Бекітемін
«Әбілқас Сағынов атындағы Қарағанды техникалық университеті» КеАҚ
Басқарма Төрағасы – Ректор
_____ С.С. Сагинтаева
«11» марта 2025 ж. № 13
Басқарманың шешімі

ІШКІ НОРМАТИВТІК ҚҰЖАТ

АҚПАРАТТЫҚ ҚАУІПСІЗДІК САЯСАТЫ

ІНҚ II-03-2025

Әзірлеуші: ақпараттық қауіпсіздік инженері
Д.К. Читян _____

Қарағанды

Мазмұны

1 Қолдану саласы 3
2 Нормативтік сілтемелер 3
3 Терминдер, анықтамалар және қысқартулар 4
4 Жауапкершілік және өкілеттіктер 5
5 Жалпы қағидалар 6
6 Саясатты іске асыру жөніндегі шаралар 7
7 Құпиялылыққа қойылатын жалпы талаптар 8
8 Пайдаланушылардың ақпараттық жүйелерге қол жеткізу тәртібі 8
9 Желілік қауіпсіздік 9
10 Жергілікті қауіпсіздік 10
11 Құпиясөз саясаты 12
12 Физикалық қауіпсіздік 12
13 Ұйымның активтерін басқару 14
14 Еңбек ресурстарын басқару 15
15 Ақпаратты қайталау, сақтық көшірме жасау және сақтау 16
16 Ақпараттық қауіпсіздік аудиті 16
17 Саясат талаптарын бұзу 17
18 Ішкі нормативтік құжаттаманы келісу, бекіту және қолданысқа енгізу 17
19 Сақтау 18
20 АҚ Саясатын қайта қарау және өзектендіру тәртібі 18

1 Қолдану саласы

1.1 Ақпараттық қауіпсіздік саясаты (бұдан әрі – саясат) «Әбілқас Сағынов атындағы Қарағанды техникалық университеті» КеАҚ (бұдан әрі – Университет) қолданыстағы заңнаманың, Қазақстан Республикасының нормативтік құқықтық актілерінің және университеттің басқа да ішкі регламенттерінің талаптарына сәйкес әзірленді.

1.2 Бұл құжат университеттің өз қызметі шеңберінде ақпаратты қорғауды қамтамасыз ету тәсілін білдіреді. Ақпараттық активтерді қорғау ақпараттық қауіпсіздікті басқару жүйесінің (бұдан әрі – АҚБЖ) қатаң белгіленген қолданылу саласында жүзеге асырылады.

1.3 Осы Саясаттың ережелері ақпаратты өңдеу, сақтау, беру және қорғау үшін пайдаланылатын университеттің барлық цифрлық ақпараттық ресурстары мен жүйелеріне қолданылады. Осы саясатты сақтау Университеттің ақпараттық жүйелері мен деректеріне қол жеткізе алатын қызметкерлерді (штаттық, уақытша, қоса атқаратын, шарт бойынша және т.б.), тағылымдамадан өтушілерді, практиканттарды, сондай-ақ үшінші тұлғаларды (мердігерлерді, аудиторларды және т. б.) қоса алғанда, университеттің цифрлық ресурстарының барлық пайдаланушылары үшін міндетті болып табылады.

1.4 Саясат ережелері университеттің ақпараттық жүйелері мен құжаттарына қатысы бар клиенттер мен өзге де үшінші тұлғалардың назарына олардың университетпен өзара іс-қимылы шеңберінде қаншалықты қажет болса, соншалықты жеткізіледі.

1.5 Осы Саясатпен танысу әрбір қызметкер үшін жұмысқа қабылдау кезінде міндетті болып табылады.

1.6 Ақпараттық қауіпсіздікті қамтамасыз ету процесі сыртқы және ішкі ортадан туындайтын қорғаныс параметрлерін үнемі реттеуді және жаңа қауіптерге бейімделуді талап ететін үздіксіз процесс ретінде қарастырылады.

1.7 Осы саясатқа, сондай-ақ осындай қажеттілік туындауына қарай ақпараттық қауіпсіздік жөніндегі өзге де рәсімдер мен құжаттарға уақтылы өзгерістер енгізу үшін кедергілер болмауы тиіс.

1.8 Осы Саясаттың ережелері ішкі нормативтік және әдістемелік құжаттарда қолданылады, сондай-ақ контрагенттермен шарттар жасасу кезінде ескеріледі. Саясат университеттің ішкі нормативтік құжаты болып табылады.

2 Нормативтік сілтемелер

Осы саясатты әзірлеу кезінде ақпараттық қауіпсіздік саласындағы мынадай нормативтік құқықтық актілер мен стандарттар пайдаланылды:

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

«Ақпараттық-коммуникациялық технологиялар және ақпараттық қауіпсіздікті қамтамасыз ету саласындағы бірыңғай талаптарды бекіту туралы»

Қазақстан Республикасы Үкіметінің 2016 жылғы 20 желтоқсандағы № 832 қаулысы;

«Байланыс туралы» Қазақстан Республикасының 2004 жылғы 5 шілдедегі №567-II Заңы;

«Ақпаратқа қол жеткізу туралы» Қазақстан Республикасының 2015 жылғы 16 қарашадағы № 401-V Заңы;

ҚР СТ ISO/IEC 27001-2023 «Ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Ақпараттық қауіпсіздіктің менеджмент жүйелері. Талаптар»;

ҚР СТ ISO/IEC 27002-2023 «Ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Ақпараттық қауіпсіздікті басқару құралдары»;

Қазақстан Республикасының 2007 жылғы 24 желтоқсандағы № 691 ҚР СТ 1699-2007 Мемлекеттік стандарты. «Бақылау жүйелері және қол жетімділікті басқару»;

Қазақстан Республикасының Мемлекеттік стандарты ҚР СТ 34.005-2002 «Ақпараттық технология. Негізгі терминдер мен анықтамалар»;

«Дербес деректер және оларды қорғау туралы» Қазақстан Республикасының 2013 жылғы 21 мамырдағы № 94-V Заңы.

3 Терминдер, анықтамалар және қысқартулар

1) Суперпайдаланушы – кез келген операцияларды орындауға толық құқықтары бар АЖ әкімшісі;

2) ПОҚ – профессорлық-оқытушылар құрамы;

3) АТД – Ақпараттық технологиялар департаменті;

4) Қағидалар – жүйеде іс-әрекеттерді орындаудың міндетті шарттары;

5) Рұқсатсыз әрекет – ақпаратты өңдеудің белгіленген қағидаларын бұзу;

6) Пайдаланушы – ақпаратты белгіленген қол жеткізу құқықтары шеңберінде пайдаланатын субъект;

7) Жергілікті желі (LAN) – деректерді беру үшін қосылған түйіндер тобы;

8) Ақпараттық жүйе (АЖ) – функционалдық міндеттерді шешуге арналған ИКТ, персонал және құжаттама жиынтығы;

9) Ақпараттық қауіпсіздік (АҚ) – АЖ мен деректердің қауіптен қорғалуы;

10) АҚ инциденті – АЖ немесе деректердің жұмысына қауіп төндіретін іркіліс немесе бұзушылық;

11) Құпия ақпарат – заң бойынша қолжетімділігі шектеулі мәліметтер;

12) Электрондық ақпараттық ресурстар - электрондық жеткізгіштердегі немесе АЖ-дегі цифрлық нысанды ақпарат;

13) Бағдарламалық қамтамасыз ету (БҚ) – құжаттамасы бар бағдарламалар мен кодтардың жиынтығы;

14) Есептеу техникасының құралдары - деректерді өңдеудің бағдарламалық және аппараттық элементтері;

15) Утилита - ОЖ және жабдықпен жұмыс істеуге арналған қосалқы бағдарлама;

16) ДББЖ (деректер базасын басқару жүйесі) — деректер базасын құруға, сақтауға, модификациялауға және басқаруға, сондай-ақ берілген ережелер мен шектеулерді сақтай отырып, деректерге қол жеткізуді қамтамасыз етуге арналған бағдарламалық қамтамасыз ету. ДББЖ әртүрлі операциялар кезінде деректердің тұтастығын, қауіпсіздігін, дәйектілігін және қалпына келтірілуін қамтамасыз етеді.

17) ОЖ (Операциялық жүйе) – компьютер ресурстарын басқаруға арналған бағдарламалық қамтамасыз ету;

18) ДД (Дербес деректер) – Дербес деректер субъектісіне жататын мәліметтер;

19) АЖДД (ДД ақпараттық жүйесі) - дербес деректерді өңдеу жүйесі;

4 Жауапкершілік және өкілеттіктер

4.1 Осы Саясатты Университет Басқарма Төрағасы - Ректоры Басқарма шешімінің негізінде бекітеді.

4.2 Университет Басшылығы:

- тұтастай алғанда ақпараттық қауіпсіздіктің (АҚ) қажетті деңгейін ұстап тұру үшін өзіне жауапкершілік алады;
- ақ саласындағы қызметті барлық қажетті ресурстармен (қаржылық, кадрлық, техникалық)қамтамасыз етеді;
- АҚ критериилерін және оның тиімділігін анықтайды және оларды үнемі қайта қарап отырады.

4.3 АҚ бойынша жауапты қызметкер:

- осы Саясатты және ілеспе регламенттерді әзірлеуді, енгізуді, қолдауды және өзектендіруді үйлестіреді;
- АҚ талаптарының орындалуына мониторинг ұйымдастырады, жоғары басшылық үшін ДББЖ жұмыс істеуі туралы есеп дайындайды;
- АҚ инциденттерін қызметтік тергеуге бастамашылық жасайды және процестерді түзету бойынша ұсыныстар енгізеді.

4.4 Құрылымдық бөлімшелердің басшылары:

- АҚ жөніндегі қызметкерлерге ішкі құжаттардың талаптарын уақтылы жеткізеді;
- олардың бөлімшелеріне тиесілі ақпараттық активтерді бөледі, оларға қол жеткізуге өтінімдерді келіседі;
- бөлімше қызметкерлерінің АҚ бойынша саясат талаптарын және өзге де актілерді орындауын қамтамасыз етеді;
- АҚ бойынша жауапты тұлғаға барлық оқиғалар немесе АҚ талаптарын бұзуға күдік туралы дереу хабарланып отырады.

4.5 Университет қызметкерлері мен ПОҚ:

- АҚ өзінің лауазымдық міндеттері шеңберінде және қорғалатын ақпараттық активтермен жұмыс істеу кезінде қойылатын талаптардың сақталуына дербес жауап береді;

- осы Саясатты және оның негізінде әзірленген құжаттарды Қазақстан Республикасының ішкі нормативтік актілері мен заңнамасына сәйкес бұзғаны үшін жауапты болады;

- тәртіптік, әкімшілік немесе өзге де жауапкершілік шараларын жоғары басшылық бұзушылықтың сипаты мен ниетін ескере отырып, қызметтік тергеу нәтижелері бойынша қолданады.

5 Жалпы қағидалар

5.1 Мақсаттар мен міндеттер.

5.1.1 Университеттің ақпараттық қауіпсіздігінің мақсаты - ақпараттық активтерді қатерлерден, соның ішінде зиянды әрекеттерден, апаттардан, персоналдың қателіктерінен және техникалық іркілістерден қорғау, сондай-ақ технологиялық процестердің үздіксіз жұмысын қамтамасыз ету.

5.1.2 Ақпараттық қауіпсіздік бағыты ақпараттық технологиялар департаментінде құрылды, ал оның міндеттері мен функцияларын АҚ бойынша жауапты адам орындайды:

- АҚ бойынша нормативтік құжаттарды әзірлеу және өзектендіру;
- құпия ақпарат пен дербес деректерді қорғау;
- қауіптерді бағалау және техникалық қорғау шараларын ұйымдастыру;
- АҚ жағдайын бақылау, осал жерін анықтау және жою;
- жоспарлы тексерулер жүргізу және инциденттерді тергеу;
- дербес деректерді өңдейтін бөлімшелермен өзара іс-қимыл жасау;
- қызметкерлерді АҚ мәселелеріне оқыту;
- инциденттерге дайындықты қамтамасыз ету және оларға жедел пайымдау жасау.

5.2 Ақпараттық қауіпсіздік қызметкерлерінің ұйымдық-құқықтық мәртебесі.

