Бекітемін
«Әбілқас Сағынов атындағы Қарағанды техникалық университеті» КеАҚ
Басқарма Төрағасы – Ректоры
_____ Сагинтаева С.С.
Басқарманың «14» қаңтар 2026 ж.
№ 29 шешімі

ІШКІ НОРМАТИВТІК ҚҰЖАТ

АҚПАРАТТЫ КРИПТОГРАФИЯЛЫҚ ҚОРҒАУ ҚҰРАЛДАРЫН ПАЙДАЛАНУ ЕРЕЖЕСІ

ІНҚ II-04-2026

Әзірлеген: Ақпараттық қауіпсіздік жөніндегі инженер
Д.К. Читян _____

Қарағанды

Құжатты рұқсатсыз көшіруге тыйым салынады

Мазмұны

1 Қолдану саласы 3
2 Нормативтік сілтемелер 3
3 Терминдер, анықтамалар және қысқартулар 3
4 Жауапкершілік және өкілеттіктер 4
5 Жалпы қағидалар 4
6 АКҚҚ-мен жұмыс 5
7 Кілттер бұзылған жағдайда әрекет ету 6
8 Негізгі ақпаратты жою 6
9 Келісу, бекіту және қолданысқа енгізу 7
10 Сақтау 7
11 Қайта қарау және өзектендіру тәртібі 8

Құжатты рұқсатсыз көшіруге тыйым салынады

1 Қолдану саласы

1.1 Осы ақпаратты криптографиялық қорғау құралдарын пайдалану Ережесі (бұдан әрі — Ереже) «Әбілқас Сағынов атындағы Қарағанды техникалық университеті» КеАҚ-та (бұдан әрі - Университет) ақпаратты криптографиялық қорғау құралдарын қолдануға қойылатын талаптарды белгілейді.

1.2 Ақпаратты криптографиялық қорғау құралдары электрондық құжаттар мен деректерді ашық байланыс арналары арқылы беру кезінде олардың құпиялылығын қамтамасыз ету үшін, сондай-ақ дербес деректерді және өзге де құпия ақпаратты рұқсатсыз кіруден және ағып кетуден қорғау үшін қолданылады.

1.3 Осы Ереженің талаптары ақпаратты криптографиялық қорғау құралдары пайдаланылатын университеттің барлық ақпараттық жүйелеріне, сондай-ақ оларды пайдалануға жіберілген қызметкерлер мен өзге де тұлғаларға қолданылады.

1.4 Осы Ереже Университеттің ішкі нормативтік құжаты болып табылады және ақпаратты криптографиялық қорғау құралдарының барлық пайдаланушылары үшін міндетті болып табылады.

2 Нормативтік сілтемелер

2.1 Ережені әзірлеу кезінде пайдаланылған нормативтік құжаттар:

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

2) ҚР СТ ИСО/МЭК 27002-2023 «Ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Ақпараттық қауіпсіздікті басқару шаралары».

3) ҚР СТ ИСО/МЭК 27001-2023 «Ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Ақпараттық қауіпсіздікті басқару жүйелері. Талаптар».

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

2.2 Ереже Университеттің ішкі нормативтік құжаты болып табылады және Университеттің ақпараттық қауіпсіздік саясатына сәйкес келеді.

3 Терминдер, анықтамалар және қысқартулар

3.1 Осы Ережеде мынадай терминдер, анықтамалар мен қысқартулар пайдаланылады:

1) Университет — «Әбілқас Сағынов атындағы Қарағанды техникалық университеті» КеАҚ.

2) АККҚ — ақпаратты криптографиялық қорғау құралдары.

3) Негізгі ақпарат – криптографиялық түрлендірулерді орындау үшін пайдаланылатын деректер.

4) кілтті бұзу – жеке кілт рұқсат етілмеген адамдарға немесе процестерге қол жетімді болған немесе болуы мүмкін оқиға.

5) АККҚ пайдаланушысы – ақпаратты криптографиялық қорғау құралдарын пайдалануға жіберілген университет қызметкері.

6) АҚҚ — Университеттің ақпараттық қауіпсіздік қызметі.

7) АТД — Университеттің ақпараттық технологиялар департаменті.

4 Жауапкершілік және өкілеттіктер

4.1 Ақпараттық қауіпсіздік қызметі ақпаратты криптографиялық қорғау құралдарын қолдануды әдістемелік сүйемелдеуді жүзеге асырады, негізгі ақпаратты бұзуға байланысты инциденттерді тергеуге қатысады және криптографиялық қорғау шараларын жетілдіру жөнінде ұсыныстар енгізеді.

4.2 Ақпараттық технологиялар департаменті ақпаратты криптографиялық қорғау құралдарын техникалық пайдалануды, негізгі ақпаратты басқаруды, бұзу анықталған кезде кілттерді бұғаттауды және ауыстыруды қамтамасыз етеді.

4.3 Ақпаратты криптографиялық қорғау құралдарын пайдаланушылар осы Ереженің талаптарын сақтауға, негізгі ақпараттың, кілт тасығыштардың сақталуына және ақпаратты криптографиялық қорғау құралдарына рұқсатсыз қол жеткізудің алдын алуға дербес жауапты болады.

5 Жалпы қағидалар

5.1 Ақпаратты криптографиялық қорғау құралдарын пайдалануға Басқарма Төрағасының – Университет ректорының немесе уәкілетті тұлғаның бұйрығымен тағайындалған уәкілетті тұлғалар ғана жіберіледі.

5.2 Негізгі ақпарат бөгде адамдардың кіруіне, оның жоғалуына, көшірілуіне немесе рұқсатсыз пайдаланылуына жол бермейтін жағдайларда сақталуға тиіс. Негізгі ақпараттың сақталуын қамтамасыз ету мақсатында оларды бөлек сақтауды қамтамасыз ете отырып, резервтік көшірмелер жасалады.

5.3 Ақпаратты криптографиялық қорғау құралдары пайдаланылатын жұмыс орындарында олардың жұмыс істеуін бұзуға қабілетті бағдарламалық қамтамасыз етуді пайдалануға тыйым салынады. Мұндай бағдарламалар анықталған кезде ақпаратты криптографиялық қорғау құралдарымен жұмыс бұзушылықтар жойылғанға дейін дереу тоқтатылуға тиіс.

5.4 Негізгі ақпаратқа нұқсан келтіру фактілері Ақпараттық технологиялар департаменті мен Ақпараттық қауіпсіздік қызметін дереу хабардар етуге тиіс. Бұзылған кілттерді бұғаттау белгіленген тәртіппен жүзеге асырылады, ал жұмысты қайта бастауға олар ауыстырылғаннан кейін ғана жол беріледі.

5.5 Негізгі ақпаратты жою фактісін міндетті құжаттаумен белгіленген талаптарға сәйкес жүзеге асырылады.

6 АКҚҚ-мен жұмыс

6.1 Ақпаратты криптографиялық қорғау құралдарымен (АКҚҚ) жұмыс істеуге Университеттің Бірінші басшысының тиісті бұйрығымен тағайындалған уәкілетті тұлғалар тартылады.

6.2 Тиісті бұйрықпен АКҚҚ-ны пайдалануға, шифрлау кілттерін алуға және пайдалануға уәкілеттік берілген адамдар:

1) АКҚҚ-мен жұмыс істеу процесінде оларға белгілі болған құпия ақпаратты құпия сақтауға;

2) АКҚҚ жабық кілттерінің мазмұнын құпия сақтауға;

3) негізгі ақпарат тасығыштардың және АКҚҚ-ны пайдалануға байланысты басқа да құжаттардың сақталуына жеке жауап береді.

6.3 Университетте бөгде адамдардың оларға қол жеткізу, негізгі ақпаратты рұқсатсыз пайдалану немесе көшіру мүмкіндігін болдырмайтын түйінді тасығыштарды сақтау шарттары қамтамасыз етілген. Негізгі тасымалдағыштар жеке пайдаланылатын шкафтарда (жәшіктерде, сейфтерде) сақталуы тиіс.

6.4 Тасымалдаушылардың ақауларының салдарынан негізгі ақпараттың жоғалуын болдырмау үшін тасымалдаушыларды негізгі ақпараттан алғаннан кейін резервтік көшірмелер жасалуы керек. Көшірмелер сәйкесінше таңбалануы керек және түпнұсқалар сияқты қолданылуы керек. Қолданыстағы және резервтік негізгі тасымалдағыштарды бөлек сақтау қамтамасыз етілуге тиіс.

6.5 Пайдаланушы АКҚҚ орнатылған компьютерде бағдарламалық АКҚҚ жұмыс істеуін бұзуы мүмкін бағдарламалардың (оның ішінде вирустардың) орнатылмауы және пайдаланылмауы үшін жауап береді.

6.6 Жұмыс орнында АКҚҚ-мен жабдықталған, көрсетілген құралдардың жұмысын бұзатын бөгде бағдарламалар немесе вирустар табылған жағдайда, осы жұмыс орнында ақпаратты қорғау құралдарымен жұмыс тоқтатылуы және осы бұзушылықтың теріс салдарын талдау және жою жөніндегі іс-шаралар ұйымдастырылуы тиіс.

6.7 АКҚҚ пайдаланушыларға:

1) негізгі ақпарат тасығыштардың мазмұнын жария етуге немесе тасығыштардың өзін оларға жіберілмеген адамдарға беруге, түйінді ақпаратты дисплейге және принтерге шығаруға;

2) кілттерді пайдаланудың штаттық рәсімдері болып табылмайтын жұмыстарды жүргізу кезінде (ақпаратты шифрлау/транскрипциялау,

электрондық цифрлық қолтаңбаны тексеру және т.б.), сондай-ақ басқа компьютерлердің диск жетектеріне немесе USB оқырмандарына дербес электрондық есептеу машинасының (бұдан әрі-ДЭЕМ) диск жетегіне немесе USB оқырманына негізгі тасымалдағышты енгізуге;

3) негізгі тасығышта бөгде ақпаратты жазуға;

4) АКҚҚ бағдарламалық жасақтамасына қандай да бір өзгерістер енгізуге;

5) жаңа ақпаратты жазу үшін бұрын жұмыста болған негізгі құралдарды пайдалануға тыйым салынады.

7 Кілттер бұзылған жағдайда әрекет ету й

7.1 жеке кілттерді бұзу деп мыналар түсініледі:

1) олардың жоғалуы (оның ішінде кейіннен табылуымен),

2) ұрлау,

3) жария ету,

4) рұқсатсыз көшіру,

5) оларды байланыс арналары арқылы ашық түрде беру,

6) негізгі тасымалдаушыға немесе осы ақпарат құралдарындағы негізгі ақпаратқа қол жеткізе алатын қызметкерді кез келген себеппен жұмыстан шығару,

7) нәтижесінде жеке кілттер рұқсатсыз тұлғаларға және (немесе) процестерге қолжетімді болуы мүмкін негізгі ақпаратты жария етудің кез келген басқа түрлері.

7.2 Пайдаланушы жеке кілттің бұзылу фактісін дербес анықтап, осы оқиғаның мәнін бағалауы керек. АКҚҚ көмегімен берілген құпия ақпараттыромаға келу салдарын іздестіру және оқшаулау жөніндегі іс-шараларды пайдаланушының өзі ұйымдастырады және жүзеге асырады.

7.3 Пайдаланушының кілті бұзылған жағдайда, ол басқа абоненттермен желі арқылы байланысты дереу тоқтатып, Университеттің Ақпараттық технологиялар департаментінің басшысы мен Ақпараттық қауіпсіздік қызметінің қызметкерін хабардар етуі керек. Кілттің бұзылуы туралы хабарлама келгеннен кейін 1 сағаттан кешіктірмей, АТД жүйеде Пайдаланушының кілтін құлыптауы керек. Жүйеде жұмысты қалпына келтіру бұзылған кілттерді ауыстырғаннан кейін ғана мүмкін болады.

8 Негізгі ақпаратты жою

8.1 Біржолғы пайдалану тасығыштарынан негізгі ақпаратты жою оларды пайдалану мүмкіндігін болдырмайтын, сондай-ақ негізгі ақпаратты қалпына келтіру арқылы жойылмайтын физикалық зақым келтіру жолымен жүргізіледі.

8.2 Бірнеше рет пайдаланылатын тасымалдағыштардан негізгі ақпаратты жою негізгі тасымалдаушыға зақым келтірместен негізгі ақпаратты өшіру арқылы жүзеге асырылады (оны бірнеше рет пайдалану мүмкіндігін қамтамасыз

ету үшін). Негізгі ақпарат тиісті бірнеше рет қолданылатын негізгі ақпарат құралдары үшін қабылданған технология бойынша жойылады.

8.3 Негізгі ақпаратты жою кезінде Пайдаланушылар жасайтын іс-әрекеттер тиісті актіде тіркеледі және пайдаланушы мен АҚҚ қызметкері қол қояды.

9 Келісу, бекіту және қолданысқа енгізу

9.1 Осы Ереже қызметі ақпараттық жүйелерді пайдалануға, ақпаратты криптографиялық қорғау құралдарын пайдалануға байланысты Университеттің құрылымдық бөлімшелерінің басшыларымен келісуге жатады. Егер Ереженің қағидалары материалдық жауапкершілік немесе негізгі ақпарат жеткізгіштерін есепке алу мәселелерін қозғаған жағдайда, келісу тиісті жауапты бөлімшелермен жүзеге асырылады.

9.2 Осы Ережені келісу талап етілетін лауазымды адамдар мен құрылымдық бөлімшелердің тізбесін құжатты әзірлеуші оның мазмұны мен қолданылу саласын ескере отырып айқындайды.

9.3 Ереженің жобасын қарау мерзімі оны алған сәттен бастап бес жұмыс күнінен аспауға тиіс. Ескертулер мен ұсыныстар дәлелді және нақты нысанда ресімделеді.

9.4 Ескертулер болмаған кезде немесе олар есепке алынғаннан кейін құжатқа Келісуші тұлғалар қол қояды және атқарушы органға Басқармаға бекітуге беріледі.

9.5 Осы Ереженің қолданысқа енгізілген күні олардың бекітілген күні болып есептеледі. Бекітілген сәттен бастап ережелер орындау үшін міндетті болып табылады.

9.6 Жаңа редакцияны бекіту немесе өзгерістер енгізу кезінде Ереженің алдыңғы нұсқасы күшін жояды және жарамсыз болып саналады.

10 Сақтау

10.1 Осы Ереженің түпнұсқасы Университеттің Ақпараттық қауіпсіздік қызметінде сақталады.

10.2 Ереженің электрондық нұсқасы мүдделі құрылымдық бөлімшелер мен уәкілетті қызметкерлер үшін қолжетімділікті қамтамасыз ете отырып, университеттің корпоративтік ақпараттық ресурстарында орналастырылады.

10.3 Университет қызметкерлерін осы Ережемен таныстыру ішкі нормативтік құжаттар үшін белгіленген тәртіппен танысу парағын ресімдеумен жүзеге асырылады.

10.4 Көшірмелерді есепке алу, рұқсатсыз пайдаланудың алдын алу және құжаттың құрылымдық бөлімшелерде сақталуына олардың басшылары жауапты болады.

Құжатты рұқсатсыз көшіруге тыйым салынады

11 Қайта қарау және өзектендіру тәртібі

11.1 Осы Ережені қайта қарауды Ақпараттық қауіпсіздік қызметі кемінде екі жылда бір рет жүзеге асырады және құжат талаптарын ақпаратты криптографиялық қорғау құралдарын пайдаланудың ағымдағы шарттарына, АТ-инфрақұрылымын дамытуға және АҚБЖ талаптарына сәйкес келтіруге бағытталған.

11.2 Ережені жоспардан тыс өзектендіру АҚБЖ-ның қолданылу саласы өзгерген кезде, Қазақстан Республикасы заңнамасының және ақпараттық қауіпсіздік саласындағы стандарттардың талаптары өзгерген кезде, криптографиялық қорғаудың жаңа құралдары енгізілген кезде, сондай-ақ инциденттердің, ішкі тексерулер мен ақпараттық қауіпсіздік аудиттерінің нәтижелері бойынша жүргізіледі.

11.3 Осы Ережеге өзгерістер мен толықтырулар жаңа редакция не жекелеген өкімдік құжат түрінде ресімделеді және осы Ережені бекіту үшін белгіленген тәртіппен бекітіледі.

Құжатты рұқсатсыз көшіруге тыйым салынады

Ф.01-2022

Келісу парағы

Лауазымы	Аты-жөні	Күні	Қолы
Басқарма мүшесі – Цифрландыру жөніндегі проректор	Амиров А.Ж.	9.12.25	
Заң қызметінің басшысы	Аязбаева Г.С.	9.12.25	
Software-орталығының басшысы	Штефан К.Б.	9.12.25	

Ф.02-2022

Танысу парағы

Лауазымы	Аты-жөні	Күні	Қолы