжатқа өзгеріс енгізген тұлға		
			Өзгерістерді енгізген тұлғаның Т.А.Ә.	Қолы	Мерзімі