5.2.1 АҚ бойынша қызметкерлердің ақпараттық жүйелері бар үй-жайларға кіруге құқығы бар және қауіп төнген кезде деректерді өңдеуді тоқтатуды талап ете алады;

5.2.2 Ақпараттық қауіпсіздік мәселелеріне қатысты бөлігінде ақпараттық технологияларды қолдану мәселелері бойынша пайдаланушылар мен әкімшілерден қажетті ақпаратты алуға құқығы бар;

5.2.3 Ақпараттық қауіпсіздікке жауапты қызметкерлердің ақпаратты қорғау және өңдеу жөніндегі талаптарға сәйкестігін тексеру мақсатында қолданыстағы және енгізілетін ақпараттық жүйелер мен бағдарламалық қамтамасыз етуге аудит жүргізуге құқығы бар. Заңнаманың талаптарына сәйкессіздіктер анықталған немесе қауіпсіздікке елеулі қатерлерді іске асыру тәуекелі болған кезде, бұл қызметкерлер бұзушылықтар жойылғанға дейін

көрсетілген АЖ және БҚ пайдалануды тоқтата тұруға немесе тыйым салуға құқылы.

5.2.4 АҚ қызметкерлері ақпараттық қауіпсіздік стандарттарына сәйкестігі үшін үнемі аттестаттаудан өтуге және осы саладағы өз құзыреттерін растауға міндетті.

5.3 Ақпараттық қауіпсіздік саясатының принциптері

5.3.1 Университеттің ақпараттық қауіпсіздік саясаты мынадай қағидаттарға негізделеді:

1) Ақпараттың құпиялылығын, тұтастығын және қолжетімділігін сақтау арқылы ақпараттық қауіпсіздікті қамтамасыз етуге;

2) Құпиялылық – ақпаратқа тек уәкілетті тұлғаларға қол жеткізуді ұсынуға (уәкілетті тұлға – тіркеуден өткен және өзінің есептік жазбасымен кірген сайтқа кіруші);

3) Тұтастық – тек қана уәкілетті тұлғалардың жалпыға қолжетімді электрондық ақпараттық ресурстарға (дербес компьютерлер, корпоративтік электрондық пошта, Directum және т. б.) өзгерістер енгізуге;

4) Қолжетімділік – уәкілетті пайдаланушыларға өздерінің қызметтік міндеттерін орындау үшін электрондық ресурстарға (ДК, электрондық пошта, Directum және т.б.) қол жеткізуді қамтамасыз етуге.

6 Саясатты іске асыру жөніндегі шаралар

6.1 Университетте ақпараттық қауіпсіздікті қамтамасыз ету шаралары:

1) құқықтық – заңнамалық және нормативтік актілер;

2) ұйымдастыру – әкімшілік рәсімдер мен регламенттер;

3) физикалық – қор ғаныс конструкциялары мен техникалық құралдар;

4) техникалық – аппараттық және бағдарламалық қорғау әдістері.

6.2 Құқықтық қорғау шаралары ақпаратты пайдалануды реттейтін, оны өңдеу кезінде қызметкерлердің құқықтары мен міндеттерін айқындайтын және белгіленген талаптарды бұзғаны үшін жауапкершілікті қамтамасыз ететін нормативтік құқықтық актілерді қамтиды. Бұл шаралар оқиғалардың алдын алуға бағытталған және университеттің ақпараттық жүйелерімен жұмыс істейтін пайдаланушылар мен сыртқы мердігерлерді үнемі хабардар етуді талап етеді.

6.3 Ұйымдастырушылық (әкімшілік) қорғау шаралары ақпараттық жүйелерді пайдалану ережелерін белгілейді, пайдаланушылардың қолжетімділігін реттейді, сыртқы мердігерлердің жұмыс тәртібін айқындайды және ақпараттық қауіпсіздіктің ықтимал қатерлерін болдырмайды. Бұл шаралар инциденттер туындаған кезде ықтимал тәуекелдер мен шығындарды азайтады.

6.4 Физикалық қорғаныс шаралары университеттің маңызды инфрақұрылымына рұқсатсыз кіруді шектеуге арналған механикалық және электронды-механикалық құрылғыларды пайдалануды қамтиды. Олардың

құрамына бейнебақылау, күзет дабылы, кіруді бақылау жүйелері және басқа да инженерлік-техникалық қауіпсіздік құралдары кіреді.

6.5 Техникалық (аппараттық-бағдарламалық) қорғау шаралары университеттің ақпараттық жүйелеріне енгізілген мамандандырылған жабдықтар мен бағдарламалық қамтамасыз ету арқылы іске асырылады. Бұл шаралар пайдаланушыларды сәйкестендіру мен аутентификациялауды, қол жеткізу құқықтарын бөлуді, оқиғаларды тіркеуді, деректерді криптографиялық қорғауды және университеттің ақпараттық ортасының қауіпсіздік деңгейін арттыруға бағытталған басқа мүмкіндіктерді қамтамасыз етеді.

7 Құпиялылыққа қойылатын жалпы талаптар

7.1 Университетте ақпараттың құпиялылығын қамтамасыз етуге қойылатын негізгі талаптар оның сыртқы шығып кетуіне (жария етілуіне) жол бермеу және оған тек уәкілетті тұлғалар үшін қол жеткізуді қамтамасыз ету болып табылады.

7.2 Пайдаланушылардың университеттің ақпараттық жүйелеріндегі барлық іс-әрекеттері міндетті түрде журналға жазылуға тиіс: іс-әрекеттер туралы ақпаратты әкімшілер мәтіндік лог-файлдарға тіркейді және университет серверлерінде кемінде үш жыл сақталады және кемінде екі ай жедел қолжетімділікте болады.

8 Пайдаланушылардың ақпараттық жүйелерге қол жеткізу тәртібі

8.1. Ақпараттық жүйелерге қолжетімділікті басқару пайдаланушылардың әрекеттерін сәйкестендіруді, аутентификациялауды және тіркеуді қамтамасыз ететін стандартты ОЖ (Windows Server, Linux) және ДББЖ құралдарын пайдалана отырып жүзеге асырылады.

8.2. Университетте рұқсатсыз кіруден қорғаудың сертификатталған немесе рұқсат етілген құралдары, соның ішінде кіруді басқару, тіркеу, антивирустық қорғаныс, брандмауэр, қауіпсіздікті талдау және интрузияны анықтау ішкі жүйелері қолданылады.

8.3. Пайдаланушылардың барлық әрекеттері тек әкімші қол жеткізе алатын жүйелік журналдарда жазылады. Ол жазбалардың толықтығына жауап береді және оларды сұраныс бойынша АҚ-ға жауап береді.

8.4. Әкімшілік қолжетімділік АҚ жөніндегі инженермен міндетті келісе отырып, қызметтік жазба бойынша беріледі. Жалпы немесе алдын ала орнатылған есептік жазбаларды пайдалануға тыйым салынады. Қол жеткізу құқығын арттыру да келісуді қажет етеді.

8.5. Журналдарда тіркеусіз мәліметтер базасына кіруге тыйым салынады. Супер пайдаланушылар жұмыстан шығарылған кезде, парольдер жұмыстан шығарылған күні өзгереді.

8.6. Ақпараттық жүйелерге өзгерістер енгізу қауіпсіздік талаптарын ескере отырып жүзеге асырылады, жоспарлау, тестілеу, енгізу және кейінгі мониторингті қамтиды. Барлық өзгерістер АҚ саясатына сәйкес келуі және қажет болған жағдайда қайта қаралуы тиіс.

9 Желілік қауіпсіздік

9.1 Интернеттегі университеттің ішкі желісіне қол жеткізу

9.1.1 Ішкі желіге кіру тек желіаралық реттелген экран арқылы ғана жүзеге асырылады.

9.1.2 Желінің периметрінен тыс қолжетімділікке ақпараттық қауіпсіздік жөніндегі жауапты адаммен келісе отырып, белгілі бір порт бойынша және белгілі бір уақытқа АТД директорының өкімі бойынша ғана рұқсат етіледі.

9.1.3 Жеке емес, топтық және анонимді есептік жазбаларды қолдана отырып, жергілікті желіге қашықтан кіруге тыйым салынады.

9.1.4 Университеттің корпоративтік желісінің ресурстарына қашықтан қол жеткізуді әкімшілендіру кезінде мынадай талаптар қойылады:

Пайдаланушыларға қашықтан қол жеткізу тек VPN технологиясын немесе басқа шифрлау хаттамаларын қолдана отырып, тіркелген жеке есептік жазбалар негізінде қамтамасыз етіледі.

9.2 Тыйымдар мен шектеулер

9.2.1 Университеттің компьютерлік желілерінің қауіпсіздігін және тұрақты жұмыс істеуін қамтамасыз ету мақсатында:

1) кез келген компьютерлік жабдықты (соның ішінде сымсыз кіру нүктелері, маршрутизаторлар, желілік принтерлер, IP-камералар, медиа ойнатқыштар, дербес ноутбуктер және т.б.) АТД-не және АҚ-ға жауапты адаммен алдын ала келіспей, университеттің жергілікті желісіне өз еркімен қосылуға.

2) Жұмыс станцияларын, компьютерлерді және өзге де желілік жабдықтарды желілік розеткалар, VLAN немесе басқа да коммуникациялық интерфейстер арасында АТД-мен келіспей жылжытуға.

3) Университеттің ақпараттық ресурстарын (Интернет желісін қоса алғанда):

– желілік/онлайн ойындарға қатысуға;

– коммерциялық, жабысқақ немесе қажетсіз жарнамаларды (соның ішінде СПАМды) таратуды пайдалануға;

- заңмен тыйым салынған зиянды бағдарламаны, заңсыз мазмұнды контентті сақтауға немесе таратуға тыйым салынады.

4) желілік сканерлеуді, трафикті ұстап қалуды, қорғау құралдарын (мысалы, желіаралық экрандарды, прокси-серверлерді) айналып өту әрекеттерін, сондай-ақ егер бұл қызметкердің міндетіне кірмесе және АТД мен

АҚ-мен келісілмеген болса, желілік инфрақұрылымды талдауға байланысты кез келген әрекеттерді орындауға.

5) VPN-туннельдерді, прокси-қосылыстарды немесе сүзу және трафикті бақылау жүйелерін рұқсатсыз айналып өтудің өзге де арналарын жасау үшін бағдарламалық қамтамасыз етуді немесе құрылғыларды пайдалануға.

6) Желілік инфрақұрылымның жұмысына әсер етуі немесс АҚ талаптарын бұзуы мүмкін DHCP, DNS, FTP, веб-серверлер және басқа қызметтер сияқты желілік қызметтерді өз бетінше орнатуға және пайдалануға.

7) Желілік адаптердің параметрлерін, IP мекенжайын, шлюз параметрлерін, DNS және басқа желілік параметрлерді жұмыс құрылғыларында тиісті өкілеттіктерсіз немесе АТД нұсқауларынсыз өзгертуге тыйым салынады.

9.3 Қорғаныс құралдарын сатып алу

9.3.1 Университетте ақпаратты қорғау құралдары мен жүйелерін сатып алу, енгізу және пайдалану ақпараттық қауіпсіздікке жауапты және ақпараттық технологиялар департаментімен (АТД) және университет басшылығымен келісу бойынша ғана жүзеге асырылады. Бұл қолданыстағы АТ-инфрақұрылыммен үйлесімділікті, қолданылу тиімділігін және ақпараттық қауіпсіздік саласындағы Қазақстан Республикасының нормативтік құқықтық актілерінің талаптарына сәйкестігін қамтамасыз ету үшін қажет.

9.3.2 Ақпаратты қорғау құралдарын таңдау кезінде уәкілетті мемлекеттік органдар берген сәйкестік сертификаттары немесе қолданылуы туралы оң қорытындылары бар шешімдерге басымдық беріледі. Белгіленген тәртіппен сертификатталмаған немесе тіркелмеген қаражатты пайдалануға негіздеме болған кезде және АҚ бойынша жауапты адамнан жазбаша келісім алғаннан кейін ғана жол беріледі.

9.3.3 Сатып алынатын ақпаратты қорғаудың барлық құралдары, егер бұл қорғау тетіктерінің дұрыс жұмыс істеуі мен өзектілігі үшін қажет болса, Техникалық құжаттамамен, лицензиялармен, сондай-ақ техникалық қолдау мен жаңартуға арналған шарттармен сүйемелденуге тиіс.

10 Жергілікті қауіпсіздік

10.1 Вирусқа қарсы қорғаныс

10.1.1 Вирусқа қарсы қорғаныс университет пайдаланушыларының серверлері мен жұмыс орындарын зиянды бағдарламалық жасақтамадан қорғауды қамтамасыз етуге арналған.

10.1.2 Пайдалануға берілген әрбір компьютерде немесе серверде, сондай-ақ операциялық жүйені қайта орнатқаннан кейін АТД қызметкерлері міндетті түрде вирусқа қарсы бағдарламаны орнатады және іске қосады.

10.1.3 Вирусқа қарсы қорғауды өшіруге немесе антивирустық базаның жаңартуларын рұқсатсыз өшіруге тыйым салынады. Вирусқа қарсы бағдарламалық қамтамасыз етуді орнатуды және жаңартуды бақылауды АТД қызметкерлері орталықтандырылған түрде жүзеге асырады.

10.1.4 Жаппай вирустық шабуыл болған жағдайда, АТД қызметкерлері инфекцияның ауқымын анықтайды, қауіпті оқшаулайды, оның таралуын блокқа қояды және АҚ жөніндегі инженермен бірге инфекцияның көзін, вирустың әсер ету және таралу сипатын анықтайды, сондай-ақ салдарын жояды. Қажет болса, осалдықтарды жою үшін патчтар мен бағдарламалық қамтамасыз ету құралдары жаңартылып орнатылады.

10.2 Ақпараттық жүйелерге және деректерді сақтау жүйелеріне қол жеткізу құқықтарын ажырату, рұқсат етілмеген кіруден (РЕК) қорғау.

10.2.1 Университеттің ақпараттық жүйелеріне тек тіркелген логиндер мен парольдер арқылы қол жеткізуге болады.

10.2.2 Операциялық жүйелер мен қосымшаларға қол жеткізу кезінде артықшылықтарды барынша азайту қағидаты іске асырылады.

10.2.3 Университеттің ұйымдық және техникалық бөлімшелері қол жеткізу деңгейі және өңделетін ақпарат түрі бойынша бөлінеді. Бұл пайдаланушылардың құқықтары рөлдерге сәйкес шектелген тиісті АЖ құралдарымен жүзеге асырылады.

10.2.4 АЖ әкімшісі қол жеткізу журналын жүргізеді, рұқсат етілмеген кіру (РЕК) әрекеттерін тіркейді және бұл туралы АҚ жөніндегі инженерге хабарлайды.

10.2.5 Жұмыстан шығарылған қызметкерлердің есептік жазбаларын пайдалануға қатаң тыйым салынады.

10.3 Электрондық поштаны, Интернет желісін пайдалану.

10.3.1 Қазақстан Республикасының заңнамасында тыйым салынған немесе шектелген материалдарды таратуға тыйым салынады.

10.3.2 Құпия ақпаратты тек корпоративтік электрондық пошта арқылы ғана беруге рұқсат етіледі.

10.3.3 Қызметкерлердің жұмыс орындарындағы электрондық пошта тек қызметтік хат алмасу үшін пайдаланылады.

10.3.4 Корпоративтік поштаның логині мен паролін АТД қызметкерлері АТД директорының атына қызметтік жазба негізінде қызметкерлер мен студенттерге береді.

10.3.5 Күдікті тіркемелері бар және белгісіз жіберушілерден келген хаттарды ашуға тыйым салынады. Мұндай жағдайлар туралы АҚ жөніндегі инженерге дереу хабарлау қажет.

10.3.6 Құпия ақпаратты әлеуметтік желілерде жариялауға және оны мессенджерлер (WhatsApp, Telegram және т.б.) арқылы беруге тыйым салынады.

10.3.7 Құпия ақпаратты өңдеуге арналған жұмыс орындарында жеке серверлері Қазақстан Республикасынан тыс жерлерде орналасқан «бұлтты» деректер қоймаларын пайдалануға тыйым салынады.

11 Құпиясөз саясаты

11.1 Жеке паролі бар барлық пайдаланушылар оны құпия сақтайды, оны есте ұстайды немесе бөгде адамдар үшін қол жетімсіз жерде тіркейді.

11.2 Пайдаланушы парольдерін пайдалану, ауыстыру және тоқтату процестерін ұйымдастырушылық және техникалық қамтамасыз ету АТД қызметкерлерін әкімшілендіруге жүктеледі.

11.3 Пароль саясатын сақтау талаптары барлық пайдаланушыларға, соның ішінде әкімшілерге (желілер, серверлер, ақпараттық жүйелер), ерекшеліктерсіз қолданылады. Парольдерді қалыптастырудың, ауыстырудың және бұғаттаудың барлық рәсімдері белгіленген ережелерге сәйкес болуы тиіс.

11.4 Парольді енгізген кезде пайдаланушы оны бөгде адамдардың (мысалы, артқы жағындағы адам, адамның саусақтардың қозғалысын тікелей немесе шағылысқан жарықта бақылауы) және техникалық құралдардың (стационарлық және ұялы телефондарға салынған бейнекамералар және т.б.) көру мүмкіндігін болдырмауы қажет.

11.5 Пайдаланушы парольді ауыстыру рәсімі мынадай жағдайларда дербес жүргізіледі:

1) бірінші авторизация кезінде, әкімші берген уақытша парольді өзгерту қажет болғанда;

2) парольдің қолданылу мерзімі аяқталған кезде;

3) парольді өзгерту туралы өз бетінше шешім қабылдаған кезде.

11.6 Пароль бұзылған кезде пайдаланушының паролін өзгерту рәсімі пайдаланушы жұмыс істейтін (жұмыс істеген) құрылымдық бөлімше басшысының қызметтік жазбасы негізінде жүзеге асырылады. Парольді ауыстыру себебін негіздей отырып, қызметтік жазба кейіннен қызметтік жазбаны АТД қызметкеріне орындауға жіберетін ақ жауапты қызметкерімен келісе отырып, АТД-ге жіберілуі тиіс.

11.7 Жұмыстан шығарылған немесе жұмыстан шыққан, басқа құрылымдық бөлімшеге ауыстырылған, оқуды бітірген, оқудан шығарылған пайдаланушылардың есептік жазбаларын бұғаттауды «айналып шығу» парағына қол қою кезінде АТД қызметкерлері жүргізеді.

12 Физикалық қауіпсіздік

12.1 Қауіпсіздік аймағын ұйымдастыру

12.1.1 Ақпаратты өңдеу құралдарымен байланысты аса маңызды және сезімтал активтер арнайы бөлінген қауіпсіздік аймақтарында орналастырылады. Бұл аймақтар қорғалатын периметрмен шектелген және физикалық кедергілермен және кіруді бақылау құралдарымен жабдықталған.

12.1.2 Ақпараттық жүйелерді қорғау мақсатында:

– ұялы құрылғылардың фото-, бейне-, аудио аппаратурасын, сондай-ақ цифрлық камераларын пайдалануға арнайы рұқсат болған жағдайда ғана жол беріледі;

– келушілердің қауіпсіздік аймақтарына кіруі университеттің уәкілетті қызметкерлерінің сүйемелдеуімен, рұқсаты болған жағдайда, келу күні мен уақытын міндетті түрде тіркей отырып жүзеге асырылады;

- маңызды ақпаратқа және оны өңдейтін жабдыққа қол жеткізу бақыланады және қауіпсіздік аймақтарына жіберілген қызметкерлердің бекітілген тізіміне енгізілгендерге ғана беріледі;

- қызметкерлер мен сыртқы персоналдың визуалды сәйкестендіру құралдары болуы тиіс; үшінші тұлғаларға Университет өкілдерінің ертіп жүруімен ғана рұқсат етіледі;

- қызметкерлер мен үшінші тарап қызметкерлеріне қол жеткізу құқығы үнемі қайта қаралады және жаңартылады;

12.1.3 Қауіпсіздік аймақтарында техникалық жұмыстарды жүргізу осы аймақтарда міндеттердің болуы мен орындалу қағидаларын айқындайтын ішкі регламенттер мен нұсқаулықтар бойынша жүзеге асырылады. Маңызды жабдыққа қызмет көрсетуге тек сертификатталған персоналға ғана рұқсат беріледі.

12.2 Жабдықтың қауіпсіздігі

12.2.1 Жұмыс кеңістігі халықтың санитариялық-эпидемиологиялық саламаттылығы саласындағы уәкілетті органдар бекіткен санитариялық нормалар мен талаптарды сақтай отырып ұйымдастырылады.

12.2.2 Ақпараттық қауіпсіздікке жауаптылар қараусыз қалған жабдықты қорғау және белгіленген ережелерді бұзғаны үшін жауапкершілік мәселелері бойынша қызметкерлер арасында түсіндіру жұмыстарын жүргізеді.

12.2.3 Активтерді қорғалатын аумақтан тыс жерге шығару, олардағы деректерді міндетті түрде жоюмен қайта пайдалану, орнын ауыстыру және кәдеге жарату тәртібі Жабдық пен бағдарламалық қамтамасыз етуді түгендеу мен паспорттаудың ішкі қағидаларында айқындалады.

12.2.4 Ақпараттық технологиялар департаменті жұмыс станциялары мен серверлерді олардың конфигурацияларын тексерумен үнемі түгендеп отырады.

12.2.5 Пайдаланушылар қараусыз қалған жабдықты қорғау ережелері туралы хабардар болуы және осы ережелерді сақтамаудың салдарын түсінуі керек.

12.2.6 Ақпаратқа рұқсатсыз қол жеткізу, жоғалту немесе бүліну тәуекелдерін азайту үшін мыналарды қолдану ұсынылады:

- «таза үстел» саясаты – қағаз тасымалдағыштар мен алынбалы дискілерге қатысты;

- «таза экран» саясаты – ақпаратты өңдеу құрылғыларына қатысты.

12.2.7 Келесі шараларды да ескеру қажет:

1) Маңызды ақпараты бар тасымалдаушылар, егер олар пайдаланылмаса немесе үй-жай бос болса, тазалануы және құлыпталуы тиіс;

2) Компьютерлер, терминалдар мен принтерлер жұмыс аяқталғаннан кейін өшірілуі керек;

3) Қараусыз қалған жабдық парольдермен немесе өзге де құралдармен қорғалуы тиіс;

4) Белгілі бір белсенді емес уақыт өткеннен кейін экранды автоматты түрде бұғаттауды орнату керек;

5) Құпия ақпараты бар құжаттарды басып шығарғаннан кейін дереу принтерлерден алу қажет.

13 Ұйымның активтерін басқару

13.1 Активтерді есепке алу және пайдалану

13.1.1 Ақпарат болып табылатын немесе ақпаратты қамтитын немесе ақпаратты өңдеуге, сақтауға, беруге қызмет ететін және университет үшін құндылығы бар материалдық немесе материалдық емес объект (бұдан әрі - ақпаратты өңдеу құралдарымен байланысты Активтер; Актив) қорғалуы және басқарылуы тиіс.

13.1.2 Ақпараттық қауіпсіздікті қамтамасыз етудің негізгі объектілері (активтері) мынадай элементтер болып табылады:

1) Таратылуы шектелген мәліметтерді қамтитын және магниттік, оптикалық және басқа негізде тасығыштарда, ақпараттық физикалық өрістерде, массивтерде және деректер базаларында құжаттар немесе жазбалар түрінде ұсынылған Ақпараттық ресурстар;

2) Ақпаратты өңдеу жүргізілетін ақпараттық жүйелердің бағдарламалық құралдары (операциялық жүйелер, деректер базасын басқару жүйелері, басқа да жалпы жүйелік және қолданбалы бағдарламалық қамтамасыз ету) ;

3)Байланыс және деректерді берудің автоматтандырылған жүйелері (телекоммуникация құралдары);

4)Ақпарат берілетін байланыс арналары (оның ішінде таралуы шектеулі);

5) Ақпараттық ресурстарды өңдеуге, сақтауға және беруге арналған есептеу техникасы құралдары (аппараттық құралдар).

13.1.3. Активтерді қорғауды қамтамасыз ету үшін:

1) Қолдану шекараларын анықтау;

2) Активтерді түгендеу;

3) Активтерді сәйкестендіру;

4) Университетте қабылданған жіктеу жүйесіне сәйкес Активтерді жіктеу және таңбалау;

5) Активтерді лауазымды тұлғаларға (иелеріне) бекіту және активтердің АҚ басқару жөніндегі іс-шараларды іске асыру үшін олардың жауапкершілік шараларын айқындау.

13.1.3 Активтердің иесі активтердің бүкіл өмірлік циклі бойына активтерді дұрыс басқаруды қамтамасыз етеді.

13.1.4 Оларды есепке алуды, бақылауды ұйымдастыру активтерінің қозғалысына мониторингті жүзеге асыру және қорғаудың тиісті деңгейін қамтамасыз ету мақсатында ұйымда ақпаратты өңдеу құралдарымен байланысты активтердің тізбесі жүргізіледі, онда активтің атауы, активтің сыныбы, активтің түрі, активтің маңыздылығы туралы ақпарат қамтылады.

14 Еңбек ресурстарын басқару

14.1 Жұмысқа қабылдау кезінде персоналды тексеру

14.1.1 Жұмысқа қабылдау кезінде, сондай-ақ үшінші тарап ұйымдарынан мердігерлер мен пайдаланушыларды тарту кезінде дербес деректердің құпиялылығын сақтай отырып, Университеттің ішкі регламенттеріне және Қазақстан Республикасының қолданыстағы заңнамасына сәйкес мұқият тексеру жүргізіледі.

14.1.2 Қызметі қолжетімділігі шектеулі қызметтік ақпаратты өңдеумен не құпия мәліметтермен және тиісті техникалық құралдармен байланысты кандидаттар мен ұйымдарды тексеруге ерекше назар аударылады.

14.1.3 Университеттің ақпараттық жүйелеріне қол жеткізетін бөгде ұйымдардың қызметкерлері мен өкілдері ақпараттық қауіпсіздік талаптарын сақтау туралы келісімге қол қоюға міндетті. Бұл ресурстарды ұрлау, алаяқтық және теріс пайдалану қаупін азайту үшін қажет.

14.1.4 Университеттің ақпараттық жүйелеріне, жабдықтарына немесе ресурстарына қол жеткізуді ұсынар алдында қызметкер, мердігер немесе үшінші тарап ұйымының өкілі құпиялылық және ақпаратты жария етпеу туралы келісімге қол қояды.

14.1.5 Ақпараттық қауіпсіздік саласындағы функциялар мен жауапкершілік Университет қызметкерлерінің лауазымдық нұсқаулықтарында және/немесе еңбек шарттары талаптарында бекітіледі.

14.1.6 Штатқа қабылданатын қызметкерлер туралы барлық ақпарат Қазақстан Республикасының еңбек заңнамасына сәйкес жиналуға және өңделуге тиіс.

14.1.7 Үшінші тараптармен өзара іс-қимыл кезінде ақпараттық қауіпсіздікті қамтамасыз ету жөніндегі талаптар мен жауапкершілік шаралары жасалатын шарттардың талаптарында көрсетілуі тиіс.

14.1.8 Университеттің ақпараттық жүйелерін АҚ-пен қамтамасыз етуге байланысты жұмыстарға сыртқы ұйымдарды тарту кезінде осы объектілердің лауазымды тұлғасы (иесі) қол жеткізу, пайдалану шарттарын және оларды бұзғаны үшін жауапкершілік шараларын регламенттейтін шарттар жасасады.

14.2 Ақпараттық қауіпсіздік саласындағы қызметкерлердің хабардарлығын арттыру және оқыту

14.2.1 Университеттің барлық қызметкерлері осы Саясаттың ережелерімен, сондай-ақ бекітілген Ақпараттық қауіпсіздік ережелерімен және нұсқаулықтарымен танысуға міндетті. Танысу болуы керек

14.2.2 Саясат талаптарына және ілеспе нұсқаулықтарға кез келген өзгерістер мен толықтырулар олардың функционалдық міндеттеріне сәйкес ақпараттық жүйелерге қол жеткізе алатын қызметкерлерге уақтылы жеткізілуі тиіс.

14.2.3 Ақпараттық қауіпсіздік мәселелері бойынша оқыту немесе нұсқау беру қызметкер Университеттің ақпараттық ресурстары мен жүйелерін пайдалануды бастағанға дейін жүргізіледі.

14.3 Еңбек жағдайларын өзгерту және жұмыстан шығару

14.3.1 Еңбек шарты тоқтатылған немесе қызметкердің еңбек қызметінің шарттары өзгерген кезде Университеттің ақпараттық жүйелері мен ресурстарына қол жеткізудің барлық түрлері — физикалық және логикалық — жойылады немесе қайта қаралады. Бұл кіру идентификаторларын, жазылымдарды өшіруді, сондай-ақ қазіргі қызметкердің мәртебесін растайтын құжаттарды қайтарып алуды қамтиды.

14.3.2 Қызметкерлердің еңбек қатынастары аяқталғаннан кейін қолданылатын ақпараттық қауіпсіздік саласындағы міндеттемелері еңбек шартында бекітілуге тиіс.

15 Ақпаратты қайталау, сақтық көшірме жасау және сақтау

15.1 Деректердің физикалық тұтастығын қамтамасыз ету мақсатында, сондай-ақ қорғалатын ақпарат пен ақпараттық жүйелердің конфигурацияларын қасақана немесе байқаусызда жоюды немесе бұрмалауды болдырмау мақсатында тиісті техникалық және бағдарламалық резервтік көшіру құралдары болған кезде деректер базасының, конфигурациялардың, параметрлер файлдарының және конфигурациялық файлдардың резервтік көшірмесі ұйымдастырылады.

15.2 Аппараттық ақаулар, вирустық шабуылдар (төлем бағдарламаларын қоса алғанда) нәтижесінде жоғалуы мүмкін аса маңызды ақпараттың кепілдендірілген қалпына келтірілуін қамтамасыз ету үшін дискілердің мазмұнына күнделікті сақтық көшірме жасалады. Процесс тиісті бағдарламалық жасақтама мен жабдық болған кезде қосымша сақтық көшірме көмегімен автоматты түрде орындалады.

15.3 Резервтік көшіру процесін ұйымдастыруға, резервтік көшірмелерді сақтауға және ақпаратты қалпына келтіруге жауапкершілік ақпараттық жүйелердің әкімшілеріне және АТД уәкілетті қызметкерлеріне жүктеледі.

16 Ақпараттық қауіпсіздік аудиті

16.1 Ақпараттық қауіпсіздікті басқару жөніндегі ұйымның тәсілінің барабарлығы мен тиімділігіне сенімділікті қамтамасыз ету мақсатында ақпараттық қауіпсіздік аудиті тәртіппен және мерзімдерде жүргізілуі мүмкін.

16.2 Аудитті АҚ қамтамасыз етуге жауапты университеттің құрылымдық бөлімшесінің мамандары, сондай-ақ тиісті біліктілігі бар бөгде ұйымдардың сарапшылары орындай алады.

16.3 Аудит жүргізу мемлекеттік органның ақпараттандыру объектілерінің ақпараттық қауіпсіздігінің ағымдағы жай-күйін, оның осы Саясаттың мақсаттары мен міндеттеріне, ақпараттандыру саласындағы қолданыстағы заңнаманың, ақпараттық қауіпсіздік саласындағы халықаралық және мемлекеттік стандарттардың талаптарына сәйкестігін бағалауды жүзеге асыруға мүмкіндік береді.

16.4 Аудит бағдарламасы ақпараттандыру объектісін және оның компоненттерін аспаптық тексеруді қамтиды. Аспаптық тексеру мыналарды қамтуы мүмкін:

- АТ-инфрақұрылымы мен ақпараттық жүйелердің қорғалу аудиті;
- енуге тестілеу (желілік периметрдің қауіпсіздігін бағалау);
- осалдықтар үшін бағдарламалық кодты талдау;
- жүктемені тестілеу (өнімділікті бағалау).

16.5 Аудит нәтижелері қолданыстағы ақпараттық қауіпсіздік жүйесіндегі «әлсіз» жерлерді анықтауға және оны оңтайландыруға, қолданылатын қауіпсіздік шараларын жақсартуға ықпал етуі тиіс. Аудит нәтижелері тәуекелдерді талдау және бағалау үшін кіріс ретінде пайдаланылуы керек.

16.6 Жүргізілген аудит нәтижелері құжатталады және басшылықтың назарына жеткізіледі.

17 Саясат талаптарын бұзу

17.1 Университеттің ақпараттық қауіпсіздікті басқару жүйесі болашақта ұйым қызметкерлерінің мұндай бұзушылықтардың алдын алу үшін тежеуші фактор ретінде ақпараттық қауіпсіздік талаптарын бұзған кезде тәртіптік практиканы қолдануды көздейді.

17.2 Тәртіптік практика алдын ала тексерулерсіз, бұзушылықтар жасау мән-жайлары мен фактілерін нақтылаусыз қолданылмауға тиіс. Қызметкерлер немесе қызметкерлер тобы тарапынан бұзушылық фактісі анықталған жағдайда, ҚР заңнамасына сәйкес шаралар қолданылады.

18 Ішкі нормативтік құжаттаманы келісу, бекіту және қолданысқа енгізу

18.1 Ішкі нормативтік құжаттама тиісті облысқа жауапты бөлімше басшысымен және ұйым басшылығымен келісілуі тиіс. Егер нормативтік акт қаржылық мәселелерді қозғаса, оны келісу бас бухгалтермен жүргізіледі. Келісу құжаттың мазмұнына және олардың құзыреттеріне қарай айқындалған лауазымды адамдармен жүргізіледі. Құжатты келісу қажет тұлғалардың тізбесін айқындау үшін жауапкершілік құжатты әзірлеушіге жүктеледі.

18.2 Құжаттаманы қарау мерзімі алынған сәттен бастап бес жұмыс күнінен аспауға тиіс. Барлық ескертулер дәлелденіп, нақты түрде көрсетілуі керек.

18.3 Ескертулер болмаған жағдайда құжатқа тиісті лауазымды адамдар қол қояды және бекітуге беріледі.

18.4 Келісілгеннен кейін құжат ұйымның ресми ресурстарында одан әрі орналастыру үшін мемлекеттік және қажет болған жағдайда ағылшын тіліне аударылуға тиіс.

18.5 Әзірлеуші және Келісуші тұлғалар қол қойған құжат ұйымның басшысына немесе уәкілетті тұлғаға бекітуге беріледі.

18.6 Құжаттың қолданысқа енгізілген күні оның бекітілген күні болып есептеледі. Құжат бекітілген сәттен бастап күшіне енеді және орындау үшін міндетті болып табылады.

18.7 Бекітілген құжат мұрағатқа немесе Құжаттамалық сүйемелдеуге жауапты бөлімшеге ұйымның ішкі талаптарына байланысты қағаз және/немесе электрондық форматта сақтауға беріледі.

18.8 Жаңартылған немесе өзектендірілген құжат қолданысқа енгізілген кезде құжаттың алдыңғы нұсқасы күшін жояды және жарамсыз деп есептеледі.

19 Сақтау

19.1 Университеттің сайтында ішкі нормативтік құжаттаманың электрондық нұсқасын орналастырғаннан кейін орындаушылар онымен танысады және барлық құжаттар үшін міндетті болып табылатын танысу парағына өз қолтаңбаларын қояды. Кафедраларда және бөлімшелерде қызметкерлерді келіп түскен құжаттармен таныстыру үшін кафедра меңгерушісі және/немесе бөлімше басшысы жауап береді.

19.2 Құжатты көбейтуге, көшірмелерін есепке алуға, рұқсатсыз пайдалануға және сақтауға бөлімше басшысы жауапты болады.

19.3 Құжаттың толық электрондық нұсқасы электрондық түрде, ал титул парағы мен танысу парағы баспа түрінде сақталады.

20 АҚ Саясатын қайта қарау және өзектендіру тәртібі

20.1 Ақпараттық қауіпсіздік саясатын қайта қарау кемінде екі жылда бір рет жүргізіледі және Саясатта айқындалған қорғау шараларын нақты жағдайларға және ақпаратты қорғауға қойылатын ағымдағы талаптарға сәйкестендіруді көздейді.

20.2 Саясатқа жоспардан тыс өзгерістер енгізу АҚ инциденттерін талдау нәтижелері, АҚ-ны қамтамасыз етудің пайдаланылатын шараларының өзектілігі, жеткіліктілігі мен тиімділігі, АҚ-ның ішкі аудиттерін жүргізу нәтижелері және басқа да бақылау іс-шаралары бойынша жүргізілуі мүмкін.

20.3 Ережелер, нұсқаулықтар, техникалық талаптар және басқалар сияқты нақты регламенттеуші құжаттар осы Саясатқа қосымшалар түрінде ресімделеді.

Олар қажеттілігіне қарай әзірленеді және өзектендіріледі, Басқарма Төрағасы – ректордың немесе уәкілетті лауазымды адамның бұйрығымен бекітіледі және оларды басқарма деңгейінде бекіту қажеттілігінсіз негізгі саясат сияқты заңды күшке ие болады.

Ф.01-2022

Келісу парағы

Лауазымы	Аты-жөні	Күні	Қолы
Басқарма мүшесі - Стратегиялық даму және цифрландыру жөніндегі проректор	Т.Е. Канапьянов		
Заң бөлімінің бастығы	Г.С. Аязбаева		
ЭҚжБЕД директоры - бас бухгалтер	А.Х. Абильтусупова		
ӘЗД директоры	М.М. Кожухова		
АТД директор	Г.Д. Аубакиров		

Ф.02-2022

Танысу парағы

Лауазымы	Аты-жөні	Күні	Қолы