

Бекітілді

«Ғарыштық техника және
технологиялар институты» ЖШС
директорының бұйрығымен

2026 ЖЫЛҒЫ «13» 10 №267-0

**«Ғарыштық техника және технологиялар институты»
жауапкершілігі шектеулі серіктестігінің
ақпараттық қауіпсіздік саясаты**

Алматы қ., 2026 ж.

1. Жалпы ережелер

1. Осы «Ғарыштық техника және технологиялар институты» жауапкершілігі шектеулі серіктестігінің ақпараттық қауіпсіздік саясаты (бұдан әрі – Саясат) «Ғарыштық техника және технологиялар институты» жауапкершілігі шектеулі серіктестігінің (бұдан әрі – Институт) ақпараттық қауіпсіздікті қамтамасыз ету саласындағы мақсаттарын, қағидаттарын, қызметінің негізгі бағыттарын, ұйымдастырушылық және техникалық шараларын айқындайды.

2. Нормативтік сілтемелер

2. Осы Саясатты әзірлеу кезінде Қазақстан Республикасының мынадай нормативтік құқықтық актілері, стандарттар және Институттың ішкі нормативтік құжаттары ескерілді:

1) Қазақстан Республикасының 2026 жылғы 9 қаңтардағы № 255-VIII ҚРЗ Цифрлық кодексі;

2) Қазақстан Республикасының 2015 жылғы 23 қарашадағы № 414-V ҚРЗ Еңбек кодексі, оның ішінде қызметкерлердің киберқауіпсіздік талаптарын сақтауы, қызметкерлерді жұмыс берушінің киберқауіпсіздік талаптарын сақтау жөніндегі актілерімен таныстыру және олардың орындалуына ішкі бақылауды жүзеге асыру бөлігінде 22 және 23-баптардың талаптары;

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

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

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

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

7) ақпараттандыру, ақпаратты қорғау, дербес деректерді қорғау және ақпараттық қауіпсіздікті қамтамасыз ету саласындағы Қазақстан Республикасының өзге де нормативтік құқықтық актілері;

8) ҚР СТ ISO/IEC 27001-2023 «Ақпараттық қауіпсіздік, киберқауіпсіздік және құпиялылықты қорғау. Ақпараттық қауіпсіздік менеджменті жүйелері. Талаптар», Қазақстан Республикасы Сауда және интеграция министрлігі Техникалық реттеу және метрология комитеті төрағасының 2023 жылғы 14 қарашадағы № 440-НҚ бұйрығымен қолданысқа енгізілген;

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

10) ҚР СТ ISO 31000 «Тәуекел менеджменті. Қағидаттар мен нұсқаулық»;

11) Институттың ақпараттық қауіпсіздік, ақпаратты қорғау, ақпараттық жүйелерді пайдалану және ақпараттық активтерді басқару саласындағы қызметті регламенттейтін ішкі нормативтік құжаттары.

3. Терминдер мен қысқартулар

3. Саясатта келесі терминдер мен қысқартулар пайдаланылады:

1) Институт – «Ғарыштық техника және технологиялар институты» жауапкершілігі шектеулі серіктестігі;

2) АҚ – ақпараттық қауіпсіздік;

3) АҚБЖ – ақпараттық қауіпсіздікті басқару жүйесі;

4) Институт директоры – Институт қызметіне жалпы басшылықты жүзеге асыратын, Саясатты және ақпараттық қауіпсіздік бойынша өзге де ішкі құжаттарды бекітетін, сондай-ақ ақпараттық қауіпсіздікті қамтамасыз ету мәселелері бойынша шешімдер қабылдайтын бірінші басшы;

5) ақпараттық қауіпсіздік жөніндегі қызметкер (бұдан әрі – АҚ қызметкері) – ақпараттық қауіпсіздік саласындағы қызметті ұйымдастыруға, үйлестіруге, бақылауға және жетілдіруге, сондай-ақ ақпараттық қауіпсіздік бойынша ішкі құжаттар талаптарының сақталуына мониторинг жүргізуге жауапты Институт қызметкері;

6) әкімші – ақпараттық жүйелерді, серверлік, желілік жабдықтарды, жұмыс станцияларын, бағдарламалық қамтамасыз етуді, пайдаланушылардың есептік жазбаларын және Институттың өзге де ақпараттық ресурстарын әкімшілендіруді жүзеге асыратын Институт қызметкері;

7) құрылымдық бөлімше басшысы – өз өкілеттіктері шегінде қарамағындағы бөлімше қызметкерлерінің ақпараттық қауіпсіздік талаптарын сақтауын ұйымдастыруға жауапты Институт қызметкері;

8) пайдаланушы – Институт қызметкері не Институттың ақпараттық ресурстарына қол жеткізу құқығы берілген өзге уәкілетті тұлға;

9) жауапты қызметкер – ақпараттық қауіпсіздікті қамтамасыз ету, ақпараттық активтерді пайдалану, ақпараттық жүйелерді сүйемелдеу немесе белгіленген талаптардың орындалуын бақылау жөніндегі жекелеген іс-шараларды орындау үшін тағайындалған немесе айқындалған Институт қызметкері;

10) ақпараттық қауіпсіздік жөніндегі жұмыс тобы – ақпараттық қауіпсіздікті қамтамасыз ету мәселелерін қарау, ақпараттық қауіпсіздік тәуекелдері мен инциденттерін талдау, сондай-ақ ақпаратты қорғау шараларын жетілдіру жөнінде ұсыныстар мен ұсынымдар әзірлеу үшін қажет болған жағдайда Институт директорының актісімен құрылатын уақытша консультативтік-кеңесші орган. Жұмыс тобының құрамы, міндеттері және қызмет ету мерзімі Институт директорының актісімен айқындалады;

11) актив – Институт үшін құндылығы бар және қорғауға жататын кез келген материалдық немесе материалдық емес объект;

12) ақпараттық актив – Институт қызметінде пайдаланылатын ақпарат, құжаттар, дерекқорлар, электрондық файлдар, техникалық құжаттама, бағдарламалық қамтамасыз ету, ақпараттық жүйелер және өзге де ресурстар;

13) физикалық қорғау шаралары – үй-жайларға, жабдықтарға, ақпараттық жүйелерге, ақпаратты өңдеу құралдары мен ақпарат тасығыштарға рұқсатсыз физикалық қол жеткізудің алдын алуға, сондай-ақ оларды зақымданудан, жоғалудан, ұрланудан және өзге де физикалық әсерлерден қорғауға бағытталған ұйымдастырушылық және инженерлік-техникалық шаралар жиынтығы;

14) ақпараттық қауіпсіздік инциденті – ақпараттың, ақпараттық жүйелердің,

ақпараттық ресурстардың немесе Институттың ақпараттық-коммуникациялық инфрақұрылымының құпиялылығының, тұтастығының немесе қолжетімділігінің бұзылуына әкеп соққан немесе әкеп соғуы мүмкін оқиға немесе оқиғалар жиынтығы.

4. Негізгі мақсаттар мен қағидаттар

4. Ақпараттық қауіпсіздікті қамтамасыз ету Институттың тұрақты жұмыс істеуі мен дамуының, ұйымның стратегиялық мақсаттарына қол жеткізудің, іскерлік беделін сақтаудың, ғылыми-техникалық әзірлемелерді, дербес деректерді және өзге де ақпараттық активтерді қорғаудың негізгі факторларының бірі болып табылады.

5. Ақпараттық қауіпсіздікті қамтамасыз ету жөніндегі қызмет ақпараттық қауіпсіздіктің ішкі және сыртқы қатерлерінің іске асуы салдарынан Институтқа қаржылық, беделдік, материалдық, құқықтық және өзге де залал келтірудің алдын алуға бағытталған.

6. Саясат мынадай негізгі мақсаттарға қол жеткізуге бағытталған:

1) Институт ақпараттық активтерін ақпараттық қауіпсіздіктің өзекті қатерлерінен қорғауды қамтамасыз ету;

2) ақпараттық қауіпсіздік тәуекелдерін және қатерлердің іске асуының ықтимал салдарын азайту;

3) Институт ақпараттық жүйелері мен ақпараттық-коммуникациялық инфрақұрылымының тұрақты және қауіпсіз жұмыс істеуін қамтамасыз ету;

4) Институт қызметінің Қазақстан Республикасының заңнамасы мен ақпараттық қауіпсіздік саласындағы халықаралық стандарттар талаптарына сәйкестігін қамтамасыз ету;

5) мемлекеттік органдардың, серіктестердің, тапсырыс берушілердің, ғылыми ұйымдардың және өзге де мүдделі тараптардың Институтқа деген сенімін сақтау;

6) Институт қызметкерлері арасында ақпараттық қауіпсіздіктің корпоративтік мәдениетін қалыптастыру және дамыту.

7. Көрсетілген мақсаттарға мынадай жай-күйді қамтамасыз ету және тұрақты қолдау арқылы қол жеткізіледі:

1) ақпараттық ресурстардың уәкілетті пайдаланушылар үшін белгіленген өкілеттіктерге сәйкес қолжетімді болуы;

2) Институт ақпараттық жүйелерінің, желілік инфрақұрылымының және сервистерінің тұрақты жұмыс істеуі;

3) таратылуы шектеулі ақпараттың, дербес деректердің, қызметтік ақпараттың және ғылыми-техникалық қызмет нәтижелерінің құпиялылығын қамтамасыз ету;

4) ақпаратты өңдеу, сақтау және беру кезеңдерінің барлығында оның тұтастығы мен дұрыстығын қамтамасыз ету.

8. Институтта ақпараттық қауіпсіздікті қамтамасыз ету мынадай қағидаттар негізінде жүзеге асырылады:

1) заңдылық;

2) ақпаратты қорғауға кешенді тәсіл қолдану;

3) ақпараттық қауіпсіздікті қамтамасыз ету процесінің үздіксіздігі;

- 4) қорғау шараларының ақылға қонымды жеткіліктілігі;
- 5) тәуекелдерді басқару;
- 6) қызметкерлердің жеке жауапкершілігі.

9. Ақпараттық қауіпсіздікті қамтамасыз ету кезінде ең маңызды талаптар мыналар болып табылады:

- 1) Институтта өңделетін және сақталатын ақпараттың құпиялылығын қамтамасыз ету;
- 2) қызметтің үздіксіздігін және ақпараттық ресурстардың қолжетімділігін қамтамасыз ету;
- 3) ақпараттың тұтастығы мен дұрыстығын қамтамасыз ету;
- 4) жеткізушілердің, мердігерлердің және серіктестердің Институт ақпараттық қауіпсіздік талаптарына сәйкестігін қамтамасыз ету;
- 5) ақпараттық жүйелер мен инфрақұрылымның осалдықтарын уақтылы анықтауды және жоюды қамтамасыз ету.

10. Институттың ақпараттық қауіпсіздікті басқару жүйесін құру қағидаттары мыналар болып табылады:

- 1) ақпараттық активтерді рұқсатсыз қол жеткізуден қорғау;
- 2) ақпаратты жоғалтудан, жоюдан, өзгертуден және жария етуден қорғау;
- 3) ақпараттың құпиялылығын, тұтастығын және қолжетімділігін қамтамасыз ету;
- 4) Қазақстан Республикасы заңнамасының және Институттың ішкі нормативтік құжаттарының талаптарын сақтау;
- 5) ақпаратты қорғаудың ұйымдастырушылық, техникалық және бағдарламалық құралдарын қолдану;
- 6) ақпараттық қауіпсіздік тәуекелдерін тұрақты негізде басқару.

5. Институт директорының ақпараттық қауіпсіздікті қамтамасыз ету жөніндегі мақсаттарға қол жеткізу бойынша іс-әрекеттері

11. Институт директоры ақпараттық қауіпсіздікті қамтамасыз етуге, ақпараттық активтерді қорғауға және Институттың ақпараттық-коммуникациялық инфрақұрылымының тұрақты жұмыс істеуіне бағытталған іс-шараларға қажетті ұйымдастырушылық, әкімшілік және ресурстық қолдау көрсетеді.

12. Институт директоры ақпараттық қауіпсіздікті қамтамасыз етуді ұйымның стратегиялық мақсаттарына қол жеткізудің, жарғылық міндеттерді орындаудың, іскерлік беделді сақтаудың, ғылыми-техникалық ақпаратты, дербес деректерді және Институт қызметінде пайдаланылатын өзге де мәліметтерді қорғаудың маңызды шарттарының бірі ретінде таниды.

13. Институт директоры:

- 1) осы Саясатты және ақпараттық қауіпсіздік бойынша өзге де ішкі нормативтік құжаттарды бекітеді;
- 2) осы Саясат талаптарын іске асыру үшін қажетті ұйымдастырушылық, кадрлық, техникалық және қаржылық ресурстардың бөлінуін қамтамасыз етеді;
- 3) ақпараттық қауіпсіздікті қамтамасыз ету жөніндегі іс-шараларды ұйымдастыруға және бақылауға жауапты қызметкерді тағайындайды;
- 4) Институттың құрылымдық бөлімшелері мен қызметкерлері арасында

ақпараттық қауіпсіздік саласындағы рөлдердің, өкілеттіктердің және жауапкершіліктің бөлінуін қамтамасыз етеді;

5) осы Саясаттың іске асырылуына жалпы бақылауды жүзеге асырады;

6) ішкі аудиттердің, тәуекелдерді бағалаудың, ақпараттық қауіпсіздік инциденттерін тергеп-тексерудің нәтижелерін қарайды және түзету іс-шаралары бойынша шешімдер қабылдайды;

7) ақпараттық қауіпсіздік саласында анықталған бұзушылықтар мен сәйкессіздіктерді жою бойынша шаралар қабылдауды қамтамасыз етеді;

8) Институт қызметкерлерінің ақпараттық қауіпсіздік мәселелері бойынша хабардарлығын арттыруға ықпал етеді;

9) қызметкерлерді Институттың киберқауіпсіздік талаптарын сақтау жөніндегі актілерінің талаптарымен таныстыруды және олардың орындалуына ішкі бақылауды ұйымдастыруды қамтамасыз етеді.

6. АҚ саясатының сипаттамасы, қағидаттары, ережелері мен талаптары

14. Институттың ақпараттық қауіпсіздік мақсаттарына қол жеткізу мынадай қағидаттар мен талаптарға негізделеді:

1) Институттың ақпараттық активтерін ақпараттық қауіпсіздіктің ішкі және сыртқы қатерлерінен қорғау;

2) ақпараттық ресурстарға, ақпараттық жүйелерге және ақпаратты өңдеу құралдарына рұқсатсыз қол жеткізудің алдын алу;

3) пайдаланушылардың қол жеткізу құқықтарын олардың лауазымдық міндеттеріне және ең төмен қажетті артықшылықтар қағидатына сәйкес бөлу;

4) ақпараттық қауіпсіздік оқиғаларын, пайдаланушылар мен әкімшілердің әрекеттерін оқиғаларды тіркеу журналдарында тіркеу және сақтау;

5) ақпараттық қауіпсіздік жөніндегі қызметкердің және ақпараттық жүйелер әкімшілерінің ақпараттық қауіпсіздік оқиғаларына тұрақты мониторинг және талдау жүргізуі;

6) ақпараттық ресурстардың, бағдарламалық қамтамасыз етудің және ақпараттық жүйелер баптауларының тұтастығын қамтамасыз ету;

7) ақпаратты рұқсатсыз өзгертуден, жоюдан, бұғаттаудан, көшіруден және таратудан қорғау;

8) ақпараттық қауіпсіздік осалдықтарын, қатерлерін және инциденттерін уақтылы анықтауды қамтамасыз ету;

9) пайдаланушыларды, құрылғыларды және ақпараттық жүйелерді аутентификациялау мен сәйкестендіруді қамтамасыз ету;

10) зиянды бағдарламалық қамтамасыз етудің әсерін болдырмау бойынша ұйымдастырушылық және техникалық шараларды қолдану;

11) деректерді беру арналары мен ақпараттық алмасуды қорғауды қамтамасыз ету.

15. Институтта ақпараттық қауіпсіздікті қамтамасыз ету мынадай қорғау шаралары арқылы іске асырылады:

1) құқықтық;

2) ұйымдастырушылық;

3) бағдарламалық-техникалық;

4) физикалық.

16. Ақпараттық қауіпсіздікті құқықтық қамтамасыз етудің негізін Қазақстан Республикасының заңнамасы, ақпараттық қауіпсіздік саласындағы халықаралық стандарттар, Институттың ішкі нормативтік құжаттары, сондай-ақ осы Саясаттың мақсаттарына қол жеткізу және талаптарын орындау үшін әзірленген ұйымдастырушылық-өкімдік және техникалық құжаттама құрайды.

17. Ұйымдастырушылық қорғау мынадай іс-шаралар арқылы іске асырылады:

- 1) ақпараттық қауіпсіздік саласындағы рөлдер мен жауапкершілікті бөлу;
- 2) ақпараттық активтерді басқару;
- 3) ақпаратты және ақпараттық активтерді жіктеу;
- 4) ақпараттық жүйелер мен ресурстарға қол жеткізуді басқару;
- 5) ақпараттық қауіпсіздік тәуекелдерін басқару процестерін ұйымдастыру;
- 6) ақпараттық қауіпсіздік бойынша ішкі бақылау мен аудитті ұйымдастыру;

7) ақпараттық қауіпсіздік инциденттеріне ден қою процестерін ұйымдастыру;

8) қызметкерлерді ақпараттық қауіпсіздік және киберқауіпсіздік саласында оқытуды, оларға нұсқама беруді, ішкі құжаттармен таныстыруды және олардың хабардарлығын арттыруды ұйымдастыру;

9) қызметкерлердің ақпараттық қауіпсіздік және киберқауіпсіздік саласындағы белгіленген талаптарды сақтауына ішкі бақылауды ұйымдастыру.

Ұйымдастырушылық қорғау шараларын ақпараттық қауіпсіздік жөніндегі қызметкер құрылымдық бөлімшелердің басшыларымен және ақпараттық жүйелер өкімшілерімен бірлесіп әзірлейді, енгізеді және бақылайды.

18. Бағдарламалық-техникалық қорғау мынадай іс-шаралар арқылы іске асырылады:

- 1) пайдаланушыларды сәйкестендіру және аутентификациялау;
- 2) аса маңызды ақпараттық ресурстар үшін көп факторлы аутентификацияны қолдану;
- 3) пайдаланушылардың қол жеткізу құқықтарын бөлу;
- 4) қауіпсіздік оқиғаларын тіркеу және мониторинг жүргізу;
- 5) бағдарламалық қамтамасыз ету мен конфигурациялардың тұтастығын бақылау;
- 6) антивирустық қорғау және зиянды бағдарламалық қамтамасыз етуден қорғау құралдарын қолдану;
- 7) жаңартуларды басқару және осалдықтарды жою;
- 8) желілік инфрақұрылым мен байланыс арналарын қорғау;
- 9) ақпараттың резервтік көшірмесін жасау және оны қалпына келтіру;
- 10) рұқсатсыз қол жеткізуден қорғау құралдарын пайдалану.

19. Ақпараттық қауіпсіздікті қамтамасыз ету кезінде ең маңызды талаптар мыналар болып табылады:

- 1) ақпараттың құпиялылығын, тұтастығын және қолжетімділігін қамтамасыз ету;
- 2) Институт қызметінің үздіксіздігін және ақпараттық жүйелердің тұрақты жұмыс істеуін қамтамасыз ету;
- 3) ғылыми-техникалық, қызметтік және қолжетімділігі шектеулі өзге де

ақпараттың сақталуын қамтамасыз ету;

4) жеткізушілердің, мердігерлердің және өзге де үшінші тараптардың Институттың ақпараттық қауіпсіздік талаптарына сәйкестігін қамтамасыз ету.

7. Ақпараттық қауіпсіздікті басқару шеңберіндегі қызметкерлердің жалпы функциялары мен жауапкершілігі

20. Институт қызметкерлерінің ақпараттық қауіпсіздікті қамтамасыз ету шеңберіндегі негізгі функциялары мыналар болып табылады:

1) Қазақстан Республикасы заңнамасының, осы Саясаттың және Институттың ақпараттық қауіпсіздік және киберқауіпсіздік саласындағы өзге де ішкі актілерінің талаптарын сақтау;

2) ақпаратты, ақпараттық жүйелерді, ақпараттық ресурстарды және Институт активтерін қорғау жөніндегі талаптарды орындау;

3) еңбек міндеттерін орындау барысында қол жеткізілген құпия ақпаратты, дербес деректерді, таратылуы шектеулі қызметтік ақпаратты және өзге де мәліметтерді жария етпеу жөніндегі міндеттемелерді сақтау;

4) ақпараттың құпиялылығын, тұтастығын және қолжетімділігін бұзуға әкеп соғуы мүмкін әрекеттердің алдын алу;

5) корпоративтік есептік жазбаларды, парольдерді, электрондық поштаны, Интернет желісін, мобильді құрылғыларды, ақпарат тасығыштарды, бағдарламалық қамтамасыз етуді және ақпаратты өңдеудің өзге де құралдарын қауіпсіз пайдалану талаптарын сақтау;

6) Институттың ішкі құжаттарында көзделген ақпараттық қауіпсіздік және киберқауіпсіздік талаптарымен танысу, нұсқамадан өту және хабардарлықты арттыру жөніндегі өзге де іс-шараларға қатысу;

7) Институттың киберқауіпсіздік жөніндегі актілерінің талаптарын сақтау;

8) анықталған ақпараттық қауіпсіздік инциденті, ықтимал инцидент белгілері, күмәнді белсенділік, анықталған қатер, есептік деректердің ықтимал компрометациясы немесе ақпараттық қауіпсіздіктің бұзылуына әкеп соғуы мүмкін өзге де мән-жайлар туралы келтірілген залалдың бар-жоғына қарамастан, ақпараттық қауіпсіздік жөніндегі қызметкерге, тиісті ақпараттық жүйенің әкімшісіне және (немесе) тікелей басшысына дереу хабарлау.

21. Ақпараттық қауіпсіздік жөніндегі қызметкер:

1) ақпараттық қауіпсіздік тәуекелдерін талдауды, бағалауды және мониторинг жүргізуді жүзеге асырады, сондай-ақ оларды төмендету жөніндегі шараларды әзірлейді;

2) осы Саясаттың және ақпараттық қауіпсіздік жөніндегі өзге де құжаттар талаптарының сақталуын бақылайды;

3) ақпараттық қауіпсіздікті қамтамасыз ету мәселелері бойынша құрылымдық бөлімшелердің қызметін үйлестіреді;

4) қызметкерлерді Институттың ішкі құжаттарымен олардың ақпараттық қауіпсіздік және киберқауіпсіздік талаптарына қатысты бөлігінде таныстыруды ұйымдастырады;

5) қызметкерлерді ақпараттық қауіпсіздік және киберқауіпсіздік саласындағы талаптармен таныстыру, оларға нұсқама беру және хабардарлығын арттыру жөніндегі материалдарды әзірлейді және өзектендіреді;

- 6) жүргізілген таныстыру мен нұсқаманың есебін ұйымдастырады;
- 7) өз құзыреті шегінде қызметкерлердің ақпараттық қауіпсіздік және киберқауіпсіздік саласындағы белгіленген талаптарды орындауына ішкі бақылауды жүзеге асырады;
- 8) қызметкерлерден ақпараттық қауіпсіздік инциденттері, ықтимал инциденттердің белгілері, қатерлер және күмәнді белсенділік туралы хабарламаларды қабылдайды, олардың тіркелуін ұйымдастырады және әкімшілермен, құрылымдық бөлімшелердің басшыларымен және өзге де жауапты қызметкерлермен олардың құзыреті шегінде бірлесіп әрекет ете отырып, инциденттерге ден қоюды үйлестіреді.

22. Қажет болған жағдайда ақпараттық қауіпсіздікті қамтамасыз етудің жекелеген мәселелерін қарау үшін Институт директорының актісімен ақпараттық қауіпсіздік жөніндегі жұмыс тобы құрылуы мүмкін. Жұмыс тобының құрамына Институт директоры не ол уәкілеттік берген тұлғалар, ақпараттық қауіпсіздік жөніндегі қызметкер, әкімшілер, құрылымдық бөлімшелердің басшылары және қызметі Институттың ақпараттық активтерін пайдаланумен байланысты өзге де қызметкерлер кіре алады.

8. Саясатты бұзған жағдайда қойылатын талаптар

23. Институт директоры осы Саясатты іске асыру, оның орындалуына қажетті жағдайларды қамтамасыз ету және ақпараттық қауіпсіздік мәселелері бойынша шешімдер қабылдау үшін жалпы жауапкершілікті өзіне алады.

24. Институттың құрылымдық бөлімшелерінің басшылары қарамағындағы бөлімшелер қызметкерлерінің осы Саясат талаптарын орындауын ұйымдастыруға, сондай-ақ өз өкілеттіктері шегінде ақпараттық қауіпсіздіктің белгіленген талаптарының сақталуына жауапты болады. Құрылымдық бөлімшелердің басшылары қарамағындағы бөлімшелер қызметкерлерінің киберқауіпсіздіктің белгіленген талаптарын сақтауын қамтамасыз етеді және өз өкілеттіктері шегінде ішкі бақылауды жүзеге асыруға қатысады.

25. Институт қызметкерлері осы Саясаттың, ақпараттық қауіпсіздік және киберқауіпсіздік жөніндегі ішкі нормативтік құжаттардың, ақпараттық ресурстарды, есептік жазбаларды, парольдерді, бағдарламалық қамтамасыз етуді, мобильді құрылғыларды, ақпарат тасығыштарды және ақпаратты өңдеу құралдарын пайдалану қағидаларының талаптарын сақтау үшін дербес жауапты болады.

26. Институт қызметкерлері еңбек міндеттерін орындау барысында өздеріне белгілі болған құпия ақпаратты, дербес деректерді, таратылуы шектеулі қызметтік ақпаратты, ғылыми-техникалық құжаттаманы және өзге де мәліметтерді жария етпеу үшін жауапты болады.

27. Институттың барлық қызметкерлері осы Саясаттың және Институттың ақпараттық қауіпсіздік пен киберқауіпсіздік жөніндегі өзге де ішкі актілерінің талаптарын сақтауға міндетті. Қызметкерлер көрсетілген талаптармен Институт белгілеген тәртіппен таныстырылуға тиіс. Танысу фактісі қызметкердің тиісті журналдағы, танысу парағындағы қолтаңбасымен не танысу фактісін растауға мүмкіндік беретін ақпараттық жүйе арқылы расталады.

Қазақстан Республикасы Еңбек кодексінің 23-бабы 1-тармағының 6)

тармақшасына сәйкес жұмыс беруші Қазақстан Республикасының Еңбек кодексінде көзделген жағдайларда және тәртіппен қызметкерлерге тәртіптік жаза қолдануға құқылы. Осы Саясат талаптарын бұзу тәртіптік теріс қылық болып табылған жағдайда тәртіптік жаза Қазақстан Республикасы Еңбек кодексінің 64–66-баптарында белгіленген тәртіппен қолданылады.

28. Осы Саясатты бұзушылықтарға, оның ішінде, мыналар жатады:

1) логиндерді, парольдерді және қол жеткізудің өзге де деректемелерін үшінші тұлғаларға беру;

2) Институттың ақпараттық ресурстары мен ақпараттық жүйелеріне рұқсатсыз қол жеткізуді ұсыну;

3) лицензияланбаған немесе рұқсат етілмеген бағдарламалық қамтамасыз етуді орнату және пайдалану;

4) ақпараттық қауіпсіздіктің белгіленген талаптарын бұза отырып, рұқсат етілмеген ақпарат тасығыштар мен құрылғыларды қосу;

5) құпия ақпаратты, таратылуы шектеулі қызметтік ақпаратты немесе дербес деректерді жария ету;

6) дербес деректерді өңдеу, сақтау және қорғау тәртібін бұзу;

7) келтірілген залалдың немесе ақпараттық жүйелер жұмысының бұзылуының бар-жоғына қарамастан, анықталған ақпараттық қауіпсіздік инциденті, ықтимал инцидент белгілері, күмәнді белсенділік, анықталған қатер немесе есептік деректердің ықтимал компрометациясы туралы ақпараттық қауіпсіздік жөніндегі қызметкерге, әкімшіге және (немесе) тікелей басшыға хабарламау не уақтылы хабарламау;

8) ақпараттың резервтік көшірмесін жасау, сақтау, жою немесе қалпына келтіру тәртібін бұзу;

9) ақпаратты қорғау құралдарын айналып өту, ажырату немесе олардың жұмысын қасақана бұзу;

10) зиянды бағдарламаларды, қорғауды айналып өтуге арналған бағдарламалық құралдарды немесе ақпараттық жүйелерге құқыққа сыйымсыз әсер етудің өзге де құралдарын жасау, пайдалану немесе тарату;

11) ақпараттың құпиялылығын, тұтастығын немесе қолжетімділігін бұзуға әкеп соққан не әкеп соғуы мүмкін өзге де әрекеттер немесе әрекетсіздік;

12) Институт белгілеген киберқауіпсіздік талаптарын бұзу, оның ішінде ақпараттық жүйелерді, ақпараттық ресурстарды, корпоративтік есептік жазбаларды және ақпаратты өңдеу құралдарын қауіпсіз пайдалану қағидаларын сақтамау;

13) Институттың ішкі актілерінде осындай танысу немесе нұсқама көзделген жағдайларда киберқауіпсіздік мәселелері бойынша міндетті танысудан немесе нұсқамадан өтуден бас тарту.

9. Қызметкерлерді киберқауіпсіздік талаптарымен таныстыруды және ішкі бақылауды ұйымдастыру

29. Осы Саясат және қызметкерлер үшін ақпараттық қауіпсіздік пен киберқауіпсіздік талаптарын белгілейтін Институттың өзге де ішкі актілері тиісті қызметкерлердің назарына Институт белгілеген тәртіппен жеткізіледі. Қызметкерлердің танысу фактісі нұсқамаларды (таныстыруды) тіркеу

журналындағы, танысу парағындағы қолтаңбамен не танысу фактісін растауға мүмкіндік беретін ақпараттық жүйе арқылы расталады. Саясат Институттың ішкі ақпараттық ресурсында не қызметкерлер үшін қолжетімді өзге де ресурсында орналастырылады.

30. Қызметкерлерді Институттың ішкі актілерінде белгіленген киберқауіпсіздік талаптарымен таныстыруды ақпараттық қауіпсіздік жөніндегі қызметкер кадр қызметімен, құрылымдық бөлімшелердің басшыларымен және ақпараттық жүйелер әкімшілерімен олардың құзыреті шегінде өзара іс-қимыл жасай отырып ұйымдастырады.

31. Таныстыру:

1) қызметкерді жұмысқа қабылдау кезінде;

2) киберқауіпсіздік талаптарын белгілейтін Институттың жаңа ішкі құжаттары бекітілген немесе қолданыстағы ішкі құжаттарға елеулі өзгерістер енгізілген кезде;

3) қызметкердің лауазымдық міндеттері өзгерген кезде, егер мұндай өзгеріс ақпараттық жүйелер мен ақпараттық ресурстарға жаңа немесе кеңейтілген қолжетімділік беруге байланысты болса;

4) ақпараттық қауіпсіздік инциденттерінің, анықталған бұзушылықтардың нәтижелері бойынша немесе жаңа елеулі қатерлер пайда болған кезде қажеттілігіне қарай;

5) Институттың ішкі актілерінде белгіленген өзге де жағдайларда жүргізіледі.

32. Институтта киберқауіпсіздік мәселелері бойынша кіріспе, бастапқы, қайталама және жоспардан тыс таныстыру (нұсқама) жүргізілуі мүмкін. Тиісті іс-шараларды өткізу тәртібі мен кезеңділігі Институттың ішкі актілерінде айқындалады.

33. Жүргізілген таныстыруды (нұсқаманы) есепке алу Қызметкерлердің киберқауіпсіздік жөніндегі нұсқамаларын тіркеу журналында не нақты қызметкердің танысу күнін, мазмұнын және фактісін растау мүмкіндігін қамтамасыз ете отырып, электрондық нысанда жүзеге асырылады.

34. Қызметкерлердің киберқауіпсіздік талаптарын орындауына ішкі бақылауды ақпараттық қауіпсіздік жөніндегі қызметкер құрылымдық бөлімшелердің басшыларымен және ақпараттық жүйелер әкімшілерімен олардың құзыреті шегінде өзара іс-қимыл жасай отырып, Институттың ішкі актілері талаптарының сақталуын, ақпараттық қауіпсіздік оқиғалары мониторингінің нәтижелерін, анықталған бұзушылықтар мен инциденттерді талдау, сондай-ақ жоспарлы және жоспардан тыс тексеру іс-шараларын өткізу арқылы жүзеге асырады. Ішкі бақылау нәтижелері қажет болған жағдайда қызметтік жазбамен, актімен, есеппен, чек-парақпен не Институттың өзге де ішкі құжатымен ресімделеді.

10. Саясатты қайта қарауға қойылатын талаптар

35. Осы Саясат Институттың ақпараттық қауіпсіздікті қамтамасыз ету саласындағы негіз қалаушы құжаты болып табылады және Институттың барлық қызметкерлерінің орындауы үшін міндетті. Саясат қажеттілігіне қарай қайта қаралады. Саясатқа өзгерістер мен толықтырулар Институттың ақпараттық

қауіпсіздік саласындағы қызметіне қатысты Қазақстан Республикасының заңнамасы өзгерген кезде, сондай-ақ ақпараттық қауіпсіздіктің белгіленген шараларын өзгертуді талап ететін мән-жайлар анықталған кезде енгізіледі.