«Ахмет Байтұрсынұлы
атындағы Қостанай
өңірлік университеті»
КЕАҚ

BU
BAITURSYNULY
UNIVERSITY

Бекітемін
Басқарма Төрағасы – Ректор
_____ С. Қуанышбаев
«16» 12 2025 ж.

ҚАҒИДАЛАР

АҚПАРАТТЫҚ ҚАУІПСІЗДІК ТӘУЕКЕЛДЕРІН БАҒАЛАУ ӘДІСТЕМЕСІ

Қ 128-2025

Қостанай

Алғы сөз

1 Бағдарламалық қамтамасыз етуді әзірлеу және сүйемелдеу бөлімімен **ӘЗІРЛЕНДІ**

2 Бағдарламалық қамтамасыз етуді әзірлеу және сүйемелдеу бөлімімен **ЕНГІЗІЛДІ**

3 Басқарма Төрағасы-Ректордың 26.12.2025 жылғы № 357 НҚ бұйрығымен **БЕКІТІЛДІ ЖӘНЕ ҚОЛДАНЫСҚА ЕНГІЗІЛДІ**

4 ӘЗІРЛЕУШІ:
В. Гриднева – бағдарламалық қамтамасыз етуді әзірлеу және сүйемелдеу бөлімінің бастығы;

5 САРАПШЫЛАР:
В. Петрович – қаржы-экономикалық қызметінің бастығы;
А. Шмит – техникалық қамтамасыз ету бөлімінің бастығы.

6 ТЕКСЕРУ КЕЗЕҢДІЛІГІ 3 жыл

7 АЛҒАШ РЕТ ЕНГІЗІЛДІ

Мазмұны

1-тарау. Жалпы ережелер

1. Осы Қағидалар «Ақпараттық қауіпсіздік тәуекелдерін бағалау әдістемесі» (бұдан әрі – Әдістеме) «Ахмет Байтұрсынұлы атындағы Қостанай өңірлік университеті» КЕАҚ-та (бұдан әрі – Университет) Университеттің ақпараттық және олармен байланысты активтеріне әсер ететін тәуекелдерді талдау және бағалау тәртібін белгілейді.

2. Әдістеменің мақсаты – ақпаратты және онымен байланысты активтерді қорғауды қамтамасыз ету, олардың құпиялылығын, тұтастығы мен қолжетімділігін сақтау, сондай-ақ қатерлердің іске асуының білім беру, әкімшілік процестерге және Университеттің беделіне ықпалын барынша азайту үшін Университеттің ақпараттық қауіпсіздік тәуекелдерін бағалау.

3. Ақпараттық қауіпсіздік тәуекелдерін талдау қатерлер мен осалдықтардың түрлерін анықтау, олардың ықтималдығы мен салдарын бағалау, Университет активтерін қорғаудың тиімді жүйесін құру және тәуекелдерді төмендету жөніндегі қажетті іс-шараларды жоспарлау үшін қажет.

4. Тәуекелдерді талдау нәтижелері тәуекелдерді өңдеу жоспарларын қалыптастыру, қорғау шараларын түзету және Университеттің ықтимал оқыс оқиғаларға жалпы орнықтылығын арттыру үшін пайдаланылады.

5. Қағидалар Университеттің нормативтік-анықтамалық құжаттамасының құрамына кіреді, Университеттің барлық қызметкерлері үшін міндетті болып табылады, сондай-ақ Университеттің ақпараттық жүйелері мен құжаттарына қол жеткізе алатын өзге де үшінші тұлғалардың назарына жеткізіледі.

2-тарау. Нормативтік сілтемелер

5. Әдістеме мынадай құжаттардың талаптары мен ұсынымдарына сәйкес әзірленді және рәсімдерді белгілейді:

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

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

3) «Ақпараттандыру объектілерін сыныптау қағидаларын және ақпараттандыру объектілерінің сыныптауышын бекіту туралы» Қазақстан Республикасы Инвестициялар және даму министрінің міндетін атқарушының 2016 жылғы 28 қаңтардағы № 135 бұйрығы;

4) Қазақстан Республикасы Қаржы министрлігі Мемлекеттік мүлік және жекешелендіру комитеті төрағасының 2020 жылғы 05 маусымдағы № 350 бұйрығымен бекітілген, 03.10.2023 ж. өзгерістерімен «Ахмет Байтұрсынұлы атындағы Қостанай өңірлік университеті» КЕАҚ Жарғысы;

5) ҰС 002-2025 Ұйым стандарты. Іс қағаздарын жүргізу;

6) ҚП 001-2025 Құжатталған процедура. Құжаттаманы басқару;

7) Қ 054-2024 «Ахмет Байтұрсынұлы атындағы Қостанай өңірлік университеті» КЕАҚ ақпараттық қауіпсіздік саясаты;

8) Е 127-2025 «Ахмет Байтұрсынұлы атындағы Қостанай өңірлік университеті» КЕАҚ ақпаратты өңдеу құралдарымен байланысты активтерді сәйкестендіру, сыныптау және таңбалау қағидалары.

3-тарау. Терминдер мен анықтамалар

6. Осы Әдістемеде мынадай терминдер мен анықтамалар қолданылады:

1) Ақпараттық қауіпсіздік оқыс оқиғасы – ақпараттық-коммуникациялық инфрақұрылымның немесе оның объектілерінің жұмысындағы, олардың жұмыс істеуіне қатер төндіретін және/немесе ақпаратты заңсыз алуға, көшіруге, таратуға, өзгертуге, жоюға не бұғаттауға жағдай жасайтын жеке немесе сериялы түрде туындайтын іркіліс.

2) Ақпараттық қауіпсіздік тәуекелі (R) – қатер іске асқан жағдайда ақпаратты өңдеу құралдарымен байланысты активтерге залал келтіру мүмкіндігі.

3) Ақпараттық қауіпсіздік қатері – ақпараттық қауіпсіздік оқыс оқиғасының туындауына алғышарттар жасайтын жағдайлар мен факторлардың жиынтығы.

4) Актив құндылығы (Si) – осы актив өңдейтін немесе қамтамасыз ететін ақпараттың құпиялылығы, тұтастығы және қолжетімділігі бұзылған жағдайда ықтимал залалды көрсететін, университет қызметі үшін АТ активінің маңыздылығын интегралды бағалау.

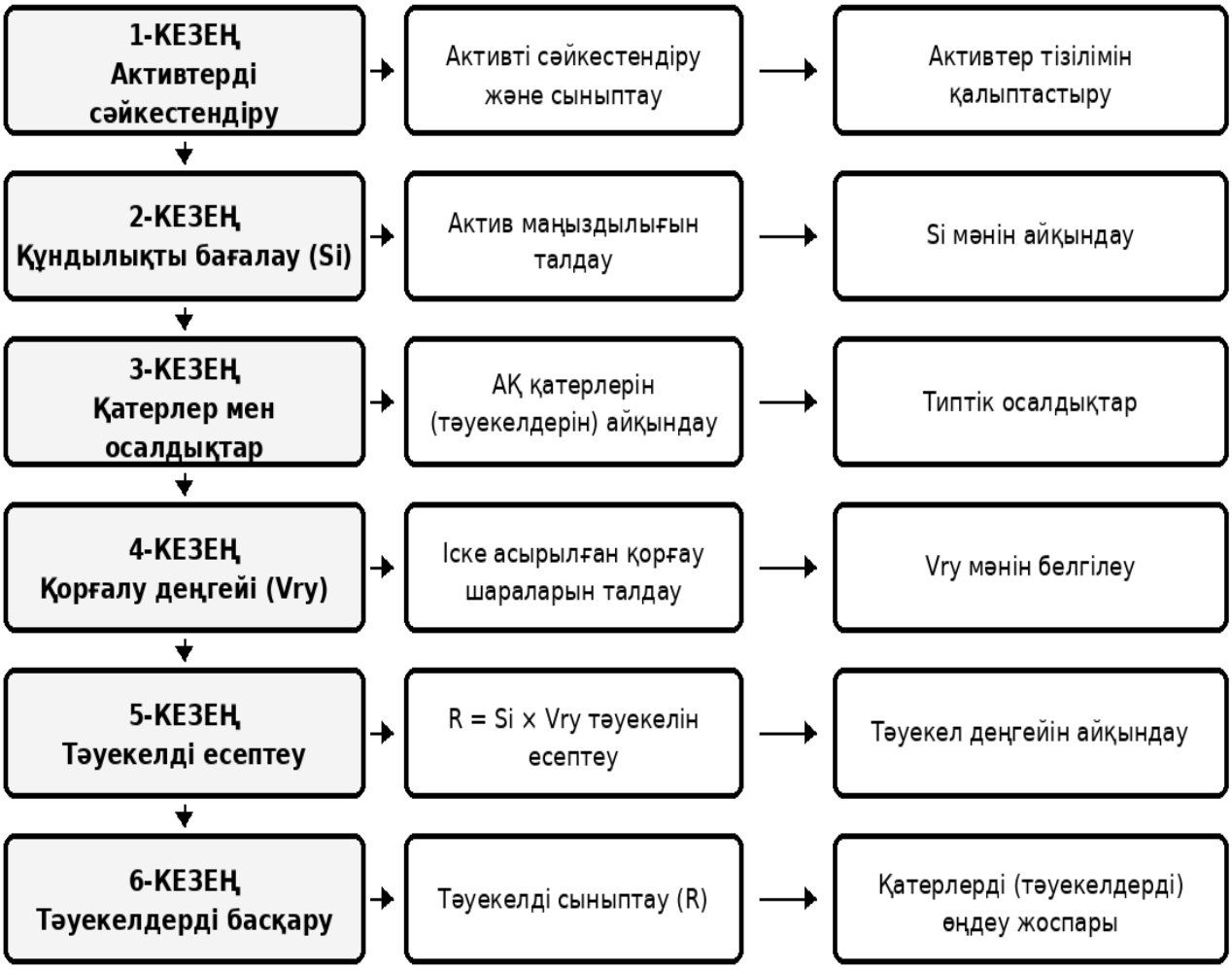
5) Қатердің іске асу ықтималдығы (Vry) – қорғау құралдарының болуы, толықтығы және тиімділігі ескеріле отырып, қатердің табысты іске асу ықтималдығының шартты балдық бағасы.

6) Осалдық – ақпаратты өңдеу құралдарымен байланысты активтің кемшілігі, оны пайдалану ақпараттың тұтастығының, құпиялылығының немесе қолжетімділігінің бұзылуына әкелуі мүмкін.

4-тарау. Тәуекелдерді талдау кезеңдері

Университеттің ақпараттық қауіпсіздік (бұдан әрі – АҚ) тәуекелдерін бағалау алгоритмі бірнеше кезеңнен тұрады (1-сурет):

- актив түрін айқындау;
- активтердің құндылығын айқындау – Si;
- қатерлерді және оларға сәйкес осалдықтарды айқындау, қатерлердің іске асу ықтималдығын бағалау;
- ақпараттық қауіпсіздік тәуекелін айқындау;
- АҚ тәуекелін төмендету жөніндегі жоспарларды қалыптастыру.



1-сурет. Ақпараттық қауіпсіздік тәуекелдерін бағалау схемасы

5-тарау. Актив түрін айқындау

7. Университеттің АҚ тәуекелдерін талдаудың бірінші кезеңінде ақпаратты өңдеу құралдарымен байланысты активтің түрі (бұдан әрі – Актив) айқындалады.

8. Активтерді айқындау және сыныптау «Ахмет Байтұрсынұлы атындағы Қостанай өңірлік университеті» КЕАҚ-тың ақпаратты өңдеу құралдарымен байланысты активтерді сәйкестендіру, сыныптау және таңбалау қағидаларына сәйкес жүзеге асырылады.

9. Тәуекелдерді талдау шеңберінде активтердің мынадай түрлері пайдаланылады:

− материалдық активтер – материалдық нысаны бар серверлік, желілік, компьютерлік және өзге де жабдық;

− материалдық емес активтер – университет үшін құндылығы бар және ақпаратты өңдеу, сақтау және беру үшін пайдаланылатын ақпараттық активтер (дерекқорлар, электрондық каталогтар, қызметтік ақпарат) және бағдарламалық қамтамасыз ету активтері (операциялық жүйелер, қолданбалы және лицензиялық БҚ).

10. Техникалық қамтамасыз ету бөлімінің және бағдарламалық қамтамасыз етуді әзірлеу және сүйемелдеу бөлімінің қызметкерлері жыл сайын 1-кестеге сәйкес активтер тізілімін жасайды.

1-кесте. Университет активтерінің тізілімі (толтыру үлгісімен)

№	Активтің / активтер тобының атауы	Актив түрі	Саны	Актив сыныбы	Қолжетімділік деңгейі
1	2	3	4	5	6
1	Антивирустық бағдарлама	БҚ активі	1	3 класс	Шектеулі
2	Ноутбук	Физикалық актив	200	3 класс	Шектеулі
4	ААЖ сервері	Физикалық актив	1	2 класс	Шектеулі

11. Активтер тізбесі және олардың сыныпталуы туралы мәліметтер көрсетілген ақпаратты өңдеу құралдарымен байланысты активтерді сәйкестендіру, сыныптау және таңбалау қағидаларында белгіленген мерзімдер мен тәртіпте өзектендірілуге жатады және ақпараттық қауіпсіздік тәуекелдерін бағалауды жүргізу үшін бастапқы деректер болып табылады.

12. Активтердің құндылығын бағалау (Si) 1-ден 10-ға дейінгі он балдық шкала бойынша жүзеге асырылады және активтің университет қызметі үшін маңыздылық дәрежесін көрсетеді (2-кесте). Si мәні актив сыныбын, өңделетін деректер санатын және ықтимал залалды ескере отырып айқындалады.

2-кесте. Активтердің құндылығын бағалау шкаласы (Si)

Si мәні	Құндылық деңгейі	Түсіндірме	Мысалдар
1	2	3	4
1–2	Өте төмен	Актив жалпыға қолжетімді ақпаратты қамтиды; АҚ бұзылуы залал келтірмейді	Сайттың ашық беттері, жарнамалық материалдар, ескі немесе пайдаланылмайтын ДК және периферия; сайттың уақытша қолжетімсіздігі (сервердің істен шығуы, DDoS)
3–4	Төмен	Актив қосалқы міндеттер үшін пайдаланылады; іркілістер негізгі процестерге әсер етпейді	Жалпы пайдаланылатын компьютерлік техника; негізгі процестерге қатыспайтын қосалқы құжаттар мен файлдардың жоғалуы
5–6	Орташа	Актив жұмыс процестеріне қатысады; іркілістер уақытша қолайсыздықтар туғызуы мүмкін, деректер жоғалмайды	ДД жоқ университет оқытушылары мен қызметкерлерінің жұмыс станциялары; қосалқы сервистер серверлері, жергілікті желі; деректер жоғалмайтын, оңай қалпына келтірілетін іркілістер

Si мәні	Құндылық деңгейі	Түсіндірме	Мысалдар
1	2	3	4
7–8	Жоғары	АҚ бұзылуы құпия ақпараттың немесе ДД-ның әшкереленуіне, университет процестері немесе беделі үшін елеулі салдарға әкелуі мүмкін, бұл ретте университеттің критикалық функциялары сақталады	Студенттер мен қызметкерлердің ДД-сы бар қызметкерлердің жұмыс станциялары; құпия ақпараты бар дерекқор серверлері; деректер жоғалмайтын негізгі АЖ уақытша іркілістері
9-10	Критикалық	АҚ бұзылуы университет қызметінің елеулі тоқтауына немесе физикалық инфрақұрылым мен резервтік көшірмелерді қоса алғанда, критикалық активтердің бүлінуіне/жоғалуына әкеледі.	Өрт, сервер бөлмесінің су басуы, серверлер мен резервтердің толық жоғалуы; АТ-инфрақұрылымның физикалық бұзылуы

Ескертпе: ДД — университеттің білім алушылары мен қызметкерлерінің дербес деректері.

13. Жыл сайын активтердің жалпы тізілімі және активтердің құндылығын бағалау шкаласы (Si) негізінде 3-кестеге сәйкес әрбір активтің маңыздылық дәрежесі бағаланады.

3-кесте. Активтердің маңыздылық дәрежесін балдық жүйе бойынша бағалау (толтыру үлгісімен)

№	АТ активі	Актив түрі	Құндылықтың негіздемесі	Si
1	2	3	4	5
1	АЖ дерекқор серверлері	Материалдық	Оқу және қызметтік деректерді, оның ішінде резервтік көшірмелерді сақтау	8
2	Электрондық құжат айналымы жүйесі	Материалдық емес	Білім беру және басқару процестерін қамтамасыз ету	6
3	Жергілікті есептеу желісі	Материалдық	АЖ мен сервистерге қолжетімділікті қамтамасыз етеді	5
4	ДД бар қызметкерлердің жұмыс станциялары	Материалдық	Дербес және құпия деректермен жұмыс;	7
5	Серверлік инфрақұрылым (физикалық серверлер, резервтік жүйелер)	Материалдық	Критикалық активтер; авария, өрт немесе апат салдарынан жоғалуы университет жұмысын тоқтатады	10

6-тарау. Қатерлерді және оларға сәйкес осалдықтарды айқындау

14. АҚ-ны қамтамасыз етуге жауапты қызметкерлер жыл сайын Университеттің АҚ қатерлері (тәуекелдері) каталогын және А қосымшасына сәйкес типтік осалдықтар анықтамалығын қалыптастырады.

15. АҚ тәуекелдерін бағалау кезінде қатердің болуы бағаланбайтыны ескеріледі, өйткені кез келген қатер өзінің табиғаты бойынша ықтимал болып табылады. Әрбір қатер бойынша қолданыстағы қорғау шараларын ескере отырып, оның іске асуының қалдық ықтималдығы бағаланады – осылайша қатердің іске асуының қалдық ықтималдығы айқындалады.

16. АҚ қатерлерінің іске асуының қалдық ықтималдығын нақты енгізілген қорғау шараларын ескере отырып айқындау мақсатында қорғалу деңгейінің шартты балдық бағасы (Vry) пайдаланылады.

17. Vry мәні 4-кестеде келтірілген қорғау құралдарымен қамтамасыз етілу деңгейін бағалау шкаласына сәйкес активтің қорғау құралдарымен қамтамасыз етілу дәрежесі негізінде айқындалады.

4-кесте. Қорғау құралдарымен қамтамасыз етілу деңгейін бағалау шкаласы (Vry)

Қорғау құралдарымен қамтамасыз етілу деңгейі	Vry мәні
Барлық қажетті қорғау құралдары енгізілген және жұмыс істейді	Vry = 0
Қажетті қорғау құралдарының 50%-ы болған жағдайда	Vry = 5
Қажетті қорғау құралдарының 80%-дан астамы жоқ	Vry = 10

18. Әрбір актив бойынша әрбір қатер үшін тиісті осалдықтарды (ұйымдастырушылық, техникалық, бағдарламалық, физикалық) жоюға бағытталған нақты іске асырылған қорғау шараларына талдау жүргізіледі.

19. Талдау нәтижелері бойынша активтің қорғау құралдарымен қамтамасыз етілу дәрежесі айқындалады және Vry мәні белгіленеді.

20. Әрбір актив және тиісті қатерлер бойынша қорғау құралдарымен қамтамасыз етілу дәрежесін бағалау нәтижелері мен Vry мәндері №5 жиынтық кесте түрінде ресімделеді.

5-кесте. Активтер мен қатерлер бойынша Vry бағалаудың жиынтық кестесі (толтыру үлгісімен)

№	Актив	Қатер	Іске асырылған қорғау шаралары	Қамтамасыз етілу бағасы	**Vry**
1	Қызметкерлердің жұмыс станциялары	Зиянды БҚ	Антивирустық қорғау, ОЖ мен БҚ-ны тұрақты жаңарту	100 % қамтамасыз етілу	**0**
2	Университеттің веб-ресурстары	DDoS-шабуылдар	Провайдердің базалық шаралары, мамандандырылған қорғаудың болмауы	50 % қамтамасыз етілу	**5**

7-тарау. Ақпараттық қауіпсіздік тәуекелін айқындау

21. АҚ тәуекелін айқындау актив құндылығы мен қатердің іске асу ықтималдығының көбейтіндісі негізінде мына формула бойынша жүзеге асырылады:

$$R = Si \times Vry.$$

мұндағы:

- Si - АТ активінің құндылығы;
- Vry - енгізілген қорғау шараларын ескере отырып, қатердің іске асу ықтималдығының шартты балдық бағасы;
- R - ақпараттық қауіпсіздік тәуекелінің деңгейі.

22. АҚ тәуекелі мәнін есептеу бұрын айқындалған Si және Vry мәндерінің негізінде «актив – қатер» әрбір үйлесімі үшін жүргізіледі. Тәуекел деңгейін есептеу нәтижелері 6-кестеге сәйкес АҚ тәуекелін бағалау нәтижелері түрінде ресімделеді.

6-кесте. АҚ тәуекелін бағалау нәтижелері (толтыру үлгісімен)

Актив	Қатер	Si	Vry	R	Тәуекел деңгейі
ДҚ серверлері	Зиянды БҚ (ransomware)	9	6	54	Орташа
Жұмыс станциялары	Фишинг	6	5	30	Бірқалыпты

23. Тәуекелдерді басқарудың басымдылығын айқындау және басқарушылық шешімдерді таңдау үшін R мәніне байланысты АҚ тәуекелі деңгейін түсіндіру шкаласы қолданылады (7-кесте).

7-кесте. АҚ тәуекелі деңгейін түсіндіру шкаласы (R)

R мәні	Тәуекел деңгейі	Тәуекел сипаттамасы	Тәуекелді төмендету жоспары
0–10	Төмен	Университет қызметіне елеулі әсер етпейтін мардымсыз тәуекел	Рұқсат етілетін тәуекел, ағымдағы қызмет шеңберінде бақылау
11–30	Бірқалыпты	Қатер іске асқан кезде тәуекел процестердің жергілікті бұзылуына әкелуі мүмкін	Бақылау, жағдайлар өзгерген кезде шараларды жоспарлау
31–60	Орташа	Тәуекел жекелеген процестердің іркілістеріне және қосымша шығындарға әкелуі мүмкін	Орта мерзімді перспективада төмендету шаралары талап етіледі
> 60	Жоғары	Тәуекел қызметтің елеулі бұзылуына, қаржылық және беделдік шығындарға әкеледі	Жол берілмейтін тәуекел, басым тәртіппен төмендету талап етіледі

24. Тәуекелді бағалау нәтижелері негізінде АҚ қатерлерін (тәуекелдерін) өңдеу жоспары қалыптастырылады, онда басым активтер мен қатерлер айқындалады, ұйымдастырушылық, техникалық, бағдарламалық және физикалық қорғау шаралары таңдалып, енгізіледі, мерзімдер мен жауапты тұлғалар белгіленеді, сондай-ақ қажет болған жағдайда жоспарды түзете отырып, қалдық тәуекелге бақылау жүзеге асырылады.

8-тарау. Жауапкершілік

25. Техникалық қамтамасыз ету бөлімі және бағдарламалық қамтамасыз етуді әзірлеу және сүйемелдеу бөлімі активтің сыныптамасын айқындауға, активтер тізілімін мерзімді қайта қарауға жауапты болады және оның жыл сайынғы жаңартылуын қамтамасыз етеді.

26. Университетте АҚ-ны қамтамасыз етуге жауапты қызметкерлер Университеттің АҚ қатерлері (тәуекелдері) каталогын және типтік осалдықтар анықтамалығын қалыптастыруға және өзектендіруге, активтердің қорғау құралдарымен қамтамасыз етілу деңгейін объективті бағалауға, Vry мәндерін айқындауға және осы Әдістемеге сәйкес АҚ тәуекелдері деңгейлерін есептеуге жауапты болады.

9-тарау. Өзгерістер енгізу тәртібі

27. Осы Әдістемеге өзгерістер енгізу бағдарламалық қамтамасыз етуді әзірлеу және сүйемелдеу бөлімінің бастығының, техникалық қамтамасыз ету бөлімі бастығының, зерттеулер, инновациялар және цифрландыру жөніндегі проректордың бастамасы бойынша ҚП 001-2025 Құжатталған процедура. Құжаттаманы басқаруға сәйкес жүзеге асырылады.

10-тарау. Келісу және тарату

28. Әдістемені келісу және тарату ҚП 001-2025 Құжатталған процедура. Құжаттаманы басқаруға сәйкес жүргізіледі.

29. Осы Әдістеме зерттеулер, инновациялар және цифрландыру жөніндегі проректормен, құқықтық қамтамасыз ету және мемлекеттік сатып алу бөлімінің бастығымен, персоналды басқару бөлімінің бастығымен және құжаттамалық қамтамасыз ету бөлімінің бастығымен келісіледі.

30. Осы Әдістеменің түпнұсқасы «Келісу парағымен» бірге қабылдау-тапсыру актісі бойынша ҚҚБ-ға сақтауға беріледі.

31. Осы Әдістеменің жұмыс данасы Университет сайтында ішкі корпоративтік желіден қолжетімділікпен орналастырылады.

А қосымшасы

«Ахмет Байтұрсынұлы атындағы Қостанай өңірлік университеті» КЕАҚ ақпараттық қауіпсіздігінің типтік осалдықтары анықтамалығы
(толтыру үлгісімен)

№	Қатер	Осалдық	Мысал
1	Зиянды БҚ (вирустар, трояндар, ransomware, spyware)	Орталықтандырылған антивирустық қорғаудың болмауы	Пайдаланушы ДК-де антивирус жоқ
		Жаңартуларды автоматты орнату бапталмаған жұмыс станцияларын пайдалану мүмкіндігі	Жекелеген жұмыс станцияларында ОЖ мен БҚ жаңартуларын автоматты орнату өшірілген немесе бапталмаған болуы мүмкін, бұл ескірген нұсқаларды пайдалануға әкеледі
		Алынбалы USB-тасымалдағыштарды жұмыс станцияларына қосқан кезде автоматтандырылған антивирустық тексерудің болмауы	Зақымданған USB-тасымалдағыш қосылған кезде зиянды бағдарламалық қамтамасыз ету жұмыс станцияларына таралады
2	DDoS-шабуылдар	Провайдерде DDoS-тен қорғау жоқ	Желілік трафиктің күрт артуы нәтижесінде университет сайтының қолжетімділігі бұзылады.

Құрастырушылар:

АҚ-ны қамтамасыз етуге
жауапты қызметкер А.Тегі

Жасалған күні: