

	«М.Қозыбаев атындағы СҚУ» КЕАҚ НАО «СҚУ им. М. Козыбаева»	СҚУ ДК 12 СД СҚУ 12	Басылым: бірінші Издание: первое	10 беттің 1 беті Стр. 1 из 10
---	--	------------------------	-------------------------------------	----------------------------------

«М. Қозыбаев атындағы Солтүстік
Қазақстан университеті» КЕАҚ
Директорлар кеңесінің шешімімен
(2021 жылғы 24 мамырдағы № 4
хаттама)
БЕКІТІЛДІ

**«М.Қозыбаев атындағы Солтүстік Қазақстан университеті» КЕАҚ
ақпараттық қауіпсіздігі жөніндегі**

ЕРЕЖЕ

1. ЖАЛПЫ ЕРЕЖЕЛЕР

1. Осы Ереже Қоғамның корпоративтік деректер беру желісінің қазіргі жай-күйі мен оны дамытудың таяу перспективаларын, пайдаланудың мақсаттарын, міндеттері мен құқықтық негіздерін, жұмыс істеу режимдерін, сондай-ақ оның ресурстары үшін қауіпсіздікке төнетін қатерлерді талдауды ескереді және оны бұзғаны үшін қағидаларды, талаптар мен жауапкершілікті белгілейді.
2. Ереже талаптары ақпаратты автоматты түрде өндейтін, оның ішінде таратылуына шектеулер қойылатын ақпарат (қызметтік хат) немесе жеке деректер, сонымен қатар, Университет қызметін сүйемелдеу, қолдау және қамтамасыз етуге бағытталған ақпараттарды өндейтін Университеттің құрылымдық бөлімшелеріне қатысты болып табылады. Ереже университетпен тасымалдаушы және тұтынушы ретінде өзара әрекеттесетін басқа да ұйымдар мен мекемелерге де қатысты болып табылады.
3. Университеттегі ақпаратты қорғау жүйесінің тиімді қалыптасуын ұйымдастыру және қамтамасыз ету жауапкершілігі білім беруді ақпараттандыру департаменті, заң бөлімі, экономикалық жоспарлау және қаржы департаменті, персоналды басқару қызметіне жүктеледі.
4. Білім беруді ақпараттандыру департаментінің директоры, заң бөлімінің басшысы, экономикалық жоспарлау және қаржы департаментінің директоры, персоналды басқару қызметінің басшысы ақпараттық қауіпсіздікті қамтамасыз ету жөніндегі техникалық және ұйымдастырушылық іс-шараларды жүзеге асырады.
5. Ақпараттық қауіпсіздік жөніндегі шешімді іске асыру шеңберінде жұмыс тобы құрылады, оның міндеттері ақпараттық қауіпсіздік саласындағы ахуалды талдау және болжау, ақпараттық қауіпсіздік тәуекелдерін анықтау және басқалар болып табылады.





2. НОРМАТИВТІК СІЛТЕМЕЛЕР

6. Ереже негізінде әзірленді:
- 1) ҚР 2015 жылдың 24 қарашасында жарияланған № 418-V «Ақпараттандыру туралы» Заңы.
 - 2) ҚР Үкіметінің 2004 жылдың 14 қыркүйегінде жарияланған № 965 «ҚР ақпараттық қауіпсіздікті қамтамасыз ету жөніндегі кейбір іс-шаралар туралы» қаулысы негізінде әзірленген.
 - 3) Ақпаратты қорғауды басқару қағидалар жиынтығын қорғалуын қамтамасыз ету әдістері ҚР СТ РК ИСО/МЭК 17799-2006 ҚР Мемлекеттік стандарты.
 - 4) Есептеу техника құралдары. Ақпаратқа санкцияланбаған қолжетімділіктен қорғау. Жалпы техникалық талаптар. СТ РК ГОСТ Р 50739-2006 ҚР Мемлекеттік стандарты.

3. БЕЛГІЛЕР МЕН ҚЫСҚАРТУЛАР

7. Ережеде келесі белгілер мен қысқартулар қолданылды:
- 1) ББАҚ – білім беруді ақпараттандыру департаменті.
 - 2) АЖ – ақпараттық жүйе.
 - 3) ДБКЖ – деректерді берудің корпоративтік желісі.
 - 4) СҚ – санкцияланбаған қолжетімділік.
 - 5) ТСБ – техникалық сүйемелдеу бөлімі.
 - 6) БЕ – бағдарламалық ету.
 - 7) ЕТҚ – есептеу техникасы құралдары.
 - 8) ДБ – деректер базасы.

4. МАҚСАТТАР МЕН МІНДЕТТЕР

8. Ереженің барлық тармақтары қол жеткізуге бағытталған негізгі мақсат ақпараттық қауіпсіздікті сенімді қамтамасыз ету және нәтижесінде ақпараттық қызмет нәтижесінде қоғамға материалдық, физикалық, моральдық немесе басқа да зиян келтіруге жол бермеу болып табылады.
9. Көрсетілген мақсатқа ДБКЖ-ның келесі жай-күйін қамтамасыз ету және тұрақты ұстап тұру арқылы қол жеткізіледі:
- 1) тіркелген пайдаланушылар үшін өңделетін ақпараттың қолжетімділігі;
 - 2) қоғамның ДБКЖ тұрақты жұмыс істеуі;
 - 3) ЕТҚ-да сақталатын, өңделетін және байланыс арналары арқылы берілетін ақпараттың құпиялылығын қамтамасыз ету;



- 4) қоғамның АЖ сақталатын және өңделетін және байланыс арналары арқылы берілетін ақпараттың тұтастығы мен түпнұсқалылығы.
10. Қойылған мақсатқа жету үшін келесі міндеттерді шешу көзделеді:
- 1) Университеттің ақпараттық ресурстарының қалыптасу процесін кездейсоқ тұлғалардың араласуынан қорғау;
 - 2) Тіркелген пайдаланушылардың ақпаратқа деген қолжетімділігін АЖ-да қолданылатын ақпараттық, бағдарламалық және криптографиялық қорғау құралдары арқылы ажырату;
 - 3) Пайдаланушылардың желілік ресурстарды пайдалануын жүйелік журналдарда тіркеу;
 - 4) Ақпараттық қауіпсіздік мамандары тарапынан журналдарды талдау арқылы пайдаланушылардың іс-әрекеттерінің дұрыстығын кезеңдік бақылау;
 - 5) Бағдарламалардың орындалу тұтастығын бақылау және бұзылу жағдайында оларды қалпына келтіру;
 - 6) Ақпаратты санкцияланбаған модификациялау, өзгертуден сақтау;
 - 7) Қолданылатын бағдарламалық құралдардың тұтастығын бақылау, сонымен қатар, олардың зиянды бағдарламалардың енуінен қорғау;
 - 8) қызметтік құпияларды және жеке деректерді өңдеу, сақтау және байланыс каналдары арқылы беру кезінде сыртқа шығудан, рұқсатсыз жария етуден немесе бұрмалаудан қорғау;
 - 9) ақпарат алмасуға қатысатын пайдаланушылардың авторизациялануы мен аутентификациялануын қамтамасыз ету;
 - 10) ақпараттық қауіпсіздікке төнетін қатерлерді, зиян келтіруге әкелетін себептер мен жағдайларды уақтылы анықтау;
 - 11) жеке және заңды тұлғалардың заңсыз әрекеттері салдарынан келтірілген зиянды азайту және оқшаулау, кері әсерін әлсірету және ақпараттық қауіпсіздікті бұзудың салдарын жою үшін жағдайлар мен нұсқаулықтар құру;
 - 12) электрондық құжат айналымын құру және үздіксіз жұмысын қамтамасыз ету;
 - 13) ақпараттық қауіпсіздіктің тұрақты аудиті.

5. АҚПАРАТТЫҚ ЖҮЙЕЛЕРДІ ПАЙДАЛАНУШЫЛАР

11. Ақпараттық жүйелерді пайдаланушыларға:
- 1) ҚР заңнамасына сәйкес негізгі құқықтары мен міндеттеріне ие және Университетте қызмет ететін қызметкерлер мен профессор-оқытушылар құрамы;
 - 2) көмекші персонал - ведомстволық бағыныстағы және бөгде ұйымдардың ақпараттық және қызметтерді тасымалдаушы мен тұтынушылары (пайдаланушылары) ретінде өзара әрекеттесетін ұйымдардың сервистік және техникалық персоналы. Соның ішінде:



- телекоммуникациялық жабдықтарды сүйемелдеуге жауапты деректерді тасымалдау корпоративтік желіліердің әкімшілігі;
 - жалпы және қолданбалы бағдарламалық қамтамасыз етуге жауапты жүйелік әкімшілер;
 - қолданбалы бағдарламалық қамтамасыз етуге жауапты әзірлеушілер;
 - инженер-бағдарламашылар, техника мамандары;
- 3) көрсетілетін қызметтерді тұтынушылар-қоғамның ақпараттық ресурстарын пайдаланатын тұлғалар және/немесе бөгде ұйымдар
- 4) студенттер, интерндер, магистрантар және докторантар.

6. ЫҚТИМАЛ ҚҰҚЫҚ БҰЗУШЫЛАРДЫҢ МОДЕЛЬДЕРІ

12. Ақпараттық қауіпсіздікті ықтимал бұзушы деп қасақана немесе байқамай әрекеттер жасау нәтижесінде ақпараттық ресурстарға бағытталған ақпараттық қауіпсіздікке түрлі қауіп-қатерлерді орындай алатын және моральдық және / немесе себеп болатын адамдар немесе алдын-ала сөз байласқан адамдар немесе адамдар тобы жатады.
13. Потенциалды құқық бұзушыларды ішкі және сыртқы деп бөлуге болады. Университеттің барлық қызметкерлері мен көмекші қызметкерлері ішкі бұзушылар бола алады. Корпоративтік желінің ақпараттық ресурстарына қол жетімділік деңгейіне байланысты оларды келесі топтарға бөлуге болады:
- 1) жеке және қызметтік құпияны құрайтын ақпаратқа қолы жететін адамдар;
 - 2) қызметтік құпияны құрайтын ақпаратқа қол жеткізуге және ақпаратты өңдеу, беру және сақтау технологиясымен айналысатын адамдар;
 - 3) жеке құпия және қызметтік құпияны құрайтын ақпаратқа қол жеткізе алмайтын, бірақ ақпаратты өңдеу, беру және сақтау технологиясымен айналысатын адамдар;
 - 4) қызмет көрсететін персонал.
14. Потенциалды бұзушылардың модельдерін құру үшін мүмкін болатын бұзушылықтардың түрлерін және әртүрлі жеке тұлғалар мен ұйымдардың мүдделерін, сондай-ақ Университеттегі басқа заңды тұлғалардың мүдделерін ескеру қажет.
15. Қоғамда заң бұзушылықтардың келесі түрлері болуы мүмкін:
- 1) Қоғамның ДБКЖ жұмыс қабілеттілігі теріс әсер етуі, оның жұмысын төмендетуі, сондай-ақ ДБКЖ дұрыс жұмысына кедергі келтіруі мүмкін бағдарламаларды рұқсатсыз пайдалану (желілік сканерлер, қарқынды кеңінен ақпарат беретін трафик және т.б.);

	«М.Қозыбаев атындағы СҚУ» КЕАҚ НАО «СҚУ им. М. Қозыбаева»	СҚУ ДК 12 СД СҚУ 12	Басылым: бірінші Издание: первое	10 беттің 5 беті Стр. 5 из 10
---	--	------------------------	-------------------------------------	----------------------------------

- 2) қарапайым әкімшіге бағдарламалардың шектеусіз санын орнатуға мүмкіндік беретін пайдаланушы жұмыс станцияларындағы жергілікті әкімшілердің құқықтарын пайдалану;
 - 3) конфигурациялық файлдарды зиянды өзгерту, жүйелердің, журналдар мен конфигурациялардың файлдарын ауыстыру, көшіру және жою мақсатында әкімшілердің құқықтарын серверлерде, коммуникациялық және өзге де жабдықтарда пайдалану
 - 4) ақпараттық қауіпсіздік талаптарын және Қоғамның нормативтік құқықтық актілерін білмегендіктен қызметкерлердің бұзушылықтары.
16. Потенциалды сыртқы бұзушылар:
- 1) бұрынғы қызметкерлер мен көмекші персонал;
 - 2) келушілер (ұйымдардың шақырылған өкілдері, азаматтар);
 - 3) жабдықты, бағдарламалық жасақтаманы, қызметтерді және т.б. жеткізетін фирмалардың өкілдері.

7. АҚПАРАТТЫ ҚОРҒАУ ҚҰРАЛДАРЫ МЕН ШАРАЛАРЫ

17. Байланыс арналары арқылы ақпараттың сыртқа шығудан қорғау құралдары мен шаралары:
- 1) ақпаратты Қоғамнан/қоғамға беру арналары арқылы сыртқа шығудан қорғау кешенді бағдарламалық жасақтаманы, қорғаудың техникалық құралдарын және ұйымдастырушылық шараларды қолдану арқылы жүзеге асырылады.
 - 2) ақпараттың сырқа шығудан анықтау үшін сыртқа шығу арналарының пайда болу мүмкіндігін жүйелі түрде бақылау және бақыланатын аймақ шегінде олардың қауіптілігін бағалау қажет. Сыртқа шығу арналарын жабу және оқшаулау ұйымдастырушылық-техникалық шаралармен қамтамасыз етіледі.
 - 3) Электрондық ақпаратты беру үшін қолданылатын арналарға сәйкес Университет қажетті техникалық қорғау құралдарымен қамтамасыз етеді (Microsoft Forefront Threat Management Gateway негізіндегі желіаралық экран, Kaspersky Endpoint Security бойынша вирусқа қарсы БҚ, Акронис Инфозащита резервтік көшіру құралдары және Effector Saver).
18. Желі ресурстарына рұқсатсыз қол жеткізуден қорғау жөніндегі шаралар NKZU.Net:
- 1) Қызметкерлер мен профессорлық-оқытушылық құрамды желіде тіркеуді "NKZU.Net компьютерлік желісі туралы" ЕП СҚМУ 08 сәйкес домен әкімшісі жүргізеді.
 - 2) білім алушыларды желіде тіркеу СҚМУ ІНҚ 12 сәйкес жүргізіледі. "Компьютерлік сыныптарда жұмыс істеу ережелері";
 - 3) пайдаланушы дерекқорына Домен әкімшісі қол жеткізе алады. Пайдаланушылардың құпия сөздері ДБ шифрланған түрде сақталады.





- 4) NKZU желісінде тіркелген кезде пайдаланушы корпоративтік поштаға қол жеткізеді;
- 5) корпоративтік почтаны пайдалану ережелерін СҚМУ ІНҚ регламенттейді 97 "М. Қозыбаев атындағы СҚМУ корпоративтік электрондық поштасы туралы ереже."
19. ЕТҚ қорғау шаралары:
- 1) қоғамда ЕТЖ-дан қорғау бірнеше бағыттар бойынша құрылады. Пайдаланушыларды тіркеудің автоматтандырылған құралдары, компьютерлік желі туралы ереже СҚМУ ЕП 08 сәйкес есептік жазбаларды бұғаттау жүйесі құрылады NKZU.net;
- 2) ЕП СҚМҚ 08 сәйкес ЖТЖ-ны, оның ішінде құпиясөздерді жоғалтқан/жария еткен және ЕТЖ істен шыққан жағдайда болдырмау жөніндегі ұйымдастыру шаралары айқындалады, компьютерлік желі туралы ереже NKZU.net;
- 3) Қоғамның ақпараттық ресурстары мен жүйелеріне НСД фактілері анықталған немесе ақпараттық қауіпсіздіктің әлеуетті қатері анықталған жағдайда, ББАҚ қызметкерлері ББАҚ директорын дереу хабардар етеді.
20. Аппараттық арнайы қосымшалардан, ескерілмеген бағдарламаларды заңсыз енгізуден және пайдаланудан қорғау:
- 1) аппараттық арнайы қосымшалардың алдын алу үшін физикалық қорғау шаралары пайдаланылады, бейнебақылау және қоғамның серверлік үй-жайына кіруді бақылау құралдары орнатылады;
- 2) қоғамда ескерілмеген бағдарламаларды заңсыз енгізуден және пайдаланудан қорғау үшін физикалық қорғауды, ЕТҚ-ға жүгіну аудитін жүргізуді және жүйелік журналдардың мониторингін қамтитын іс-шаралардан басқа, пайдаланушылардың жұмыс станцияларына орнатылуы қажет бағдарламалық қамтылымның базалық кешені белгіленеді. Базалық кешенге ЕТҚ жұмысқа қабілеттілігін қамтамасыз ету үшін қажетті лицензиялық бағдарламалық қамтамасыз ету кіреді;
- 3) қолданбалы БҚ-ны, базалық кешеннің құрамына кірмейтін сыртқы ақпарат жеткізгіштерді өндірістік мақсаттар үшін пайдалануға техникалық сүйемелдеу бөлімі ТСБ басшысының келісімі бойынша санкция береді.
21. Зиянды бағдарламалардың, вирустардың әрекеттерінен қорғау:
- 1) Қоғамда зиянды бағдарламалар мен вирустардың іс-әрекеттерінен қорғау мақсатында рұқсатсыз түрлендіру мүмкіндігінен қорғалған вирусқа қарсы бағдарламалық құралдар пайдаланылады;
- 2) вирусқа қарсы БЕ дерекқорын жаңарту вирусқа қарсы БЕ әкімшілендіру серверінің кестесіне сәйкес автоматты түрде жүргізіледі.
22. ЕТҚ-да ақпаратты қорғау:
- 1) әрбір ЕТҚ-ға қоғамның қызметкері бекітіледі. ЕТҚ-да онда жұмыс істейтін қызметкердің авторизациялау және/немесе аутентификациялау

- жүйесі пайдаланылады. ЕТҚ-ны басқа қызметкерге пайдалануға беру бөлімше басшысының рұқсатымен талап ету бойынша жүзеге асырылады;
- 2) ЕТҚ пайдалану ережелері СҚМУ ЕП 08 компьютерлік желі туралы ережемен реттеледі NKZU.net.
23. Қоғамның ресми сайтында ақпаратты қорғау:
- 1) Ақпаратты қоғамның ресми сайтында орналастыруға қолжетімділік Солтүстік Қазақстан мемлекеттік университетінің веб-сайты туралы Ереженің СҚМУ ЕП 09 сәйкес Қоғам қызметкерлеріне беріледі;
 - 2) берілетін ақпаратты қорғау сайт арқылы берілетін деректерді шифрлайтын HTTPS хаттамасын пайдалану арқылы қамтамасыз етіледі;
 - 3) сайт сервері Linux операциялық жүйесіне негізделген.
24. Бағдарламалық-аппараттық құралдардың қателерінен қорғау:
- 1) жұмысқа қабілеттілігін тексеру мақсатында пайдалануға беру алдында бағдарламалық өнімдер мен аппараттық құралдар нақты өнімдерге барынша жақын жағдайларда тестілеуге жатады. Пайдалануға жарамсыз бағдарламалық қамтылым мен аппараттық құралдар пайдалануға қабылданбайды.
25. Қорғау құралдарын біліксіз пайдаланудан, күйге келтіруден немесе заңсыз ажыратудан қорғау:
- 1) ДБКЖ қорғау құралдары пайдалануға енгізіледі, белгіленген регламентке сәйкес қоса беріледі және пайдаланылады. Бұл процесті бақылауды ақпараттық қауіпсіздікті қамтамасыз ететін ТСБ инженерлері жүзеге асырады;
 - 2) қоғамның серверлерін сүйемелдеумен КББ инженері және бағдарламалау және ақпараттық контент бөлімінің (бұдан әрі - БАКБ).
26. Есептеу техника құралдарын жабдықтың, бағдарламалық жасақтаманың, ақпараттық ресурстардың ақауларынан немесе жойылуынан қорғау:
- 1) авариялардың, табиғи апаттардың және басқа да төтенше жағдайлардың нәтижесінде ЕТҚ жұмысының бұзылуы, сондай-ақ университетте аппараттық, бағдарламалық жасақтама, ақпараттық ресурстардың жойылуы мүмкін. Мұндай жағдайларға СҚМУ ЕП 08 сәйкес тиісті қорғау шаралары көзделеді. «Компьютерлік желі туралы ереже NKZU.net».
27. Деректерді корпоративтік желісіне заңсыз қосылудан қорғау:
- 1) Электрондық және физикалық қол жетімділік құралдарын қоспағанда, коммуникацияларды заңсыз қосылудан қорғау бағдарламалық, аппараттық және ұйымдастырушылық шаралармен жүзеге асырылады. Адамдардың байланысқа қол жеткізу жөніндегі заңсыз әрекеттерін уақтылы анықтау, алдын алу және жолын кесу бойынша қажетті шаралар қолданылады.



	«М.Қозыбаев атындағы СҚУ» КЕАҚ НАО «СҚУ им. М. Козыбаева»	СҚУ ДК 12 СД СҚУ 12	Басылым: бірінші Издание: первое	10 беттің 8 беті Стр. 8 из 10
--	--	------------------------	-------------------------------------	----------------------------------

28. Желілік жабдықтың бұзылуынан, дұрыс жұмыс жасамауынан, ішінара немесе толық істен шығуынан қорғау:
- 1) Университеттің желілік жабдықтарының бұзылуы, дұрыс жұмыс істемеуі, ішінара, толық істен шығуы, ең алдымен, апаттар, табиғи апаттар және басқа да төтенше жағдайлар салдарынан болуы мүмкін.
 - 2) Университет табиғи апаттар (өрт, су тасқыны және жер сілкінісі) кезінде, сондай-ақ әр түрлі төтенше жағдайларда қолданылатын қорғаныс құралдарын енгізуге байланысты шаралар қолданылады.
29. Жабдықты рұқсатсыз қосудан, өшіруден қорғау:
- 1) Қоғамның ДБКЖ желілік жабдығы пайдалануға енгізіледі, белгіленген регламентке сәйкес сүйемелденеді және пайдаланылады. Жабдықты қосуды және ажыратуды уәкілетті техникалық персонал ТСБ басшысының келісімі бойынша жүргізеді.
30. Мұрағаттау жүйесін қорғау шаралары:
- 1) бағдарламалық өнімдер мен ақпараттық жүйелердің сақтық көшірмесін жасау, сақтау және қалпына келтіру тәртібі анықталады. Резервтік қойма ақпараттық жүйелердің үздіксіз жұмысын қамтамасыз ету үшін Жоспарға сәйкес арнайы жабдықталған бөлмеде орналасқан;
 - 2) Қоғам бөлімшелерінің серверлері мен желілік дискілерін резервтік көшіру автоматты режимде Акронис Инфозащита бағдарламалық қамтамасыз етуімен арнайы бөлінген серверге айына кемінде бір рет жүзеге асырылады.

8. АҚПАРАТТЫҚ ҚАУІПСІЗДІК АУДИТІ

31. ББАД директоры ақпараттық қауіпсіздік аудитін жүргізуге бастамашылық жасайды.
32. Ақпараттық қауіпсіздік аудиті жүргізіледі:
 - 1) жарты жылда бір рет ішкі аудитор.
 - 2) жылына бір рет ақпараттық-коммуникациялық технологиялар саласында арнайы білімі мен жұмыс тәжірибесі бар тәуелсіз сарапшылар (сыртқы ұйымдар) жүргізеді.
33. Ақпараттық қауіпсіздік аудитінің нәтижелері осы Ережені қайта қарау және оған қажетті түзетулер енгізу үшін негіз болады.

9. ЕРЕЖЕНІ ҚАЙТА ҚАРАУ

34. Осы Ережені қайта қарау мынадай жағдайларда жүргізіледі:
 - 1) қоғамның АЖ-не елеулі өзгерістер енгізу,
 - 2) заңнамадағы, қоғамның ұйымдық құрылымындағы өзгерістер,
 - 3) пайда болған ақпараттық қауіпсіздік инциденттерін.
35. Өзгерістер енгізу кезінде мыналар ескеріледі: