«Ахмет Байтұрсынұлы
атындағы Қостанай
өңірлік университеті»
КЕАҚ

BU
BAITURSYNULY
UNIVERSITY

Бекітемін
Басқарма Төрағасы – Ректор
_____ С. Қуанышбаев
27.12 2024 ж.

# ҚАҒИДАЛАР

## АНТИВИРУСТЫҚ БАҚЫЛАУДЫ ҰЙЫМДАСТЫРУ

**Қ 107-2024**

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 31.12.2024 жылғы № 328 НҚ бұйрығымен **БЕКІТІЛДІ ЖӘНЕ ҚОЛДАНЫСҚА ЕНГІЗІЛДІ**

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

**5 САРАПШЫЛАР:**
Ж. Жарлыгасов – зерттеулер, инновациялар және цифрландыру жөніндегі проректор, ауыл шаруашылығы ғылымдарының кандидаты;
А. Шмит – техникалық қамтамасыз ету бөлімінің бастығы;

**6 ТЕКСЕРУ КЕЗЕҢДІЛІГІ** **3 жыл**

**7 АЛҒАШ РЕТ ЕНГІЗІЛДІ**

## Мазмұны

## 1 тарау. Жалпы ережелер

1. Осы «Ахмет Байтұрсынұлы атындағы Қостанай өңірлік университеті» КЕАҚ-да антивирустық бақылауды ұйымдастыру қағидалары (бұдан әрі – Қағидалар) «Ахмет Байтұрсынұлы атындағы Қостанай өңірлік университеті» КЕАҚ-да (бұдан әрі – Университет) антивирустық бақылауды жүргізу тәртібін ұйымдастыру және бағдарламалық қамтамасыз ету мен ақпараттық жүйелердің компьютерлік вирустармен зақымдану фактілерінің туындауын болдырмау мақсатында әзірленді.

2. Антивирустық бақылау Университеттің ақпараттық жүйелерін, деректерін және желілерін зиянды бағдарламалық қамтамасыз етуден (БҚ), кибершабуылдардан және өзге де қатерлерден қорғауға бағытталған.

3. Қағидалар Университеттің электрондық ақпараттық ресурстарына қол жеткізе алатын барлық қызметкерлердің орындауы үшін міндетті.

4. Қағидалар Университеттің нормативтік-анықтамалық құжаттамасының құрамына кіреді және Университеттің барлық қызметкерлері үшін міндетті болып табылады.

## 2 тарау. Нормативтік сілтемелер

5. Қағидалар келесі құжаттардың талаптары мен ұсынымдарына сәйкес әзірленді және рәсімдерді белгілейді:

1) «Ақпараттандыру туралы» Қазақстан Республикасының 2015 жылғы 24 қарашадағы № 418-V 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) Қазақстан Республикасы Қаржы министрлігі Мемлекеттік мүлік және жекешелендіру комитеті төрағасының 2020 жылғы 05 маусымдағы № 350 бұйрығымен бекітілген, 03.10.2023 жылғы өзгерістерімен «Ахмет Байтұрсынұлы атындағы Қостанай өңірлік университеті» КЕАҚ Жарғысы;

4) ҰС 081-2022 Ұйым стандарты. Іс қағаздарын жүргізу;

5) ҚП 082-2022 Құжатталған процедура. Құжаттаманы басқару;

6) Е 054-2024 «Ахмет Байтұрсынұлы атындағы Қостанай өңірлік университеті» КЕАҚ Ақпараттық қауіпсіздік саясаты.

## 3 тарау. Анықтамалар

6. Осы Қағидаларда мынадай терминдер мен анықтамалар қолданылады:

1) антивирустық бақылау – ақпараттық жүйелерді, деректер мен желілерді зиянды бағдарламалық қамтамасыз етуден (вирустардан, трояндардан, құрттардан, шифрлаушылардан, шпиондық БҚ-дан және басқа қатерлерден) қорғауға бағытталған шаралар, процестер мен технологиялар кешені.

2) антивирустық бағдарламалық қамтамасыз ету (бұдан әрі – антивирустық БҚ) – ақпараттық желіге қосылған компьютерлерде, серверлерде және басқа құрылғыларда зиянды бағдарламалық қамтамасыз етуді (вирустарды, трояндарды, құрттарды, шпиондық БҚ-ны, шифрлаушыларды және басқа киберқатерлерді) анықтауға, бұғаттауға, жоюға және оның таралуын болдырмауға арналған мамандандырылған бағдарламалық кешен.

3) ақпараттық қауіпсіздік (бұдан әрі – АҚ) – ақпараттық ресурстарды рұқсатсыз қол жеткізуден, әдейі немесе кездейсоқ бұрмалаудан және жоюдан, физикалық жоюдан, оның ішінде техногендік және табиғи сипаттағы әсерлер нәтижесінде қорғауды қамтамасыз етуге бағытталған құқықтық, техникалық және ұйымдастырушылық іс-шаралар кешені, сондай-ақ ақпараттық ресурстар мен жүйелердің қорғалу жай-күйі, ақпараттың құпиялылығын, тұтастығын және қолжетімділігін қамтамасыз ету;

4) электрондық ақпараттық ресурстар (ЭАР) – электрондық нысанда қолжетімді дерекқорлар, файлдық қоймалар, ақпараттық жүйелер, веб-сайттар және өзге де ресурстар.

## 4 тарау. Негізгі мақсаттар мен міндеттер

7. Осы мақсаттар мен міндеттер Университеттің ЭАР-ын зиянды бағдарламалық қамтамасыз етуден, кибершабуылдардан және өзге де қатерлерден қорғауды қамтамасыз етуге, сондай-ақ IT-инфрақұрылымның тұрақты әрі қауіпсіз жұмысын қолдауға бағытталған Қағидаларды әзірлеу және енгізу үшін негіз болып табылады.

8. Антивирустық бақылаудың мақсаттары:

1) ақпараттық жүйелерді вирустардан, трояндардан, шифрлаушылардан, шпиондық БҚ-дан және зиянды бағдарламалардың басқа түрлерінен қорғауды қамтамасыз ету;

2) кибершабуылдар салдарынан құпия ақпараттың сыртқа таралуын болдырмау;

3) вирустық шабуылдар немесе қаскүнемдердің әрекеттері салдарынан құпия ақпараттың сыртқа таралу тәуекелдерін азайту;

4) қызметкерлерді киберқауіпсіздік қағидаларына оқыту және корпоративтік деректермен жауапты жұмыс істеу мәдениетін қалыптастыру;

5) жаңа қатерлерге жедел әрекет етуге қабілетті тұрақты қорғау жүйесін құру.

9. Антивирустық бақылаудың міндеттері:

1) корпоративтік желіге қосылған барлық құрылғыларда антивирустық БҚ-ны орнату, баптау және қолдау;

2) жаңа қатерлерден қорғау үшін антивирустық базалар мен бағдарламалық қамтамасыз етуді тұрақты жаңарту;

3) жүйелерде зиянды бағдарламалық қамтамасыз етудің бар-жоғын анықтау үшін тұрақты сканерлеу жүргізу;

4) күдікті әрекеттерді анықтау үшін желілік белсенділікті мониторингтеу және талдау.

**5 тарау. Антивирустық бақылауды жүргізу тәртібі**

10. Университет желісіне қосылған барлық компьютерлер мен серверлерге лицензиялық немесе еркін таратылатын антивирустық БҚ орнатылады.

11. Антивирустық құралдардың жаңартуларын орнатуды және баптауды техникалық қамтамасыз ету бөлімі жүзеге асырады.

12. Міндетті антивирустық бақылауға телекоммуникациялық арналар арқылы алынатын және берілетін кез келген ақпарат (кез келген форматтағы мәтіндік файлдар, деректер файлдары, орындалатын файлдар), сондай-ақ алынбалы тасымалдағыштардағы ақпарат (CD/DVD дискілер, Flash-жинақтағыштар және т.б.) жатады.

13. Пайдаланушы автоматтандырылған жұмыс орнының, сондай-ақ оның барлық сыртқы құрылғыларының мақсатты пайдаланылуын бақылауды жүзеге асырады.

14. Университет компьютерлеріне орнатылатын барлық бағдарламалық қамтамасыз ету зиянды бағдарламалардың бар-жоғына алдын ала тексеріледі. Алынбалы тасымалдағыштардағы ақпаратты бақылау оны пайдаланудың алдында тікелей жүргізіледі.

15. Айына бір реттен сиретпей қорғалатын компьютердің қатты дискілерінде сақталатын барлық файлдарға толық тексеру жүргізіледі.

16. Компьютерлік вирус бар деген күдік туындаған кезде Университет қызметкері кезектен тыс антивирустық тексеру жүргізеді және қажет болған жағдайда компьютерлік вирустың бар немесе жоқ фактісін анықтау үшін техникалық қамтамасыз ету мамандарын тартады.

17. Компьютерлік вирус анықталған кезде Университет қызметкері жұмысты тоқтатуға, вируспен зақымдану фактісі туралы техникалық қамтамасыз ету бөлімінің қызметкерлеріне, сондай-ақ осы файлдарды жұмыста пайдаланатын сабақтас бөлімшелерге хабарлауға міндетті.

18. Пайдаланушыларға Университеттің дербес компьютерлеріне лицензияланбаған бағдарламалық қамтамасыз етуді орнатуға, баптаулар мен конфигурацияларға өз бетінше өзгерістер енгізуге, сондай-ақ антивирустық бағдарламаларды өшіруге немесе жоюға тыйым салынады.

**6 тарау. Антивирустық бағдарламалық қамтамасыз етуге қойылатын базалық талаптар**

19. Антивирустық БҚ лицензиялық немесе еркін таратылатын болуы тиіс.

20. Антивирустық БҚ жаңа қатерлерден қорғау үшін вирустық базалар мен бағдарламалық модульдердің автоматты жаңартылуын қолдауы тиіс.

21. Антивирустық БҚ барлық деңгейлерде қорғауды қамтамасыз етуі тиіс: файлдар мен бағдарламаларды нақты уақыт режимінде тексеру; электрондық поштаны және тіркемелерді сканерлеу; желілік белсенділікті бақылау (брандмауэр); интернет-қорғау; желілік шабуылдардан, фишингтен және зиянды сайттардан қорғау.

22. Антивирустық БҚ Университетте пайдаланылатын операциялық және ақпараттық жүйелермен үйлесімді болуы тиіс.

23. Антивирустық БҚ жүйенің жұмысын едәуір баяулатпауы немесе қосымшалардың жұмысында іркілістер туғызбауы тиіс.

24. Антивирустық БҚ туындайтын мәселелерді жедел шешу үшін қолжетімді техникалық қолдауға ие болуы тиіс.

25. Антивирустық БҚ кейінгі талдау және есептілік үшін қатерлерді анықтауға және жоюға байланысты оқиғалар мен оқыс оқиғалар журналын жүргізуі тиіс.

26. Антивирустық БҚ басқа ақпараттық қауіпсіздік жүйелерімен (SIEM, DLP, IDS/IPS және т.б.) интеграциялану мүмкіндігін қамтамасыз етуі тиіс.

27. Корпоративтік пайдалану үшін антивирустық бағдарламалық қамтамасыз ету орталықтандырылған басқаруды, мониторингті және есептілікті қолдауы тиіс.

## 7 тарау. Жауапкершілік

28. Университет қызметкерлері антивирустық бақылауды ұйымдастыру қағидаларын және антивирустық қорғауға байланысты қауіпсіздік шараларын сақтауға жауапты болады.

29. Университет қызметкерлері антивирустық қауіпсіздіктің бұзылуына байланысты ықтимал қатерлер немесе оқыс оқиғалар туралы техникалық қамтамасыз ету бөліміне уақтылы хабарлауға жауапты болады.

30. Техникалық қамтамасыз ету бөлімінің қызметкерлері вирустық шабуылдарға байланысты оқыс оқиғаларға жедел әрекет етуге және олардың себептеріне талдау жүргізуге міндетті.

31. Университет басшылығы антивирустық бақылау шараларын іске асыру үшін қажетті ресурстармен (қаржылық, техникалық, кадрлық) қамтамасыз етуге жауапты болады.

32. Пайдаланушылар осы Қағидалардың ақпараттық қауіпсіздікті қамтамасыз ету мақсатында қойылатын талаптарын бұзғаны үшін Қазақстан Республикасының заңнамасына сәйкес жауапты болады.

## 8 тарау. Өзгерістер енгізу тәртібі

33. Осы Қағидаларға өзгерістер енгізу бағдарламалық қамтамасыз етуді әзірлеу және сүйемелдеу бөлімі бастығының, техникалық қамтамасыз ету бөлімі бастығының, зерттеулер, инновациялар және цифрландыру жөніндегі

проректордың бастамасы бойынша ҚП 082-2022 Құжатталған процедура. Құжаттаманы басқару құжатына сәйкес жүзеге асырылады.

## 9 тарау. Келісу, сақтау және тарату

34. Қағидаларды келісу, сақтау және тарату ҚП 082-2022 Құжатталған процедура. Құжаттаманы басқару құжатына сәйкес жүргізіледі.

35. Осы Қағидалар 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.

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

37. Осы Қағидалардың жұмыс данасы ішкі корпоративтік желіден кіру мүмкіндігімен Университет сайтында орналастырылады.