«Х.Досмұхамедов атындағы Атырау университеті» КеАҚ

БЕКІТЕМІН
Х. Досмұхамедов атындағы
Атырау университетінің
Басқарма төрағасы-ректор
_____ С.Н.Идрисов
«22» 09 2025 ж.

САЯСАТ

«Х.ДОСМҰХАМЕДОВ АТЫНДАҒЫ АТЫРАУ УНИВЕРСИТЕТІ» КЕАҚ
АҚПАРАТТЫҚ ҚАУІПСІЗДІК

№ 246

Атырау 2025 ж.

	Лауазымы	Т.А.Ә.	Қолы	Күні
Жасақтаған	Техникалық, IT қызмет көрсету және ақпараттық қауіпсіздікті қамтамасыз ету бөлімінің жетекшісі	А.И. Абилов		
Келісілді	Академиялық мәселелер жөніндегі проректор	А.Е. Чукуров		
	Вице проректор (цифрлық офицер)	Ж.О. Сулейменова		
	Сапа мониторингі кеңсесінің жетекшісі	Ж.Т. Кайшыгулова		
	Заңгер	К.С. Куанов		19.09.2025

Мазмұны

1 Жалпы ережелер және қолдану аясы

1.1 Осы «Х.Досмұхамедов атындағы Атырау университеті» КЕАҚ Ақпараттық қауіпсіздік саясаты (бұдан әрі – Саясат) «Х.Досмұхамедов атындағы Атырау университеті» КЕАҚ (бұдан әрі – Университет) ақпараттық қауіпсіздігін қамтамасыз ету саласындағы мақсаттарын, міндеттерін, жетекші қағидаттары мен практикалық әдістерін айқындайды.

1.2 Осы Саясатта ақпараттық қауіпсіздік Университеттің электрондық ақпараттық ресурстарын, ақпараттық жүйелерін, деректер қорын материалдық залал келтіруі, беделіне нұқсан келтіруі немесе Университетке, оның қызметкерлеріне және студенттеріне басқа да зиян келтіруі мүмкін сыртқы және ішкі қауіптерден қорғалу жағдайын білдіреді.

1.3 Саясат Университеттің нормативтік және анықтамалық құжаттамасының бөлігі болып табылады және Университеттің барлық қызметкерлері үшін міндетті болып табылады және сонымен қатар Университеттің ақпараттық жүйелері мен құжаттарына рұқсаты бар басқа үшінші тұлғаларға хабарланады.

1.4 «Х.Досмұхамедов атындағы Атырау университеті» КЕАҚ дербес деректер туралы заңнаманың сақталуын қамтамасыз ету үшін қажетті құқықтық, ұйымдастырушылық және техникалық шараларды қабылдайды немесе олардың қабылдануын қамтамасыз етеді.

2 Белгілер

Осы Саясатта келесі терминдер мен анықтамалар қолданылады:

- Қауіпсіздік мониторингі – ақпараттық қауіпсіздік оқиғаларын анықтау және анықтау үшін ақпараттық технология объектісін үздіксіз бақылау;
- аутентификация – құпия сөздерді немесе аутентификация мүмкіндіктерін (цифрлық сертификаттар, таңбалауыштар, смарт-карталар, бір реттік пароль генераторлары және биометриялық сәйкестендіру құралдары) генерациялау мен енгізуді қоса алғанда, әртүрлі параметрлердің тіркесімін пайдалана отырып, пайдаланушының түпнұсқалығын тексеру әдісі;
- кибершабуыл – компьютерлік жүйелерге, желілерге немесе құрылғыларға рұқсатсыз қол жеткізу, деректерді ұрлау, зақымдау немесе жою, жүйе жұмысын бұзу немесе қаржылық, беделге немесе басқа да зиян келтіруге бағытталған қасақана зиянды әрекет немесе әрекеттер жиынтығы;
- желіаралық қалқандар (немесе желіаралық қалқандар, желіаралық қалқандар) қалаусыз немесе зиянды желілік қосылымдарды блоктау және компьютерлік желілер мен құрылғыларды киберқауіптерден қорғау үшін желілік трафикті (деректерді) бақылайтын және сүзетін «цифрлық қабырға» рөлін атқаратын қауіпсіздік жүйелері;
- DDoS шабуылы (үлестірілген қызмет көрсетуден бас тарту шабуылы) – көбінесе желіге (ботнетке) қосылған бірнеше құрылғылар бір уақытта мақсатты серверге, қызметке немесе желіге сұраныстардың үлкен көлемін жіберетін кибершабуыл. Мұндай шабуылдың мақсаты - жүйе ресурстарын шамадан тыс жүктеу, оны тұрақты пайдаланушылар үшін қолжетімсіз ету және қызмет көрсетуден бас тарту;
- Вирус - бұл өз бетінше қайталанатын және басқа компьютерлерге тарайтын, сонымен қатар компьютердің жұмысын бұзатын, деректерге зақым келтіретін және пайдаланушының жеке мәліметтерін ұрлай алатын зиянды бағдарламалық құрал түрі;
- Зиянды бағдарламалық құрал (немесе зиянды бағдарлама) – компьютер жүйесіне зиян келтіру, жеке деректерді ұрлау, құрылғылардың жұмысын бұзу немесе оларға

рұқсатсыз кіру үшін әдейі жасалған кез келген бағдарламалық құрал. Зиянды бағдарламалық құралға вирустар, құрттар, трояндар, шпиондық бағдарламалар, төлемдік бағдарламалар және киберқауіптердің басқа түрлері кіреді.

3 Қысқартулар

АҚ – Ақпараттық қауіпсіздік
БҚ – бағдарламалық қамтылым
АЖ – Ақпараттық жүйе
АҚБЖ – Ақпараттық қауіпсіздікті басқару жүйесі
ҚББ – құрылымдық бөлімшенің басшысы
СМК – Сапа мониторингі кеңсесі

4 Нормативтік сілтемелер

Саясат келесі құжаттардың талаптары мен ұсыныстарына сәйкес әзірленді және рәсімдерді белгілейді:

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

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

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

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

4.5 ҚР СТ ISO/IEC 27005-2022. «Ақпараттық технология. Қауіпсіздікті қамтамасыз ету әдістері. Ақпараттық қауіпсіздік тәуекелдерін басқару»;

4.6 Қазақстан Республикасы Қаржы министрлігі Мемлекеттік мүлік және жекешелендіру комитеті төрағасының 2020 жылғы 5 маусымдағы №350 бұйрығымен бекітілген «Х.Досмұхамедов атындағы Атырау университеті» КЕАҚ жарғысы;

5 АҚ міндеттері мен функциялары

5.1 Осы Саясат Университеттің электрондық ақпараттық ресурстарын, ақпараттық жүйелерін және деректер базасын рұқсатсыз кіруден, пайдаланудан, ашудан, бұрмалаудан, өзгертуден немесе жоюдан қорғауға бағытталған ұйымдастырушылық және техникалық шаралар кешенін жүзеге асыру мақсатында әзірленген.

5.2 Университетте АҚ қамтамасыз ету міндеттеріне ақпараттық және желілік инфрақұрылымды қорғауды қамтамасыз етуге бағытталған кең ауқымды іс-шаралар мен әрекеттер кіреді:

- Мәліметтердің құпиялылығын қорғау: электрондық ақпараттық ресурстарды, ақпараттық жүйелерді, университеттің дерекқорларын, қызметкерлер мен студенттердің жеке деректерін, қаржылық ақпаратты, зерттеулерді және басқа да құпия деректерді зиянкестердің заңсыз әрекеттерінен, ықтимал қауіптерден, рұқсатсыз қол жеткізуден, ағып кетуден немесе ұрлықтан қорғау. Университеттің тұтынушыларымен және серіктестерімен өзара әрекеттесу кезінде кез келген нысанда берілетін ақпараттың құпиялылығын сақтау;
- Деректердің тұтастығын қамтамасыз ету: тұтастығын қамтамасыз ету және университеттің электрондық ақпараттық ресурстарына, ақпараттық жүйелеріне және деректер қорларына рұқсат етілмеген өзгертулерді немесе зақымдануларды болдырмау;

- Деректердің қолжетімділігін қамтамасыз ету: Университеттің оқу және әкімшілік процестерінің үздіксіздігін қамтамасыз ету үшін қажетті дәрежеде уәкілетті пайдаланушылар үшін Университеттің ақпараттық жүйесіне қол жеткізуді қамтамасыз ету;
- Қолжетімділікті басқару: пайдаланушының рөлдері мен артықшылықтары негізінде университеттің аппараттық құралдарына, бағдарламалық қамтамасыз етуіне, ақпараттық жүйелеріне және ақпараттық ресурстарына қызметкерлердің қол жеткізуін шектеу;
- Деректердің сақтық көшірмесін жасау және қалпына келтіру жүйесін жетілдіру: маңызды ақпараттық ресурстар мен дерекқорларды сенімді қорғауды және жылдам қалпына келтіруді қамтамасыз ету үшін деректердің сақтық көшірмесін жасау және қалпына келтіру жүйесін жаңарту;
- Зиянды бағдарламалар мен қауіптерден қорғау: DDoS шабуылдары, вирустар, зиянды бағдарламалар және басқа да ақпараттық қауіпсіздік қатерлері сияқты кибершабуылдардың әсерін болдырмау және азайту. Заманауи қауіпсіздік құралдарын орнатуды және конфигурациялауды (брандмауэрлер, шабуылдарды анықтау жүйелері, антивирустық шешімдер, СКУД жүйелері және т.б.) қоса алғанда, АҚБЖ инфрақұрылымын дамыту;
- Аппараттық құралдарды жаңарту: ескірген жабдықты (серверлер, желілік құрылғылар, деректерді сақтау) қауіпсіздік мүмкіндіктері жақсартылған заманауи үлгілерге ауыстыру;
- Бағдарламалық құралды жаңарту: операциялық жүйелерді, дерекқорларды, антивирустық бағдарламаларды және басқа бағдарламалық құралдарды соңғы қауіпсіздік жаңартуларымен ағымдағы нұсқаларға жаңарту;
- Оқиғаларды басқару жүйесін жетілдіру: нақты уақытта қауіпсіздік оқиғаларын жинауға, талдауға және жауап беруге мүмкіндік беретін процестерді және қауіпсіздік оқиғаларын басқару жүйесін (SIEM) әзірлеу;
- Заңдар мен нормативтік құқықтық актілерді сақтау: Ақпараттық қауіпсіздік саласындағы Қазақстан Республикасының заңнамалық және нормативтік құқықтық актілерінің талаптарын сақтау, ақпараттық қауіпсіздік пен дербес деректерді қорғаудың нормативтік құқықтық базасын дамыту және жетілдіру. Қамтамасыз ету;
- Тренинг және ақпараттандыру: университет қызметкерлерінің ақпараттық қауіпсіздік әдістері мен желідегі қауіпсіздік ережелері туралы хабардарлығын арттыру. Ақпараттық қауіпсіздік бойынша IT мамандары мен әкімшілерін оқыту және сертификаттау курстарын өткізу.
- Оқиғаға әрекет ету: ақпараттық қауіпсіздік инциденттеріне әрекет ету жөніндегі нұсқаулықтарды әзірлеу және енгізу. Дағдарыс (төтенше) жағдайларға байланысты шығындарды азайту және бағдарламалық қамтамасыз етуді, аппараттық құралдарды және ақпаратты қалпына келтіру. Мұндай жағдайлардың себептерін зерттеп, алдағы уақытта олардың алдын алу шараларын қабылдау.
- Тәуекелдерді басқару: қауіпті ортаның өзгеруін ескере отырып, ақпараттық қауіпсіздік тәуекелдерін бағалау және басқару. Тәуекелдерді азайту және жазатайым оқиғалардан, университет қызметкерлерінің байқаусызда жіберген қателерінен және техникалық ақаулардан болатын ықтимал шығынды азайту.
- Қауіпсіздік мониторингі: ықтимал оқиғалар мен шабуылдарды ерте анықтау үшін қауіпсіздік оқиғаларын бақылау. Ақпараттық қауіпсіздікті қамтамасыз ету үшін қолданылатын техникалық жабдықтар мен инфрақұрылымның ағымдағы жағдайын бағалау. Ескірген немесе жеткіліксіз құрамдастарды анықтау.

6 АҚ принциптері

6.1 Университеттің Ақпараттық қауіпсіздік қағидаттары ақпаратты әртүрлі қауіптерден қорғауды қамтамасыз ету үшін ұстануға тиіс негізгі нұсқаулар мен тәсілдерді білдіреді:

6.2 Тұтастық: Бұл принцип ақпараттың дәлдігін, тұтастығын және толықтығын қамтамасыз етуді қамтиды. Ақпарат оның дұрыстығына немесе сенімділігіне әсер ететін рұқсат етілмеген өзгертулерден немесе модификациялардан қорғалуы керек.

6.3 Құпиялылық: Құпиялылық принципі құпия ақпаратқа қол жеткізу олардың қызметтік міндеттерін немесе тапсырмаларын орындау үшін қажет рұқсаты бар пайдаланушыларға ғана берілуін талап етеді. Ақпаратқа рұқсатсыз қол жеткізуден қорғау құпиялылықты қамтамасыз етуде басты рөл атқарады.

6.4 Қол жетімділік: Қол жетімділік принципі ақпарат пен қатысты жүйелердің рұқсат етілген пайдаланушыларға қажетті уақытта және жерде қол жетімді болуын қамтамасыз етеді.

6.5 Аутентификация: Аутентификация принципі ақпаратқа немесе ресурстарға қол жеткізуге әрекеттенетін пайдаланушылардың, құрылғылардың немесе жүйелердің жеке басын тексеруді қамтиды. Бұған құпия сөздерді, сандық қолтаңбаларды және пайдаланушыларды анықтаудың басқа әдістерін пайдалану кіреді.

6.6 Авторизация: Авторизация принципі уәкілетті пайдаланушылардың белгілі бір ресурстар мен деректерге қол жеткізу құқықтары мен артықшылықтарын анықтайды.

6.7 Қызмет көрсетуден бас тартпау: Қызмет көрсетуден бас тартпау принципі жіберуші немесе алушы хабарламаны немесе деректерді жіберуден немесе қабылдаудан бас тарта алмайтындығына кепілдік береді. Бұған аутентификацияны қолдану арқылы қол жеткізіледі.

6.8 Міндеттерді бөлу: Міндеттерді бөлу принципі негізгі функцияларды әртүрлі қызметкерлер немесе топтар арасында бөлу арқылы жүйелік артықшылықтарды теріс пайдалануды болдырмауға бағытталған.

6.9 Деректерді бөлу: Деректерді бөлу принципі құпия деректердің құпия емес немесе жалпыға ортақ деректерден бөлінуін қамтамасыз етеді, бұл ақпараттың ағып кету қаупін азайтуға көмектеседі.

6.10 Жеке жауапкершілік: осы қағидаға сәйкес қызметкерлердің құқықтары мен міндеттерін бөлу қандай да бір бұзушылық болған жағдайда кінәлілер шеңбері анық белгілі болатындай немесе минимумға дейін төмендетілетіндей құрылымдалу керек.

6.11 Заңдылығы: Қазақстан Республикасының ақпараттық қауіпсіздік саласындағы заңнамасының талаптарын сақтау.

7 АҚ практикалық әдістері

7.1 Ақпараттық қауіпсіздік тәжірибесі ақпаратты, деректер қорын және ақпараттық жүйелерді әртүрлі қауіптерден қорғауда маңызды рөл атқарады. Университетте қолданылатын негізгі тәжірибелерге мыналар жатады:

- Пайдаланушыларды оқыту және хабардар болу: пайдаланушыларды желідегі қауіпсіздік негіздеріне, фишингтік шабуылдарға, құпия сөзді қорғауға және т.б.
- Қолжетімділікті басқару: Университеттің электрондық ақпараттық ресурстары мен АЖ-нің рұқсат етілген пайдаланушыларына қол жеткізу құқықтарын анықтау және рөлдерді беру;
- Бағдарламалық құралды жаңарту: операциялық жүйелерді, қолданбалы бағдарламалық құралды және антивирустық бағдарламалық құралды соңғы

нұсқаларға үнемі жаңарту. Белгілі осалдықтарды жабу үшін қауіпсіздік патчтарын орнату;

- Деректерді шифрлау: сақтау және желі арқылы беру кезінде деректерді шифрлау. Құпиялық деректерді қорғау үшін дискі мен файлды шифрлауды енгізу;
- Деректердің сақтық көшірмесін жасау: деректердің сақтық көшірмесін жүйелі түрде жасау және оларды қауіпсіз жерлерде сақтау;
- Бақылау және оқиғаларды тіркеу: аномалиялар мен ықтимал қауіпсіздік инциденттерін анықтау үшін қауіпсіздік мониторингі жүйесін пайдалану. Қауіптерге жылдам әрекет ету үшін оқиғаларды талдау және тіркеу;
- Физикалық қауіпсіздік: сервер бөлмелерінің физикалық қауіпсіздігін қамтамасыз ету. Университетте қолжетімділікті бақылау және бейнебақылау жүйелерін қолдану;
- Зиянды бағдарламалар мен кибершабуылдардан қорғау: Барлық компьютерлер мен серверлерде антивирустық бағдарламалық қамтамасыз етуді және желіаралық қалқандарды орнату;
- Қауіпсіздік мониторингі: Университеттің электрондық ақпараттық ресурстарын, ақпараттық жүйелерін және деректер қорын қауіпсіз пайдалануды бақылауға бағытталған ұйымдастырушылық-техникалық шаралар;
- Нормативтік талаптарға сәйкестік: Қазақстан Республикасының заңнамасымен және Университеттің ішкі құжаттарымен белгіленген деректерді қорғаудың барлық талаптарын сақтау.

8 Құқықтар мен міндеттер

8.1 Барлық қызметкерлерден Университеттің ақпараттық ресурстарын сауатты, тиімді және әдепті түрде пайдалану талап етіледі;

8.2 Университет басшылығы ақпараттық қауіпсіздік саясатын іске асыру үшін қажетті ресурстарды, оның ішінде кадрларды даярлауды қаржыландыруды, АҚ қамтамасыз ету үшін қажетті технологиялар мен қорғау құралдарын енгізуді қамтамасыз етеді;

8.3 Құрылымдық бөлімшелердің басшылары қызметкерлерді АҚ саясатымен таныстыруға дербес жауапты болады және ақпараттық қауіпсіздік талаптарының бұзылуына байланысты барлық оқиғалар мен күдікті жағдайлар туралы университеттің ақпараттық қауіпсіздікке жауапты қызметкеріне дереу хабарлауға міндетті;

8.4 Қауіпсіздік саясатын жүзеге асыру және қолдау – басшылықтан бастап ақпараттық жүйелерді пайдаланушыларға дейін университеттің барлық мүдделі тараптарының бірлескен күш-жігері. Бұл деректердің ағып кетуі мен қауіпсіздікті бұзу қаупін азайтуға көмектеседі және университеттің құнды ақпаратының қорғалуын қамтамасыз етеді.

8.5 Ақпараттық қауіпсіздік саласындағы жергілікті нормативтік құқықтық актілерді бұзғаны үшін жауапкершілік дәрежесі әрбір нақты жағдайда айқындалады.

9 Қорытынды ережелер

9.1 Бұл Саясат университеттің басқарма төрағасы – ректоры бекіткен кезден бастап күшіне енеді.

9.2 Саясат және оған енгізілетін өзгерістер «Х.Досмұхамедов атындағы Атырау университеті» ҚЕАҚ Басқарма төрағасы – ректорының бұйрығымен бекітіледі.

9.3 Басшы бекітілген Саясаттың көшірмесін бөлім қызметкерлеріне хабарлайды, олар Танысу парағына қол қоюы керек.

Университетке жұмысқа қабылданғанда немесе басқа қызметке ауысқан кезде басшы мен қызметкерлер осы Саясатпен танысуы керек.

10 Өзгерістер енгізу тәртібі

10.1 Осы Саясат жеке деректер субъектілеріне және басқаларға алдын ала ескертусіз өзгертілуі мүмкін. Саясаттың ағымдағы нұсқасы https://atyrau.edu.kz мекенжайы бойынша «Х.Досмұхамедов атындағы Атырау университеті» ҚЕАҚ корпоративтік веб-сайтында (порталында) орналастырылған.

10.2 Саясат қажеттілігіне қарай қайта қаралады. Түпнұсқа және көшірмелеріне өзгерістер мен толықтырулар енгізу үшін ҚББ жауапкершілікті өз мойнына алады.

10.3 Саясатқа өзгертулер мен толықтыруларды әзірлеуші жаңа құжатты әзірлеу және оқу ісі жөніндегі проректордың рұқсатымен белгіленген тәртіппен келісу және бекіту жолымен енгізеді және оның қолымен ресімделеді.

10.4 Саясат бекітілгеннен кейін әзірлеуші түпнұсқа көшірмені тіркеу және сақтау үшін СМК-ға береді. СМК-ға беру және ескірген және жарамсыз Саясатты қайта қарау ҚББ жауапкершілігін өз мойнына алады.

10.5 Саясаттың жаңа редакциясын бекіту жоғарыда аталған, күші жойылған құжаттарды кері қайтарып алу үшін негіз болып табылады.

10.6 СМК-да қолданылу мерзімі өтіп кеткен құжаттарды ауыстыруды бөлім басшысы – Саясатты әзірлеуші жүзеге асырады.

10.7 Саясатқа өзгерістер мен толықтырулар енгізу үшін мыналар негіз бола алады:

- заң күші бар нормативтік құқықтық актілерге жаңадан енгізілген өзгерістер мен толықтырулар;
- Басқарма төрағасы-ректордың бұйрықтары;
- құрылымдық бөлімшелер арасындағы жауапкершілікті қайта бөлу;
- құрылымдық бөлімшелерді қайта құру;
- ұйымның немесе құрылымдық бөлімшенің атауы өзгерген кезде.

КЕЛІСУ ПАРАҒЫ

№ п/п	Қызметкердің ТАӘ	Лауазымы	Танысу күні	Қызметкердің қолы

ӨЗГЕРТУЛЕР МЕН ҚОСЫМШАЛАРДЫ ТІРКЕУ ПАРАҒЫ

№ п/п	Құжат бөлімінің, тармағының, тармақшасының №	Өзгеріс енгізу күні	Негіздеме (Бұйрық №, күні)	Өзгеріс енгізілген күн	Өзгерісті енгізген тұлғаның қолы