«М. Қозыбаев атындағы Солтүстік Қазақстан университеті» КЕАҚ Директорлар кеңесінің шешімімен (2021 жылғы 24 маусырдағы № 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 ақпарттық 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.

Корпоративтік хатшының қолы
Подпись корпоративного секретаря:

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 Мемлекттік 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;

Корпоративтік хатшының қолы
Подпись корпоративного секретаря:

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. Ақпарттық 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:

Корпоративтік хатшының қолы
Подпись корпоративного секретаря:

- телекоммуникациялық жабдықтарды сүйемелдеуге жауапты деректерді тасымалдау корпоративтік желіліердің әкімшілігі;
- жалпы және қолданбалы бағдарламалық қамтамасыз етуге жауапты жүйелік әкімшілер;
- қолданбалы бағдарламалық қамтамасыз етуге жауапты әзірлеушілір;
- 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.);

Корпоративтік хатшының қолы
Подпись корпоративного секретаря:

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 компьтерлік 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.

Корпоративтік хатшының қолы
Подпись корпоративного секретаря:

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

Корпоративтік хатшының қолы
Подпись корпоративного секретаря:

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.

Корпоративтік хатшының қолы
Подпись корпоративного секретаря:

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:

Корпоративтік хатшының қолы
Подпись корпоративного секретаря:

1) ақпараттық қауіпсіздік аудитінің нәтижелері, сондай-ақ алдыңғы аудиттердің нәтижелері;
2) ақпараттық қауіпсіздік жөніндегі тәуелсіз сарапшылардың ұсынымдары;
3) ақпараттық жүйелердің Елеулі қатерлері мен осалдықтары болып табылады;
4) Ақпараттық қауіпсіздік саласындағы инциденттер туралы есептер.

36. Ақпараттық қауіпсіздік туралы ережені қайта қарау ҚР СТ ИСО / МЭК 17799-2006/2009 Қазақстан Республикасының Мемлекеттік стандартын енгізу жөніндегі нұсқаулыққа сәйкес жүргізілуі керек..
37. Осы Ереже Қоғамның АЖ үшін ақпараттық қауіпсіздік тәуекелдерін талдау және бағалау нәтижелері бойынша міндетті түрде қайта қаралуға жатады.

10. ЖАУАПКЕРШІЛІК

38. ЕТҚ-ның барлық пайдаланушылары этика ережелерін сақтай отырып, компьютерлік ресурстарды білікті, тиімді пайдалануға міндетті.
39. СВТ, ДБКЖ және АЖ пайдалану ережелері СҚМУ КП 08 компьютерлік желі туралы Ережемен реттелген NKZU.net. ЕТЖ, ДБКЖ және АЖ пайдалану ережелерін бұзғаны үшін пайдаланушы тәртіптік жауапкершілікке тартылады.
40. Қоғамның қызметкерлері осы Ереженің тармақтарын бұзғаны үшін Қазақстан Республикасының қолданыстағы заңнамасына сәйкес әкімшілік немесе өзге де жауапкершілікке тартылады.
41. АЖ ресурстардың әкімшілері желінің үздіксіз жұмысын қамтамасыз етеді және ақпараттық қауіпсіздікті қамтамасыз ету үшін қажетті техникалық шаралардың орындалуына жауап береді.

11. ҚОРЫТЫНДЫ ЕРЕЖЕЛЕР

42. Ережені бекіту, сонымен қатар, оған өзгертулер мен толықтырулар енгізу Қоғамның Директорлар Кеңесі құзыреттілігіне жатады.
43. Егер осы Ереженің жекелеген тармақтары қолданыстағы заңнамаға қайшы келсе, онда бұл тармақтар күшін жояды және осы тармақтармен реттелетін мәселелер тұрғысынан осы Ережеге тиісті түзетулер енгізілгенге дейін қолданыстағы заңнаманың нормаларын басшылыққа алу қажет.

29.03.2021 ж. № 12 хаттама
Басқарма отырысында қаралды

Корпоративтік хатшының қолы
Подпись корпоративного секретаря:

ҚҰРАСТЫРАЛҒАН:

ББАД директоры Д. Мораш

КЕЛІСІЛДІ:

Басқарма Төрағасы-Ректор орынбасарының м.а. Е. Исакаев

Бас комплаенс академ офицер И. Джемалединова

Цифрландыру жөніндегі Бас менеджер И. Курмашев

Техникалық сүйемелдеу бөлімінің инженері А. Брындин

СҚО бойынша ҰҚКД қызметкері Р. Гиматдинов

«Гуманитарлық-техникалық колледжі» МеББМ директорының Ақпараттық технологиялар жөніндегі орынбасары А. Бодряков

«Аймақаралық жаңа технологиялар орталығы» ЖШС директоры А. Чернышов

Корпоративтік хатшының қолы
Подпись корпоративного секретаря:

УТВЕРЖДЕНО
Решением Совета директоров НАО «Северо-Казахстанский университет им. М. Козыбаева» (Протокол № 4 от 24 мая 2021 года)

ПОЛОЖЕНИЕ

об информационной безопасности НАО «Северо-Казахстанский университет им. М. Козыбаева»

1. ОБЩИЕ ПОЛОЖЕНИЯ

1. Настоящее Положение учитывает современное состояние и ближайшие перспективы развития корпоративной сети передачи данных Общества, цели, задачи и правовые основы эксплуатации, режимы функционирования, а также анализ угроз безопасности для ее ресурсов и устанавливает правила, требования и ответственность за ее нарушение.
2. Требования Положения распространяются на структурные подразделения Общества в которых осуществляется автоматизированная обработка информации, в том числе информации с ограниченным распространением (служебная информация) или персональных данных, а также осуществляющих сопровождение, обслуживание и обеспечение функционирования Общества. Положение распространяется также на другие организации и учреждения, осуществляющие взаимодействие с Обществом в качестве поставщиков и потребителей (пользователей) информации и услуг.
3. За непосредственную организацию (построение) и обеспечение эффективного функционирования системы защиты информации в Обществе отвечают: Департамент информатизации образования, юридический отдел, Департамент экономического планирования и финансов, служба управления персоналом.
4. Директор Департамента информатизации образования, руководитель юридического отдела, директор Департамента экономического планирования и финансов, руководитель службы управления персоналом проводят необходимые технические и организационные мероприятия, осуществляет организацию квалифицированной разработки (совершенствования) системы защиты информации и организационного (административного) обеспечения ее функционирования в Обществе.
5. В рамках реализации решения по информационной безопасности приказом Заместителя Председателя Правления – Ректора создается

Корпоративтік хатшының қолы
Подпись корпоративного секретаря:

рабочая группа задачами которой являются анализ и прогнозирование ситуации в области информационной безопасности, выявление рисков информационной безопасности.

2. НОРМАТИВНЫЕ ССЫЛКИ

6. Положение разработано на основании:
1) Закона Республики Казахстан от 24 ноября 2015 года № 418-V «Об информатизации»;
2) Постановления Правительства Республики Казахстан от 14 сентября 2004 года № 965 «О некоторых мерах по обеспечению информационной безопасности в Республике Казахстан»;
3) Государственный стандарт Республики Казахстан СТ РК ИСО/МЭК 17799-2006 Методы обеспечения защиты свод правил по управлению защиты информаций;
4) Государственный стандарт Республики Казахстан СТ РК ГОСТ Р 50739-2006. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования.

3. ОБОЗНАЧЕНИЯ И СОКРАЩЕНИЯ

7. В Положении использованы следующие обозначения и сокращения:
1) ДИО – Департамент информатизации образования.
2) ИС – информационная система.
3) КСПД – корпоративная сеть передачи данных.
4) НСД – несанкционированный доступ.
5) ОТС – отдел технического сопровождения.
6) ПО – программное обеспечение.
7) СВТ – средства вычислительной техники.
8) БД – база данных.

4. ЦЕЛИ И ЗАДАЧИ

8. Основной целью, на достижение которой направлены все пункты Положения, является надежное обеспечение информационной безопасности и, как следствие, недопущение нанесения материального, физического, морального или иного ущерба Обществу в результате информационной деятельности.
9. Указанная цель достигается посредством обеспечения и постоянного поддержания следующего состояния КСПД:
1) доступность обрабатываемой информации для зарегистрированных пользователей;

Корпоративтік хатшының қолы
Подпись корпоративного секретаря:

2) устойчивое функционирование КСПД Общества;
3) обеспечение конфиденциальности информации, хранимой, обрабатываемой СВТ и передаваемой по каналам связи;
4) целостность и аутентичность информации, хранимой и обрабатываемой ИС Общества и передаваемой по каналам связи.

10. Для достижения поставленной цели необходимо решать следующие задачи:
1) защита от вмешательства посторонних лиц в процесс функционирования информационных ресурсов Общества;
2) разграничение доступа зарегистрированных пользователей к информации, аппаратными, программными и криптографическими средствами защиты, используемыми в ИС;
3) регистрация в системных журналах действий пользователей при использовании сетевых ресурсов;
4) периодический контроль корректности действий пользователей системы путем анализа содержимого этих журналов специалистами информационной безопасности;
5) контроль целостности (обеспечение неизменности) среды исполнения программ и ее восстановление в случае нарушения;
6) защита информации от несанкционированной модификации, искажения;
7) контроль целостности используемых программных средств, а также защиту системы от внедрения вредоносного программного обеспечения;
8) защиту служебной тайны и персональных данных от утечки, несанкционированного разглашения или искажения при ее обработке, хранении и передаче по каналам связи;
9) обеспечение авторизации и аутентификации пользователей, участвующих в информационном обмене;
10) своевременное выявление угроз информационной безопасности, причин и условий, способствующих нанесению ущерба;
11) создание условий и инструкций для минимизации и локализации нанесенного ущерба неправомерными действиями физических и юридических лиц, ослабление негативного влияния и ликвидация последствий нарушения информационной безопасности;
12) создание и обеспечение бесперебойной работы электронного документооборота;
13) постоянный аудит информационной безопасности.

5. ПОЛЬЗОВАТЕЛИ ИНФОРМАЦИОННЫХ СИСТЕМ

11. К пользователям информационных систем относятся:
1) сотрудники, профессорско-преподавательский состав, осуществляющие свою деятельность в Обществе и обладающие

Корпоративтік хатшының қолы
Подпись корпоративного секретаря:

основными правами и обязанностями в соответствии с законодательством Республики Казахстан;

2) вспомогательный персонал - обслуживающий и технический персонал сторонних организаций, осуществляющих взаимодействие с Обществом в качестве поставщиков и потребителей (пользователей) информации и услуг. В том числе:

- администраторы корпоративной сети передачи данных, ответственные за сопровождение телекоммуникационного оборудования;
- системные администраторы, ответственные за сопровождение общего и прикладного программного обеспечения;
- разработчики прикладного программного обеспечения;
- инженеры-программисты, технические специалисты;

3) потребители услуг – лица и/или сторонние организации, использующие информационные ресурсы Общества;

4) студенты, интерны, магистранты и докторанты.

6. МОДЕЛИ ПОТЕНЦИАЛЬНЫХ НАРУШИТЕЛЕЙ

12. В качестве потенциального нарушителя информационной безопасности рассматривается лицо или группа лиц, состоящих или не состоящих в сговоре, которые в результате умышленных или неумышленных действий могут реализовать разнообразные угрозы информационной безопасности, направленные на информационные ресурсы и нанести моральный и/или материальный ущерб интересам Общества.
13. Потенциальных нарушителей делятся на внутренних и внешних. К внутренним нарушителям относятся все сотрудники Общества и вспомогательный персонал. Их делят на следующие группы в зависимости от уровня доступа к информационным ресурсам корпоративной сети:

1) лица, имеющие доступ к информации, составляющую персонифицированную и служебную тайну;

2) лица, имеющие доступ к информации, составляющую служебную тайну и задействованные в технологии обработки, передачи и хранения информации;

3) лица, не имеющие доступ к информации, составляющую персонифицированные секрет и служебную тайну, но задействованные в технологии обработки, передачи и хранения информации;

4) обслуживающий персонал.

14. Для построения моделей потенциальных нарушителей необходимо принять во внимание виды наиболее возможных нарушений и интересы различных лиц и организаций, а также имеющиеся в Обществе интересы других юридических лиц.

15. В Обществе возможны следующие виды нарушений:
1) несанкционированное использование программ, способных негативно повлиять на работоспособность КСПД Общества, снизить ее производительность, а также мешающих корректной работе КСПД (сканеры сети, интенсивный широковещательный трафик и т.п.);
2) использование прав локальных администраторов на рабочих станциях пользователей, что дает возможность установки обычному пользователю неограниченного количества программ;
3) использование прав администраторов на серверах, коммуникационном и прочем оборудовании с целью вредоносного изменения конфигурационных файлов, подмены, копирования и удаления файлов систем, журналов и конфигураций;
4) нарушения сотрудниками вследствие незнания требований информационной безопасности и нормативных правовых актов Общества.
16. Потенциальные внешние нарушители:
1) бывшие сотрудники и вспомогательный персонал;
2) посетители (приглашенные представители организаций, граждане);
3) представители фирм, поставляющих технику, программное обеспечение, услуги и т.п.

7. СРЕДСТВА И МЕРЫ ЗАЩИТЫ ИНФОРМАЦИИ

17. Средства и меры защиты от утечки информации по каналам связи:
1) Защита информации от утечки по каналам их передачи из/в Общества достигается путем применения комплексных программных, технических средств защиты и организационных мер.
2) Для выявления утечки информации необходим систематический контроль возможности образования каналов утечки и оценки их опасности в пределах контролируемой зоны. Закрытие и локализация каналов утечки обеспечивается организационно-техническими мерами.
3) В соответствии с используемыми каналами передачи электронной информации в Обществе предусматриваются необходимые технические средства защиты (межсетевой экран на основе Microsoft Forefront Threat Management Gateway, антивирусное ПО Kaspersky Endpoint Security, средства резервного копирования Акронис Инфозащита и Effector Saver).
18. Меры по защите от несанкционированного доступа к ресурсам сети NKZU.Net:
1) регистрация сотрудников и профессорско-преподавательского состава в сети производится администратором домена согласно ПП СКГУ 08 Положение о компьютерной сети NKZU.net.

Корпоративтік хатшының қолы
Подпись корпоративного секретаря:

2) регистрация обучающихся в сети производится согласно ВНД СКГУ 12 Правила работы в компьютерных классах.

3) доступ к базе данных пользователей имеет администратор домена. Пароли пользователей хранятся в БД в зашифрованном виде.

4) при регистрации в сети NKZU пользователь получает доступ к корпоративной почте.

5) правила пользования корпоративной почтой регламентируются ВНД СКГУ 97 Положение о корпоративной электронной почте СКГУ им. М.Козыбаева.

19. Меры по защите СВТ:

1) Защита СВТ от НСД в Обществе строится по нескольким направлениям. Создаются автоматизированные средства регистрации пользователей, система блокирования учетных записей в соответствии с ПП СКГУ 08 Положение о компьютерной сети NKZU.net.

2) Определяются организационные меры по предотвращению НСД, в том числе в случае утраты/компрометации паролей и выхода из строя СВТ согласно ПП СКГУ 08 Положение о компьютерной сети NKZU.net.

3) В случае обнаружения фактов НСД к информационным ресурсам и системам Общества или выявления потенциальной угрозы информационной безопасности сотрудники ДИО немедленно информируют директора ДИО.

20. Защита от аппаратных спецвложений, нелегального внедрения и использования неучтенных программ:

1) Для предотвращения аппаратных спецвложений используются меры физической защиты, устанавливаются средства видеонаблюдения и контроля доступа в серверное помещение Общества.

2) Для защиты от нелегального внедрения и использования неучтенных программ в Обществе кроме мероприятий, включающих физическую защиту, проведение аудита обращения к СВТ и мониторинг системных журналов, устанавливается базовый комплекс программного обеспечения, который необходимо устанавливать на рабочие станции пользователей. В базовый комплекс включается лицензионное программное обеспечение, необходимое для обеспечения работоспособности СВТ.

3) Использование для производственных целей прикладного ПО, внешних носителей информации, не входящего в состав базового комплекса, санкционируется отделом технического сопровождения по согласованию с руководителем ОТС.

21. Защита от действий вредоносных программ, вирусов:

1) В целях защиты от действий вредоносных программ и вирусов в Обществе используются антивирусные программные средства, защищенные от возможности несанкционированной модификации.

Корпоративтік хатшының қолы
Подпись корпоративного секретаря:

2) Обновление баз антивирусного ПО происходит автоматически согласно расписанию сервера администрирования антивирусного ПО.

22. Защита информации в СВТ:

1) За каждым СВТ закрепляется сотрудник Общества. На СВТ используется система авторизации и/или аутентификации сотрудника, работающего на нем. Передача СВТ в пользование другому сотруднику, осуществляется по требованию с разрешения руководителя подразделения.

2) Правила пользования СВТ регламентированы в ПП СКГУ 08 Положение о компьютерной сети NKZU.net.

23. Защита информации на официальном сайте Общества:

1) Доступ к размещению информации на официальном сайте общества предоставляется сотрудникам Общества в соответствии с ПП СКГУ 09 Положение о веб-сайте Северо-Казахстанского государственного университета.

2) Защита передаваемой информации обеспечивается использованием протокола HTTPS, который шифрует передаваемые сайтом данные.

3) Сервер сайта базируется на операционной системе семейства Linux.

24. Защита от ошибок программно-аппаратных средств:

1) С целью проверки работоспособности, перед вводом в эксплуатацию программные продукты и аппаратные средства подлежат тестированию в условиях максимально приближенных к реальным. Не пригодные к использованию программное обеспечение и аппаратные средства в эксплуатацию не принимаются.

25. Защита от некомпетентного использования, настройки или неправомерного отключения средств защиты:

1) Средства защиты КСПД вводятся в эксплуатацию, сопровождаются и используются в соответствии с установленным регламентом. Контроль за этим процессом осуществляют инженера ОТС, обеспечивающий информационную безопасность.

2) Сопровождением серверов Общества занимается инженера ОТС и инженера отдела программирования и информационного контента (далее - ОПИК).

26. Защита СВТ от нарушений работоспособности или разрушения аппаратных, программных, информационных ресурсов:

1) В результате возникновения аварий, стихийных бедствий и иных внештатных ситуаций могут возникнуть нарушения работоспособности СВТ, а также разрушение аппаратных, программных, информационных ресурсов в Обществе. На такие случаи предусматриваются соответствующие меры защиты в соответствии с ПП СКГУ 08 Положение о компьютерной сети NKZU.net.

27. Защита от незаконного подключения к корпоративной сети передачи данных:

Корпоративтік хатшының қолы
Подпись корпоративного секретаря:

1) Защита коммуникаций от незаконного подключения кроме средств санкционированного электронного и физического доступа, осуществляется программными, техническими средствами и организационными мерами. Проводятся необходимые мероприятия для своевременного выявления, предупреждения и пресечения неправомерных действий лиц по получению доступа к коммуникациям.

28. Защита от повреждения, некорректного функционирования, частичного или полного отказа сетевого оборудования:

1) Повреждение, некорректное функционирование, частичный, полный отказ сетевого оборудования Общества может быть, в первую очередь, в результате возникновения аварий, стихийных бедствий и иных внештатных ситуаций.

2) В Обществе принимаются меры, связанные с внедрением средств защиты, которые будут использоваться в случае стихийных бедствий (пожаров, наводнений и землетрясений), а также в различных нештатных ситуациях.

29. Защита от неправомерного включения, выключения оборудования:

1) Сетевое оборудование КСПД Общества вводится в эксплуатацию, сопровождается и используется в соответствии с установленным регламентом. Включение и отключение оборудования производится уполномоченным техническим персоналом, по согласованию с руководителем ОТС.

30. Меры по защите системы архивирования:

1) Определяется порядок резервного копирования, хранения и восстановления программных продуктов и информационных систем. Хранилище резервных копий размещается в специально оборудованном помещении. Обеспечивается санкционированный доступ к хранилищу резервных копий для своевременного восстановления информации и информационных систем в случае сбоя, аварии и иных нештатных ситуациях.

2) Резервное копирование серверов и сетевых дисков подразделений Общества осуществляется в автоматическом режиме программным обеспечением Акронис Инфозащита на специально выделенный сервер не реже одного раза в месяц.

8. АУДИТ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

31. Директором ДИО инициируется проведение аудита информационной безопасности.

32. Аудит информационной безопасности проводится:

1) внутренним аудитором раз в полгода.

Корпоративтік хатшының қолы
Подпись корпоративного секретаря:

2) независимыми экспертами (внешними организациями), обладающими специальными знаниями и опытом работы в сфере информационно-коммуникационных технологий один раз в год.

33. Результаты аудита информационной безопасности служат основанием для пересмотра настоящего Положения и внесения в него необходимых корректировок.

9. ПЕРЕСМОТР ПОЛОЖЕНИЯ

34. Пересмотр настоящего Положения проводится в случае:
1) внесения существенных изменений в ИС Общества,
2) изменений в законодательстве, организационной структуре Общества,
3) возникновения инцидентов информационной безопасности.

35. При внесении изменений учитываются:
1) результаты аудита информационной безопасности, а также результаты предыдущих аудитов;
2) рекомендации независимых экспертов по информационной безопасности;
3) существенные угрозы и уязвимости информационных систем;
4) отчеты об инцидентах в области информационной безопасности

36. Пересмотр Положения об информационной безопасности должен осуществляться в соответствии с руководством по реализации Государственного стандарта Республики Казахстан СТ РК ИСО/МЭК 17799-2006/2009.

37. Настоящее Положение подлежит обязательному пересмотру по результатам проведения анализа и оценки рисков информационной безопасности Общества.

10. ОТВЕТСТВЕННОСТЬ

38. Все пользователи СВТ обязаны использовать компьютерные ресурсы квалифицированно, эффективно, придерживаясь правил этики.

39. Правила пользования СВТ, КСПД и ИС регламентированы ПП СКГУ 08 Положение о компьютерной сети NKZU.net. За нарушение правил пользования СВТ, КСПД и ИС пользователь привлекается к дисциплинарной ответственности согласно ВНД СКГУ 87 Правила наложения дисциплинарных взысканий на работников на СКГУ им. М. Козыбаева.

40. Сотрудники Общества за нарушение требований пунктов настоящего Положения будут привлекаться к административной или иной ответственности, в соответствии с действующим законодательством Республики Казахстан.

Корпоративтік хатшының қолы
Подпись корпоративного секретаря:

41. Администраторы ресурсов ИС обеспечивают непрерывное функционирование сети и отвечают за реализацию технических мер, необходимых для обеспечения информационной безопасности.

11. ЗАКЛЮЧИТЕЛЬНЫЕ ПОЛОЖЕНИЯ

42. Утверждение Положения, а также внесение изменений и дополнений в него относится к компетенции Совета директоров Общества.
43. Если отдельные пункты настоящего Положения вступают в противоречие с действующим Законодательством, эти пункты утрачивают силу и в части регулируемых этими пунктами вопросов следует руководствоваться нормами действующего Законодательства до момента внесения соответствующих изменений в настоящее Положение.

Рассмотрено на заседании Правления
Протокол № 12 от 29.03.2021 г.

РАЗРАБОТАНО:

Директор ДИО Д. Мораш

СОГЛАСОВАНО:

И.о. заместителя Председателя Правления-Ректора Е. Исакаев

Главный комплаенс академ офицер И. Джемалединова

Главный менеджер по цифровизации И. Курмашев

Инженер отдела технического сопровождения А. Брындин

Сотрудник ДКНБ по СКО Р. Гиматдинов

Заместитель директора по информационным технологиям НУО «Гуманитарно-технический колледж» А. Бодряков

Директор ТОО «Межрегиональный Центр новых технологий» А. Чернышов

Корпоративтік хатшының қолы
Подпись корпоративного секретаря: