«БЕКІТЕМІН»
Нұр-Мүбарак ЕИМУ ректоры,
Доктор, профессор Мухаммад
әш-Шаххат әл-Жинди
_____
«29» «08» 2024 ж.

САПА МЕНЕДЖМЕНТ ЖҮЙЕСІ

АҚПАРАТТЫҚ ҚАУІПСІЗДІК САЯСАТЫ

Нұр-Мүбарак ЕИМУ -001- 07-2024

Қызмет бабында пайдалану үшін

Алматы 2024

1. ӘЗІРЛЕГЕН: Сапа менеджмент жүйесі бөлімі
2. ЕНГІЗІЛДІ: «29.08.2024ж» Нұр-Мүбарак ЕИМУ Ғылыми кеңесінің №1 хаттамасымен бекітілді және қолданысқа енгізілді.
3. ТЕКСЕРІЛУ МЕРЗІМІ: 2027ж.

Келісілді:

Проректор Қ.Құрманбаев
Академиялық мәселелер департаментінің директоры М.Махмет
Заңгер Н.Абдығали
Сапа менеджмент жүйесі бөлімінің меңгерушісі Ш.Әділбаева

МАЗМҰНЫ

КІРІСПЕ

Аталған ақпараттық қауіпсіздік саясаты (бұдан әрі - Саясат) Нұр-Мүбарак Египет Ислам мәдениеті университетінде (бұдан әрі - ЖОО) ақпаратты қорғау бойынша негізгі қағидаттарды, бағыттарды және талаптарды анықтайды, ақпараттық қауіпсіздік режимін қамтамасыз ету негізін қалайды және сәйкес ережелер, қағидалар, нұсқаулықтарды әзірлеу кезінде негіз болып табылады.

Саясаттың нормативтік-құқықтық негізін Қазақстан Республикасының ақпараттық жүйелерді пайдалану мәселелері бойынша заңнамасы, Қазақстан Республикасының нормативтік құқықтық актілері және халықаралық ақпараттық қауіпсіздік басқару стандарттары құрайды.

Ақпараттық қауіпсіздікті қамтамасыз ету ЖОО-ның коммерциялық қызметін сәтті жүзеге асыру үшін қажетті шарт болып табылады. ЖОО ақпаратты ең маңызды активтердің бірі ретінде қарастырады. Ақпараттық қауіпсіздік ЖОО-ның оқу процесінің қауіпсіздігін қамтамасыз ету саласындағы жалпы саясатының бір бөлігі болып табылады. Осы салалардағы бұзушылықтар айтарлықтай салдарларға, оның ішінде клиенттердің сенімін жоғалту мен бәсекеге қабілеттіліктің төмендеуіне әкеп соғуы мүмкін.

Ақпараттық қауіпсіздікті қамтамасыз ету ақпаратты және/немесе оны қолдайтын инфрақұрылымды қорғауға бағытталған барлық әрекеттерді қамтиды. Саясат ЖОО-ның иелігіндегі және пайдаланатын барлық автоматтандырылған және телекоммуникациялық жүйелерге қатысты. Аталған құжаттың ережелері ЖОО-ның автоматтандырылған және телекоммуникациялық жүйелеріне қолжетімдігі бар барлық штаттық және уақытша қызметкерлерге қатысты.

Ақпаратты қорғауды ұйымдастырудың маңызды бөлімі – қабылданған шаралардың тиімділігін үздіксіз бақылау, ЖОО қызметкерлері үшін қабылданбайтын іс-әрекеттер тізімін, ықтимал салдарын және жауапкершілікті анықтау болып табылады.

Саясатты жүзеге асыру ақпаратты қорғаудың қажетті деңгейін қамтамасыз ету тек бір ғана құралмен (шарамен) емес, олардың қарапайым жиынтығымен мүмкін еместігін ескеруді қажет етеді. Олар жүйелі түрде өзара үйлестіріліп (кешенді түрде қолдану), ақпараттық жүйенің әрбір жеке элементі қорғаудың қамтамасыз етілген орындалуындағы біртұтас ақпараттық жүйе ретінде қарастырылуы тиіс, ал техникалық (аппараттық, бағдарламалық) құралдар мен ұйымдастырушылық шаралардың оңтайлы үйлесімін қамтамасыз ету қажет.

1. ТЕРМИНДЕР МЕН АНЫҚТАМАЛАР

Осы Саясатта келесі ұғымдар қолданылады:

Аутентификация – қол жеткізу субъектісінің ұсынған идентификаторын тексеру; шынайылықты растау.

Ақпараттық қауіпсіздік – ақпараттың оның қалаусыз жариялануынан (құпиялылықтың бұзылуы), бұрмалануынан (тұтастықтың бұзылуы), жоғалуынан немесе қолжетімдіктің төмендеуінен, сондай-ақ заңсыз көшірмеленуінен қорғау.

Қолжетімділік – авторизацияланған пайдаланушының ақпараттық жүйеден функционалдылықта қарастырылған ақпараттық қызметті қабылданатын уақыт ішінде алу мүмкіндігі.

Идентификация – субъектілер мен объектілерге идентификатор тағайындау және/немесе ұсынылған идентификаторды тағайындалған идентификаторлар тізімімен салыстыру.

Ақпараттық қауіпсіздік (АқҚ) – ақпаратты жинау, өңдеу, беру және сақтау процесінде оның құпиялылығын, тұтастығын және санкцияланған қолжетімділігін қамтамасыз етуге бағытталған әкімшілік-құқықтық, ұйымдастырушылық-реттеушілік және техникалық шаралар кешені.

Ақпараттық жүйе (АЖ) ақпаратты өңдеу – келесі өзара байланысты құрамдас бөліктерден тұратын ұйымдастырушылық-техникалық құрылым:

- деректерді өңдеу және беру үшін техникалық құралдар;
- тиісті бағдарламалық қамтамасыз ету түрінде өңдеу әдістері мен алгоритмдері;
- әртүрлі тасымалдаушыларда деректер базасы;
- деректерді автоматтандырылған өңдеуді жүзеге асыру үшін ұйымдық структуралық, тақырыптық, технологиялық немесе басқа белгілер бойынша біріктірілген персонал мен пайдаланушылар.

Құпиялылық – рұқсатсыз танысудан қорғау.

Рұқсатсыз әрекет – ақпаратты өңдеу жүйесінде белгіленген ережелерді бұзу арқылы субъектінің әрекеті.

Пайдаланушы – ақпаратты оның иесінен, иегерінен немесе делдалынан белгіленген құқықтар мен ақпаратқа қол жеткізу ережелеріне сәйкес пайдаланатын субъект.

Желілер (локальды желі, ЛЖ, LAN) – байланыс орнату мен ақпарат беру үшін станцияларды біріктіретін коммуникациялық құрылғылар жиынтығымен қосылған нүктелер, түйіндер немесе басқа құрылғылар тобы.

Қатер – объектінің жұмыс режимін әдейі немесе кездейсоқ бұзу мақсатында қауіпті әсер етуші факторларды жүзеге асыру бойынша шын немесе мүмкін болатын әрекеттер.

Сезімталдық – автоматтандырылған жүйенің кез келген сипаттамасы, оны пайдалану қатерлерді жүзеге асыруға әкелуі мүмкін.

Ақпараттың тұтастығы – ақпараттың бұрмаланбай, бастапқы күйінде сақталу қасиеті.

Шифрлау – деректерді оқу мүмкін болмайтындай етіп, шифрлау мен дешифрлау кілттерін пайдаланып түрлендіру.

2. МАҚСАТТАР, МІНДЕТТЕР ЖӘНЕ НЕГІЗГІ ПРИНЦИПТЕР

2.1 Ақпараттық қауіпсіздік жүйесінің негізгі мақсаты - ЖОО-ның корпоративтік ақпараттық жүйесін (АЖ) ақпаратқа, оның тасымалдаушыларына, өңдеу және беру процестеріне кездейсоқ немесе әдейі әсер ету арқылы материалдық, физикалық, моральдық немесе басқа да залал келтіруден қорғау, сондай-ақ қауіп деңгейін минимизациялау.

2.2 Ақпараттық қауіпсіздік жүйесінің негізгі міндеттері:

2.2.1 ақпаратты құпия емес, шектеулі таралымды, банктік, коммерциялық және басқа да құпия түрлеріне жатқызу, сондай-ақ оны заңсыз пайдаланудан қорғау үшін қорғалатын басқа да конфиденциалды ақпаратты анықтау;

2.2.2 ЖОО-ның ақпараттық ресурстарына қауіптерді болжау және уақытылы анықтау, қаржылық, материалдық және моральдық залал келтіруге, оның қалыпты жұмыс істеуі мен дамуына кедергі келтіруге ықпал ететін себептер мен жағдайларды анықтау;

2.2.3 ЖОО-ны ақпараттық ресурстардың қауіпсіздігіне қауіп төндіретін ықтимал әсерлер мен залал келтірудің мүмкіндігін барынша азайту үшін жұмыс істеу шарттарын жасау;

2.2.4 ақпараттық қауіпсіздікке қатысты қауіптерге жедел жауап беру және ЖОО-ның қызметінде теріс үрдістерді айқындау үшін механизмдер мен жағдайлар жасау, нормативтік, құқықтық, ұйымдастырушылық және техникалық шаралар мен құралдарды қолдану негізінде;

2.2.5 заңсыз әрекеттермен физикалық және заңды тұлғалар тарапынан келтірілген залалды барынша өтеу және локализациялау үшін жағдайлар жасау.

2.3 ЖОО-ның ақпараттық қауіпсіздігін қамтамасыз ету жүйесін құру және оның жұмыс істеуі келесі негізгі принциптерге сәйкес жүзеге асырылуы тиіс:

2.3.1 заңдылық - ақпаратты қорғау және ақпараттық алмасу барлық қатысушыларының заңды мүдделерін сақтау бойынша заңнаманы сақтау;

2.3.2 жүйелілік - ақпараттық қауіпсіздікті ұйымдастыру мәселелеріне логикалық және дәйекті көзқарас: алдымен ақпараттық қауіпсіздіктің тәуекелін нақты қатерлер мен ақпараттық ресурстардың сезімталдықтарына негізделген бағалау, содан кейін ЖОО-ның ерекшеліктерін ескере отырып, ұйымдастырушылық және техникалық шаралар мен қорғаныс құралдарының кешенін құру;

2.3.3 тиімділік - ақылға қонымды көлемде жүзеге асырылатын шаралар мен іс-шаралар ақпараттық қауіпсіздікті қамтамасыз ету үшін тәуекелдерді минимизациялауы керек, ал қорғаныс шараларының адекваттығы мен тиімділігі тұрақты негізде бағалануы тиіс;

2.3.4 мақсатқа сәйкестік - ақпаратты қорғау үшін жұмсалатын шығындар мен қауіптің жүзеге асырылуы кезінде мүмкін болатын жоғалтулар арасындағы өлшемді сәйкестікті сақтау;

2.3.5 үздіксіздік - жүйенің жұмыс істеу принципі, оның ішінде зиянкестер кез-келген уақытта қорғаныс шараларын айналып өту мүмкіндігін іздейді, ол үшін заңды және заңсыз әдістерді қолдануы мүмкін;

2.3.6 өзара іс-қимыл және үйлестіру - ақпараттық қауіпсіздікті қамтамасыз ету шараларын қауіпсіздік қызметінің бөлімшелері, ақпараттық технологиялар және ақпараттық ресурстарды пайдаланушы бөлімшелерінің, ақпаратты қорғау және ақпараттық жүйелерді қызмет көрсету саласындағы сыртқы мамандандырылған ұйымдардың өзара байланысы негізінде жүзеге асыру, олардың күш-жігерін мақсаттарға қол жеткізу үшін үйлестіру, сондай-ақ уәкілетті мемлекеттік органдармен өзара іс-қимыл жасау. Ақпараттық қауіпсіздікті қамтамасыз ету шараларын іске асыру кәсіби дайындық деңгейі жоғары ВУЗ бөлімшелерінің жауапты қызметкерлерімен жүргізілуі тиіс;

2.3.7 жетілдіру - қорғаныс шаралары мен құралдарын жетілдіру, өз тәжірибесіне, жаңа техникалық құралдардың пайда болуына, ақпараттық ресурстарды қорғау әдістері мен құралдары, нормативтік-техникалық талаптар, отандық және шетелдік тәжірибені ескере отырып;

2.3.8 басымдық - ЖОО-ның барлық ақпараттық ресурстарын маңыздылығы бойынша топтастыру (рейтингтеу) және ақпараттық қауіпсіздікке қатысты нақты және мүмкін болатын қауіптерді бағалау;

2.3.9 хабардарлық және жеке жауапкершілік - ақпараттық ресурстар пайдаланушылары ақпараттық бақылау мен қорғау жүйесінің бар екендігін білуі тиіс, ақпараттық қызметтер пайдаланушыларды жеке сәйкестендіреді және олардың бастамашылық еткен процестерін қадағалайды;

2.3.10 стандарттарға сәйкестік - ақпараттық қауіпсіздік жүйесі осы саладағы

4. АҚПАРАТТЫҚ ҚАУІПСІЗДІКТІ ҚАМТАМАСЫЗ ЕТУ ШАРАЛАРЫ

4.1 Ақпараттық жүйелерді қорғау шаралары келесі түрлерге бөлінеді:

- құқықтық (заңнамалық);
- моральдық-этикалық;
- ұйымдастырушылық (әкімшілік);
- физикалық;
- техникалық (аппараттық және бағдарламалық).

4.2 Заңнамалық (құқықтық) қорғау шаралары. Құқықтық қорғау шараларына елдегі қолданыстағы заңдар, жарлықтар және нормативтік актілер жатады, олар ақпаратпен жұмыс істеу ережелерін реттейді, ақпараттық қатынастарда қатысушылардың құқықтары мен міндеттерін бекітеді және осы ережелерді бұзғаны үшін жауапкершілікті белгілейді. Осылайша, олар ақпаратты заңсыз пайдалануды болдырмауға және ықтимал құқық бұзушылар үшін тежегіш фактор ретінде әрекет етеді. Құқықтық қорғау шаралары негізінен алдын алу және профилактикалық сипатта болады және пайдаланушылармен және жүйені қызмет көрсету персоналымен тұрақты түсіндіру жұмысын жүргізуді талап етеді.

4.3 Моральдық-этикалық қорғау шаралары. Моральдық-этикалық шараларға елде немесе қоғамда ЭВМ қолданудың таралуына байланысты қалыптасатын немесе қалыптасқан мінез-құлық нормалары жатады. Бұл нормалар көбінесе заңмен бекітілген нормативтік актілер сияқты міндетті емес, бірақ оларды сақтамау әдетте жеке тұлғаның, топтың немесе ұйымның беделі мен абыройының төмендеуіне әкеледі. Моральдық-этикалық нормалар жазылмаған болуы мүмкін (мысалы, адалдық, патриотизм сияқты жалпы танылған нормалар) немесе жазбаша түрде рәсімделген болуы мүмкін, яғни белгілі бір ережелер немесе нұсқаулар жинағына енгізілген. Моральдық-этикалық қорғау шаралары профилактикалық сипатта болады және бөлімшелердің ұжымдарында дені сау моральдық климат қалыптастыру бойынша тұрақты жұмыстарды жүргізуді талап етеді.

4.4 Ұйымдастырушылық (әкімшілік) қорғау шаралары. Ұйымдастырушылық (әкімшілік) қорғау шаралары - бұл ақпараттық жүйенің жұмыс істеу процестерін, оның ресурстарын пайдалану, қызмет көрсету персоналының әрекеттерін, сондай-ақ пайдаланушылардың жүйемен өзара әрекеттесу тәртібін реттейтін ұйымдастырушылық сипаттағы шаралар, олар қауіптерді іске асыру мүмкіндігін барынша қиындатуға немесе болдырмауға, сондай-ақ олардың іске асырылған жағдайда жоғалту мөлшерін азайтуға бағытталған.

4.5 Физикалық қорғау құралдары. Физикалық қорғау шаралары - бұл жүйенің компоненттеріне және қорғалатын ақпаратқа ықтимал бұзушылардың қолжетімділігін шектеу немесе болдырмау үшін арнайы механикалық, электро-немесе электронды-механикалық құрылғылар мен ғимараттарды қолдануға негізделген шаралар, сондай-ақ визуалды бақылау құралдары, байланыс және күзет сигнализациясы жүйелері.

4.6 Техникалық (бағдарламалық-аппараттық) қорғау шаралары. Техникалық (аппараттық-бағдарламалық) қорғау шаралары ақпараттық жүйелердің құрамына кіретін әртүрлі электрондық құрылғылар мен арнайы бағдарламаларды қолдануға негізделген, олар (өздігінен немесе басқа қорғау құралдарымен кешенді түрде) қорғаныс функцияларын орындайды (пайдаланушыларды сәйкестендіру және аутентификациялау, ресурстарға қолжетімділікті шектеу, оқиғаларды тіркеу, ақпаратты криптографиялық түрде қорғау және т.б.).

5. АҚПАРАТТЫҚ ҚАУІПСІЗДІКТІҢ ҚАТЕРЛЕРІ

5.1 Ақпараттық қауіпсіздік қатерлері деп қорғауға алынған ақпаратқа ықтимал теріс әсер ететін жағдайлар мен оқиғаларды түсінеді, олардың ішінде:

5.1.1 банктік құпияны, коммерциялық құпияны, университеттің басқа қорғалған ақпаратын жоғалту немесе оның бұрмалануы (рұқсатсыз өзгерту, жалған құру);

5.1.2 ақпараттың сыртқы адамдарға рұқсатсыз ашылуы (рұқсатсыз кіру, көшіру, ұрлау және т.б.), сондай-ақ ақпараттың байланыс арналарымен немесе электромагниттік сәулеленулер арқылы ағып кетуі;

5.1.3 ақпараттың қолжетімсіздігі, оның блокталуы, жабдықтардың немесе бағдарламалардың ақауы, операциялық жүйелердің, жұмыс станциялары, серверлер, маршрутизаторлар, дерекқорларды басқару жүйелері, тарату есептеу желілері жұмысының бұзылуы, вирустардың әсері, табиғи апаттар және басқа да форс-мажорлық жағдайлар;

5.1.4 жоспарлау және бақылау болмауы;

5.1.5 бағдарламалық қамтамасыз етудің төмен сенімділігі;

5.1.6 персоналдың жеткіліксіз білім деңгейі, ақпараттық технологиялар саласындағы персонал мен пайдаланушылардың біліктілігінің төмендігі.

5.2 Бұл қауіптердің әсерінен ақпараттық қауіпсіздіктің және университеттің қалыпты жұмыс істеуінің жай-күйіне теріс әсер ететін келесі салдарлар туындауы мүмкін:

5.2.1 ақпараттың ағып кетуі немесе жариялануына байланысты қаржылық шығындар;

5.2.2 жоғалған ақпаратты жою және қалпына келтірумен байланысты қаржылық

шығындар;

5.2.3 университет қызметінің бұзылуынан және міндеттемелерді орындаудың мүмкін болмауынан туындаған шығындар;

5.2.4 моральдық шығындар (университет беделінің жоғалуы).

6. ЖОО-ның АҚПАРАТТЫҚ ҚАУІПСІЗДІГІН ТЕХНИКАЛЫҚ ҚАМТАМАСЫЗ ЕТУ ШАРАЛАРЫ

6.1 Ақпараттық қауіпсіздікті техникалық қамтамасыз ету негізделуі тиіс:

6.1.1 қолданылатын қорғау құралдарының жүйелік үйлесімі мен өзара толықтырылуына;

6.1.2 қызметті лицензиялауға;

6.1.3 барлық бағдарламалық қамтамасыз ету мен қорғау құралдарының сертификаттау жүйесіне.

6.2 Ақпараттық ресурстарды қорғау жүйесі құжат айналымы, қызметкерлердің құпия құжаттармен және ақпаратпен жұмыс істеуі, әртүрлі деңгейдегі автоматтандырылған жүйелерде ақпарат өңдеу, байланыс арналарымен беру, құпия келіссөздер жүргізу барысында ақпаратты қорғауға арналған кешенді ұйымдастырушылық, техникалық, бағдарламалық және криптографиялық құралдар мен шараларды қарастыруы керек.

6.3 Университет қызметкерлеріне тиісті ақпаратқа қолжетімділік құқықтары университеттің ішкі құжаттарында анықталған тәртіп бойынша белгіленеді.

6.4 Ақпараттық қауіпсіздікті қамтамасыз ету бағыттарының бірі — техникалық саясатты жүзеге асыру, яғни ақпараттық ресурстарды ұрлау, жоғалту, жою, жария ету, ағызу, бұрмалау және жалған құрудан қорғау.

6.5 Ақпараттық қауіпсіздікті қамтамасыз ету шеңберінде техникалық саясат мыналарды қарастырады:

6.5.1 қызметкерлердің құпия ақпаратқа қол жеткізуі үшін бірыңғай рұқсат ету жүйесін енгізу;

6.5.2 қызметкерлер мен бөгде адамдардың ақпараттық құпиясы бар құжаттар өңделетін немесе сақталатын ғимараттарға және объектілерге кіруін шектеу;

6.5.3 автоматтандырылған жүйелердегі деректерге пайдаланушылардың қолжетімділігін шектеу;

6.5.4 құжаттарды, ақпараттық массивтерді есепке алу, пайдаланушылар әрекеттерін тіркеу, рұқсатсыз кіру және пайдаланушылар әрекеттерін бақылау;

6.5.5 өңделетін және берілетін ақпаратты криптографиялық түрлендіру;

6.5.6 автоматтандырылған жүйелерге вирусқа қарсы бағдарламалар енгізуді болдырмау.

6.6 Ақпараттық ресурстарды рұқсатсыз қолжетімділіктен қорғау:

6.6.1 автоматтандырылған жүйелерге қызметкерлердің рұқсаттары мен қолжетімділігін тіркеу және тексеру бойынша бірыңғай орталықтандырылған саясат;

6.6.2 қолжетімділіктің негізділігі, яғни қызметкердің ақпаратпен танысу үшін немесе оған қатысты әрекеттер жасау үшін сәйкес рұқсат формасының болуы;

6.6.3 жеке жауапкершілік, яғни қызметкердің өзіне тапсырылған ақпараттың (құжаттардың, ақпарат тасушылардың, ақпараттық массивтердің) қауіпсіздігін сақтауға және автоматтандырылған жүйеде өз әрекеттеріне жауапты болуы;

6.6.4 ақпаратты сақтау сенімділігі, яғни ақпаратты (құжаттарды, ақпарат тасушыларын, ақпараттық массивтерін) рұқсатсыз ашылудан, жоюдан, жалған құрудан немесе бұрмалаудан сақтауды қамтамасыз ету;

6.6.5 құпия құжаттармен және ақпаратпен жұмыс істегенде қызметкерлердің әрекеттерін орталықтандырылған бақылау;

6.6.6 техникалық және бағдарламалық ортаның тұтастығын қамтамасыз ету, яғни ақпаратты өңдеудің тиісті технологиясымен анықталатын бағдарламалық ортаның өзгеріссіздігі және қорғау құралдарының белгіленген функцияларды орындауы.

6.7 Ақпараттық жүйені қорғауды қамтамасыз ету болашақ автоматтандырылған жүйе қалыптасу кезеңінде қажетті қорғау шараларын әзірлеуді талап етеді, бұл сатып алынатын жабдық пен бағдарламалық қамтамасыз ету үшін қауіпсіздік талаптарын ескере отырып техникалық сипаттамаларды дайындауды білдіреді.

6.8 Ақпараттық жүйені құруға тапсырыс беру кезінде тек негізгі функционалдық қызметтер (бухгалтерлік жүйелер, процедураларды автоматтандыру жүйелері, құжат айналымы және т.б.) ғана емес, сонымен қатар жүйенің сенімді жұмыс істеуін және қажетті қауіпсіздік деңгейін қамтамасыз ететін қосымша қызметтер де ескерілуі тиіс. Сонымен қатар, барлық қызметтер мен олар арасындағы байланыс жолдары қорғауды қажет етеді.

6.9 Бірыңғай рұқсат ету жүйесінің, тіркеу және қолжетімділік беру процедураларының тиімділігін қамтамасыз ету, сондай-ақ қолжетімділік негізділігін сақтау, автоматтандырылған жүйелердің барлық пайдаланушылары үшін қолжетімді ақпараттық және бағдарламалық ресурстарды анықтау және қолданылатын бағдарламалық-техникалық құралдар арқылы әртүрлі операцияларды (оқу, жазу, өзгерту, жою, орындау) орындауды талап етеді.

6.10 Ақпаратты сақтау сенімділігін қамтамасыз ету:

6.10.1 құпия ақпарат өңделетін ғимараттарды сақтау үшін сейфтер мен металл

шкафтарын, сондай-ақ қолжетімділікті шектеу мен бақылау құралдарын қолдану;

6.10.2 автоматтандырылған жүйелерде ақпаратты криптографиялық түрлендіруді қолдану.

6.11 Қызметкерлердің әрекеттерін бақылау жүйесі:

6.11.1 құпия құжаттармен және ақпаратпен жұмыс істегенде ұйымдастырушылық шаралар мен техникалық бақылау құралдарын қолдану;

6.11.2 пайдаланушылардың ақпараттық және бағдарламалық ресурстармен әрекеттерін тіркеу (жүйелік аудит құралдарын қолдану), оның ішінде әрекеттердің уақытын, сұраушы мен сұралған ресурстардың идентификаторларын, өзара әрекеттесудің түрін және нәтижесін, сондай-ақ рұқсатсыз қолжетімділік әрекеттерін көрсету;

6.11.3 рұқсатсыз әрекеттер туралы сигнализация.

6.12 Автоматтандырылған жүйелердің тұтастығын қамтамасыз ету бағдарламалық-техникалық құралдар мен ұйымдастырушылық шаралар кешені арқылы жүзеге асырылады.

6.13 Құпия ақпаратты сыртқы байланыс арналарымен беру кезінде оның ұрлануынан, бұрмалануынан және жалған ақпараттан қорғаудың негізгі бағыты — ақпаратты криптографиялық түрлендіру, ал қысқа қашықтықтарда — қорғаулы талшықты-оптикалық байланыс жолдарын қолдану.

6.14 Ақпаратты қорғауда пайдалану қажет криптографиялық құралдармен бірге, берілген ақпараттың құпиялылық деңгейіне сәйкес, жеткілікті күшті қорғанысқа ие деректерді қорғау құралдары мен кілттер жүйесін қолдану.

6.15 Қауіпсіздікті қамтамасыз ету сапасын қамтамасыз ету жүйесінің негізін мемлекеттік басқару органдары бекіткен қауіпсіздік стандарттары мен басқа нормативтік актілер құрайды, олар ақпаратты қорғаудың түрлі бағыттары бойынша талаптарды анықтайды.

6.16 Ақпараттық қауіпсіздік жүйесін қалыптастыру сапасының қажетті деңгейін қамтамасыз ету үшін жүйелердің алдын ала жобалауы мен талдауы, қорғау құралдары мен бақылау талаптарын әзірлеу, ақпараттық ресурстардың қорғалуын бақылау жүргізілуі тиіс.

6.17 Автоматтандырылған жүйелерде аутентификацияның қолданылуы жүйеде қатысушылардың құқықтарын заңды түрде тағайындау және жүйелі процестерді орындауға кепілдік беру мақсатында қажет.

6.18 Аутентификацияның мақсаты — ақпараттық алмасуға қатысушыларды үшінші тұлғалардың араласуынан қорғау үшін өзара сәйкестендіру арқылы ақпаратты қорғау.

7. АҚПАРАТТЫҚ ҚАУІПСІЗДІКТІ ҚАМТАМАСЫЗ ЕТУ ҮШІН ҰЙЫМДАСТЫРЫЛАТЫН ШАРАЛАР

7.1 Ақпараттық ресурстардың қауіпсіздігін қамтамасыз ету міндеттері төмендегі ұйымдастыру әдістерімен шешіледі:

7.1.1 Қызметкерлердің құпия сипаттағы құжаттар мен мәліметтермен жұмыс жасауға рұқсат беру жүйесін әзірлеу және іске асыру;

7.1.2 Құпия ақпаратты (құжаттар, ақпарат тасушылар) сақтау және пайдалану үшін бірыңғай тәртіпті орнату;

7.1.3 Ақпаратты қорғау бойынша жұмыстарды үйлестіру, оны өңдеу және тасымалдау үшін қолданылатын есептеу техникасы мен байланыс жүйелерінің көмегімен.

7.2 ЖОО қызметкерімен жұмыста ақпараттық қауіпсіздікті қамтамасыз ету бойынша негізгі ұйымдастыру шаралары мыналар болып табылады:

7.2.1 Еңбек келісім-шарттарын жасау және қызметкерлерден ақпараттық қауіпсіздікті сақтау режимі мен құпия ақпараттың қауіпсіздігін қамтамасыз ету талаптарын орындауға ерікті келісім алу;

7.2.2 Қызметкерлерге ақпараттық қауіпсіздік саласындағы бастапқы нұсқаулықтарды беру, мерзімді оқу және біліктілігін арттыру.

7.3 Жеке қызметкерлер арасында міндеттерді бөлу жүйесі ақпараттық қауіпсіздіктің жалпы деңгейін айтарлықтай арттыруға ықпал етуі мүмкін. Бұл келесі әдістермен жүзеге асырылады:

7.3.1 Қызметкерлерге қолжетімді деректерді минимизациялау. Әр қызметкер тек өз міндеттерін орындау үшін қажетті деректер өңдеу процестерінің деталдарын ғана білуі тиіс. Ақпарат жинау және өңдеу процесін ұйымдастыру, сондай-ақ бөлмелерді жоспарлау қызметкерлердің жұмысты орындау барысында бір-бірімен байланыстарын барынша азайтуға немесе болдырмауға бағытталуы керек. Әр қызметкер өз жұмысы мен оған қатысты шектеулер туралы толық ақпаратқа ие болып, осы шектеулерді бұзудың салдарын нақты түсінуі тиіс;

7.3.2 Құзыреттерді бөлу және бақылауды қайтадан жүргізу. Деректерді сақтауды қамтамасыз ету бойынша жоғары талаптары бар жүйелерде жауапты жұмыс немесе процесс (мысалы, электронды құжаттың мәртебесін өзгерту) оның қажеттілігі екі қызметкермен расталғаннан кейін ғана орындалады. Уақытша немесе жаңа қабылданған қызметкерлер, сондай-ақ оқуға, тәжірибеге, стажировкаға өтетін қызметкерлер жауапты тапсырмаларды өз бетімен орындамауы тиіс.

7.4 Ақпаратты қорғаудың әкімшілік шаралары мыналарды қамтиды:

7.4.1 Автоматтандырылған жүйенің және қосымша жабдықтың физикалық қауіпсіздігін қамтамасыз ету;

7.4.2 Ақпараттық технологиялар бөлімінің қызметкерлері тарапынан қолжетімділікке және жұмыс режимін орындауға бақылауды ұйымдастыру;

7.4.3 Ақпараттық технологиялар бөлімінің қызметкерлері тарапынан қажетті файлдар көшірмелерін, бағдарламалар кітапханасын, жүйе жабдығын сақтауды қамтамасыз ету шараларының дұрыстығы мен толықтығын тексеру;

7.4.4 Қорғаудың жеке шараларының жұмысын практикалық тексеру: бағдарламалар мен жабдықтарда рұқсатсыз өзгерістердің алдын алу, тасушылардағы файлдармен жасалатын барлық процедураларға бақылау және т. б.;

7.4.5 Қызметкерлер тарапынан орындалған жұмыстардың машиналық және қолмен жазылған протоколдарын тексеру;

7.4.6 Ақпараттық технологиялар орталығының қызметкерлерін деректердің сақталуын қамтамасыз ететін барлық жаңа әзірлемелермен таныстыру.

8. ҚАУІПСІЗДІК ЖҮЙЕСІН ҚҰРУ БАҒДАРЛАМАСЫ

8.1 Саясат ЖОО-ның ақпараттық қауіпсіздік жүйесін құру бағдарламасын қалыптастыру мен іске асыру үшін әдістемелік негіз қызметін атқарады. Жалпы алғанда, ақпараттық қауіпсіздік жүйесінің жұмыс істеуі үшін Саясаттың ережелерін ескере отырып, төмендегі құжаттар әзірленіп, қабылдануы тиіс (қажет болған жағдайда жаңартылып отырады):

8.1.1 Ақпараттық қауіпсіздік қауіптерін жіктеу (талдау);

8.1.2 ЖОО ішіндегі құпия ақпаратқа жатқызылатын мәліметтерге қатысты тәртіпті айқындайтын ішкі құжат;

8.1.3 Құпия ақпаратты құрайтын мәліметтердің тізімі;

8.1.4 Әрбір функционалдық міндет пен оған сәйкес автоматтандырылған жүйе шеңберінде құпия ақпараттың сақталуын қамтамасыз ету тәртібі мен ережелерін реттейтін ұйымдастырушылық-құқықтық құжаттар.

8.2 Ақпараттық қауіпсіздікті қамтамасыз ету саласындағы техникалық саясатты іске асыру үшін төмендегі кешенді іс-шараларды әзірлеу және жүзеге асыру қажет:

8.2.1 Автоматтандырылған жүйелерде ақпаратты техникалық, бағдарламалық және криптографиялық қорғауды қамтамасыз ету шаралары;

8.2.2 Маңызды объектілер мен ғимараттарды қорғау және бақылау құралдары мен жүйелерімен жабдықтау.

8.3 Қауіпсіздік жүйесін құру процесінде қауіпсіздікті қамтамасыз етудің ең маңызды және өзекті бағыттарын, қаржылық ресурстарды ескере отырып, іске асырудың басымдықтарын қарастыру қажет.

8.4 Ақпараттық қауіпсіздіктің оңтайлы деңгейіне жету үшін келесідей шаралар қабылдануы тиіс:

8.4.1 Құпия ақпаратты құрайтын мәліметтерді анықтау тәртібін айқындайтын ішкі құжатқа ие болу және оларды қорғау ұйымын реттейтін талаптарды, сондай-ақ мәліметтерді құпия деп тану рәсімін, қажет болған жағдайда белгіленген тәртіппен оған өзгерістер мен толықтырулар енгізу;

8.4.2 Құпия ақпаратты өңдеудің қабылданған технологиясын, оның ішінде осы мақсатта пайдаланылатын ресурстарды критикалық маңызды деңгейі бойынша санаттау жүйесін тұрақты түрде талдау жүргізу;

8.4.3 Ақпараттың құпиялылығын бұзу қауіп-қатерлерінің толық тізімін анықтау және оларды туындау ықтималдығына қарай типтік бұзушы моделіне сәйкес классификациялау;

8.4.4 Қолданыстағы қорғау шаралары мен құралдарын ескере отырып, құпия ақпараттың қаупін бағалау;

8.4.5 Ақпараттың қауіпсіздігін қамтамасыз ету жүйесін әзірлеу және енгізу (ақпарат қорғау жүйесі), ол қауіп-қатер деңгейін төмендетуге бағытталған, ұйымдастырушылық шаралар мен техникалық құралдарды қамтитын жүйе болып табылады;

8.4.6 Ақпараттық қауіпсіздік саласында ЖОО қызметкерлерінің білімін тұрақты түрде арттырып, біліктілігін жоғарылату жұмыстарын жүргізу;

8.4.7 Ақпаратты қорғаудың қабылданған шараларының тиімділігін және қолайлығын кезең-кезеңімен бақылау.

9. ӨКІЛЕТТІКТЕРДІ БӨЛУ ЖӘНЕ ЖАУАПКЕРШІЛІК

9.1 ЖОО басшылығы ақпараттық қауіпсіздікті қамтамасыз ету үшін барлық бөлімшелердің қызметін үйлестіреді.

9.2 Ақпараттық қауіпсіздік бойынша стратегиялық жоспарлау мәселелерін шешу, сондай-ақ ақпарат қорғау саласындағы төтенше жағдайлар мен инциденттерді бақылау әкімшілік бөліммен бірге Ақпараттық технологиялар орталығы тарапынан жүзеге асырылады.

9.3 Осы саясатты орындау аясында ЖОО бағдарламалық-аппараттық кешеннің жұмыс істеуін және осы саясаттың ережелері мен нормаларын сақтауды тұрақты түрде бақылап, аудит жүргізеді. Аудит Ақпараттық технологиялар орталығының

күштерімен және құралдарымен, әкімшілік бөлімнің жалпы қатысуымен тұрақты негізде жүргізіледі, алдын ала бекітілген жоспар-график бойынша және бақылаушы бөлімшелердің басшылығына есептілікті ұсынумен жүзеге асырылады. Ақпараттық қауіпсіздікке қатысты тәуелсіз аудит ЖОО басшылығының шешімімен және тәуелсіз аудиторлық компанияны тарту арқылы жүргізілуі мүмкін.

9.4 Ақпараттық технологиялар орталығы ақпараттық ресурстардың қауіпсіздігін бақылауды жүзеге асырады, ережелер мен нұсқаулықтарды әзірлейді, ақпарат алмасудың барлық қатысушыларының ақпараттық қауіпсіздік талаптарын сақтауын бақылауға алады. Инциденттерді тергеу ЖОО әкімшілік бөлімінің және Ақпараттық технологиялар орталығының бірлескен күшімен жүргізіледі.

9.5 ЖОО құрылымдық бөлімшелерінің басшылары қызметкерлерді ақпараттық қауіпсіздік талаптарымен таныстыруға жауапты.

9.6 Ақпараттық жүйелер ресурстарының әкімшілері желінің үздіксіз жұмыс істеп тұруын қамтамасыз етеді және қауіпсіздік саясатын жүзеге асыру үшін қажетті техникалық шараларды іске асыруға жауапты.

9.7 Әрбір ақпараттық жүйе пайдаланушысының міндеті – ақпараттық жүйені қауіпсіз пайдалану бойынша ережелер, нұсқаулар мен ұсыныстарды сақтау және ақпараттық ресурстармен жұмыс кезінде барлық күмәнді жағдайлар туралы басшылықты хабардар ету.

9.8 Ақпараттық ресурстарды пайдалану ережелерін және тәртібін сақтамағаны үшін кінәлі тұлғаларға ЖОО-мен және қызметкермен жасалған еңбек шарттарына, сондай-ақ Қазақстан Республикасы заңнамасына және осы Саясатқа сәйкес шаралар қолданылуы мүмкін.

10. САЯСАТТЫ ҚАЙТА ҚАРАУ ТӘРТІБІ, САЯСАТТЫ РЕТТЕЙТІН ҚҰЖАТТАР

10.1 Ақпараттық технологиялар орталығы ақпаратты қорғаудың негізгі принциптері мен бағыттарын, талаптарын жыл сайын қайта қарап отырады. Саясатты қайта қарау ақпараттық қауіпсіздікті бұзу бойынша маңызды инциденттерді анықтау, жаңа осалдықтардың пайда болуы немесе ұйымдық және технологиялық инфрақұрылымдағы өзгерістер әсерінен бастапқы қауіп-қатерді бағалау негізінде жүргізіледі.