Улутстаткомдун
2024-жылдын 12-февралындагы
№13 буйругу менен бекитилген

Кыргыз Республикасынын
Улуттук статистика комитетинин
маалыматтык коопсуздук саясаты

Мазмуну

I. Жалпы жоболор

1. Маалыматтык коопсуздук саясатынын максаты

Кыргыз Республикасынын Улуттук статистика комитетинин (мындан ары – Улуттук статистика комитети) маалыматтык коопсуздук саясаты (мындан ары - "Саясат") маалыматтын коопсуздугун камсыз кылуу системасын аныктайт жана маалыматтык коопсуздук жаатындагы максаттарды жана милдеттерди, Улуттук статистика комитетинде маалыматтын коопсуздук системасын түзүүнүн негизги принциптерин системалаштырылган баяндоону билдирет.

Саясаттын негизги жоболору жана талаптары Улуттук статистика комитетинин бардык түзүмдүк бөлүмдөрү, анын ичинде Улуттук статистика комитетине баш ийген ведомстволук жана аймактык органдар, Улуттук статистика комитетинин бардык кызматкерлери (штаттык, убактылуу, контракт боюнча иштегендер ж.б.), ошондой эле Улуттук статистика комитетинин маалыматтык ресурстарын берүүчүлөр жана керектөөчүлөр катары Улуттук статистика комитетинин баш ийген ведомстволук жана аймактык органдары менен өз ара аракеттенүүнү жүзөгө ашыруучу башка жактар, уюмдар жана мекемелер тарабынан милдеттүү түрдө аткарылат.

2. Маалыматтык коопсуздук саясатынын укуктук негиздери

Ушул Саясаттын укуктук негизин Кыргыз Республикасынын Конституциясы, Кыргыз Республикасынын Жарандык кодекси, Кыргыз Республикасынын Кылмыш-жаза кодекси, Кыргыз Республикасынын Укук бузуулар жөнүндө кодекси, Кыргыз Республикасынын мыйзамдары, Кыргыз Республикасынын Президентинин Жарлыктары, Кыргыз Республикасынын Министрлер Кабинетинин (Өкмөтүнүн) токтомдору, Кыргыз Республикасынын Президентинин Жарлыгы менен жана Министрлер Кабинетинин токтому менен бекитилген маалыматтык коопсуздук чөйрөсүндөгү Кыргыз Республикасынын стратегиялык жана программалык документтери, жана Кыргыз Республикасынын мамлекеттик органдарынын маалыматтык коопсуздук чөйрөсүн жөнгө салуучу башка ченемдик укуктук актылары түзөт.

Саясат Улуттук статистика комитетинде маалыматтык технологияларды өнүктүрүүнүн учурдагы абалын жана келечегин талдоонун, Улуттук статистика комитетинин маалыматтык коопсуздугуна коркунучтарды талдоонун негизинде жана төмөнкү ченемдик укуктук актылардын талаптарына ылайык иштелип чыкты:

1) Кыргыз Республикасынын мыйзамдарына ылайык:

– 2017-жылдын 19-июлундагы №127 "Электрондук башкаруу жөнүндө";

– 1997-жылдын 5-декабрындагы №89 "Маалыматка жетүүнүн кепилдиктери жана эркиндиги жөнүндө";

– 2017-жылдын 15-декабрындагы №210 "Кыргыз Республикасынын мамлекеттик сырларын коргоо жөнүндө";

– 2006-жылдын 28-декабрындагы №213 "Кыргыз Республикасынын мамлекеттик органдарынын жана жергиликтүү өз алдынча башкаруу

органдарынын карамагындагы маалыматтарга жетүү жөнүндө";

– 2019-жылдын 8-июлундагы № 82 "Расмий статистика жөнүндө";

– 2008-жылдын 14-апрелиндеги № 58 "Жеке маалыматтар жөнүндө".

2) Кыргыз Республикасынын Өкмөтүнүн токтомдоруна ылайык;

– 2017-жылдын 21-ноябрындагы № 762 "Мамлекеттик маалыматтык системалардын маалымат базаларында камтылган маалыматтарды коргоо боюнча талаптарды бекитүү жөнүндө";

– 2017-жылдын 21-ноябрындагы № 760 "Жеке маалыматтардын сакталышынын белгиленген деңгээлдерин камсыз кылуучу жеке маалыматтардын маалыматтык системаларында аларды иштетүүдө жеке маалыматтардын коопсуздугун жана корголушун камсыз кылуу боюнча талаптарды бекитүү тууралуу";

– 2019-жылдын 31-декабрындагы № 744 "Мамлекеттик маалыматтык системаларга тиешелүү айрым маселелер жөнүндө".

Саясаттын негизги жоболору төмөнкүлөргө багытталган:

1) Улуттук статистика комитетинде маалыматтык коопсуздук чөйрөсүндө бирдиктүү саясатты түзүүгө;

2) маалыматтык коопсуздук саясатын ишке ашыруу боюнча башкаруу чечимдерин кабыл алууга жана практикалык чараларды иштеп чыгууга, маалыматтык коопсуздуктун коркунучтарынын ар кандай түрлөрүнүн кесепеттерин аныктоого, чагылдырууга жана жоюуга багытталган макулдашылган чараларды иштеп чыгууга;

3) маалыматтык коопсуздуктун талаптарын сактоо менен маалыматтык технологияларды түзүүгө, өнүктүрүү жана пайдалануу боюнча иштерди жүргүзүүдө Улуттук статистика комитетинин түзүмдүк жана аймактык органдарынын ишин координациялоого;

4) Улуттук статистика комитетинин маалыматтык коопсуздугун укуктук, техникалык жана уюштуруучулук жактан камсыздоону өркүндөтүү боюнча сунуштарды иштеп чыгууга.

3. Негизги терминдер жана аныктамалар

Административдик маалыматтар – Кыргыз Республикасынын мыйзамдарына ылайык мамлекеттик органдардын жана жергиликтүү өз алдынча башкаруу органдарынын компетенциясына таандык милдеттерди жана иш-милдеттерди аткаруу максатында алар тарабынан чогултулуучу маалыматтар;

Маалыматтык системага (тутумга) кол салуу – системанын аялуу жерлерин пайдалануу аркылуу коркунучтун ишке ашырууга алып келген бузуучу тарабынан аткарылган ар кандай аракеттер;

Маалыматтык мамилелердин субъекттеринин коопсуздугу - маалыматтык мамилелердин субъекттеринин маанилүү кызыкчылыктарын маалыматка жана/же аны иштетүү жана берүү каражаттарына таасир этүү жолу менен аларга материалдык, моралдык же башка зыян келтирүүдөн коргоо;

Маалыматтык коопсуздуктун ички аудити - электрондук башкаруунун мамлекеттик инфраструктурасынын элементтеринин маалыматтык коопсуздугунун учурдагы абалынын сапаттык жана сандык мүнөздөмөлөрүн

контролдоонун объективдүү, документтештирилген процесси, ал уюмдун өзү (маалыматтык системанын ээси/оператору) тарабынан өзүнүн кызыкчылыгында жүзөгө ашырылат;

Зыяндуу программалар – маалыматты уруксатсыз жок кылууга, бөгөт коюуга, өзгөртүүгө же көчүрүүгө же иштин үзгүлтүккө учурашына алып келген маалыматташтыруу объектинин программалары же өзгөртүлгөн программалары;

Документ – аныктоого мүмкүндүк берген маалыматтарды камтыган көрүнүктүү түзмөктөрдө жазылган маалымат;

Маалыматка жетүү – маалымат менен таанышуу же анын укуктук режими менен жөнгө салынган, анын талаптарынын так сакталышын аныктоо менен аны иштетүү мүмкүнчүлүгүн алуу;

Ресурска жеткиликтүүлүк - субъекти ошол ресурсту манипуляциялоо (колдонуу, башкаруу, өзгөчөлүктөрүн өзгөртүү ж.б.) мүмкүнчүлүгүн алуусу;

Маалыматка жеткиликтүүлүк – маалымат жүгүртүлүүчү системанын эң маанилүү мүлкү (маалыматты иштетүү каражаттары жана технологиялары), бул үчүн тиешелүү ыйгарым укуктарга ээ субъекттердин маалыматка өз убагында жана тоскоолдуксуз жеткиликтүүлүгүн камсыз кылуу мүмкүнчүлүгү менен өзгөчөлөнөт;

Табигый коркунучтар маалымат системасына жана анын адам тарабынан жасалган табияттын объективдүү физикалык процесстеринин компоненттерине же адамдын көзөмөлүнөн тышкаркы табигый кубулуштарга тийгизген таасиринен келип чыккан коркунучтар;

Окуяларды журналга түшүрүү - болуп жаткан программалык же аппараттык окуялар жөнүндө маалыматты окуяларды каттоонун электрондук журналына жазуу процесси;

Маалыматты коргоо – корголуучу маалыматтын сыртка чыгып кетүүсүн, маалыматка уруксатсыз жана байкоосуз таасир этүүнү болтурбоо боюнча иш-аракеттер;

Маалыматтарды уруксатсыз жеткиликтүүлүктөн коргоо – бул юридикалык документтерде белгиленген корголгон маалыматка укуктарды же жеткиликтүүлүк эрежелерин бузуп, кызыкдар субъект тарабынан корголгон маалыматты алууга жол бербөө боюнча иш-чаралар;

Кылмышкер – өзүмчүл, идеологиялык же башка мотивдерден атайылап иш-аракет кылган тартип бузуучу;

Идентификатор - статистикалык бирдиктердин аты/аталышы, так географиялык жайгашуусу же идентификациялык номери боюнча так идентификациялоого мүмкүндүк берүүчү символдордун ырааттуулугу;

Жеке маалыматтар - расмий статистиканы иштеп чыгууда, жүргүзүүдө жана жайылтууда колдонулган статистикалык бирдиктер жөнүндө деталдаштырылган маалыматтар;

Маалымат – объектилер, фактылар, окуялар, кубулуштар жана процесстер жөнүндө маалымат, алардын берүү формасына карабастан;

Жеке мүнөздөгү маалыматтар (жеке маалыматтар) - конкреттүү адам жөнүндө материалдык сактоочулар жазылган маалымат, ал конкреттүү адам менен окшоштурулат же окшоштурулушу мүмкүн, ушул адамды түз же кыйыр

анын биологиялык, экономикалык, маданий, жарандык же социалдык түрдүүлүгү үчүн анын биологиялык, экономикалык, маданий, жарандык же социалдык идентификация үчүн мүнөздүү болгон бир же бир нече факторлорго шилтеме жасоо жолу менен идентификациялоого мүмкүндүк берет;

Маалыматтык коопсуздук (киберкоопсуздук) – мүмкүнчүлүктөрдүн, стратегиялардын, коопсуздук принциптеринин, коопсуздук кепилдиктеринин, тобокелдиктерди башкаруу жана камсыздандыруу ыкмаларынын, кесиптик даярдыктын, практикалык тажрыйбанын жана технологиялардын жыйындысын пайдалануу менен камсыз кылынган маалыматтык инфраструктуранын объектилериндеги маалыматтын бүтүндүк (аныктыгын жана каталарга чыдамдуулугун камтышы мүмкүн), жеткиликтүүлүк жана купуялуулук касиеттерин сактоо;

Маалымат ресурстары – айрым жеке документтер, документтердин массивдери, маалыматтык системалардагы маалымат базалары;

Маалымат чөйрөсү – маалыматтардын, маалыматтык инфраструктуранын, субъекттердин топтому (жыйындысы), маалыматты чогултууну, түзүүнү, жайылтууну жана пайдалануунуу жүзөгө ашыруучу, ошондой эле бул процессте пайда болгон мамилелерди жөнгө салуучу системасы;

Маалыматтык системасы – документтердин (документтердин массивдеринин), маалыматтар базасынын, алардын берилген формасына жана маалыматтык технологияларга карабастан, анын ичинде компьютердик техникасын жана байланышты пайдалануу менен уюштуруу жагынан тартипке келтирилген жыйындысы;

Маалымат таратуу каналы корголгон маалыматка ээ болгон адамдардын уюмунан же чөйрөсүнөн тышкаркы маалымат булагынан көзөмөлсүз физикалык жол болуп саналат, ал аркылуу каракчы тарабынан корголгон маалыматты мыйзамсыз (уруксатсыз) ээлөө мүмкүн;

Өтө маанилүү жабдуулар – ишиндеги үзгүлтүктөрү же иштебей калышы, Улуттук статистика комитетинин, ага баш ийген ведомстволук же аймактык органдарынын маалыматтык системанын ээсинин жана/же операторунун ыйгарым укуктарын жүзөгө ашыруучу үчүн олуттуу мааниге ээ болгон жана аларга жүктөлгөн функцияларды аткаруунун (токтотууга) мүмкүн эместигине алып келүүчү жабдуулар;

Маалыматтын жашыруундугу – маалыматка жетүү укугуна ээ болгон субъекттердин чөйрөсүнө чектөөлөрдү киргизүү зарылдыгын көрсөткөн жана системанын (чөйрөнүн) аталган маалыматты ага жетүү укугуна ыйгарым укугу жок субъекттерден жашыруун сактоо жөндөмдүүлүгү менен камсыз кылынган маалыматка субъективдүү аныкталуучу (ыйгарылуучу) мүнөздөмө;

Корпоративдик маалымат системасы бири-бири менен байланышы бар компоненттердин топтому болуп эсептелген уюштуруу-техникалык система болуп саналат: маалыматтарды иштетүүнүн жана берүүнүн техникалык түзмөктөрү, маалымат керектөөчүлөрдүн маалымат муктаждыктарын канааттандыруу максатында маалыматтарды автоматташтырылган иштетүүнү аткаруу үчүн уюштуруу, түзүмдүк, тематикалык, технологиялык же башка өзгөчөлүктөр менен бириккен ар кандай маалымат түзмөктөрү, кызматкерлер жана пайдалануучулар боюнча тиешелүү программалык камсыздоо,

маалыматтардын массивдери (маалымат базалары) түрүндөгү иштетүү ыкмалары жана алгоритмдери;

Маалымат коргоо тармагындагы лицензия – маалыматты коргоо тармагында белгилүү бир иштерди жүргүзүү укугуна уруксат;

Метамаалыматтар - маалымат булактары, маалыматтардын усулдары, аныктамалары, классификациялары жана сапаты тууралуу маалыматтарды берүү жолу менен статистикалык маалыматтарды жана статистикалык процесстерди стандартташтырылган түрдө чагылдырган маалыматтар жана башка документтер;

Уруксатсыз иш-аракеттер – бул системада белгиленген маалыматты иштетүү эрежелерин бузган субъекттин иш-аракеттери;

Уруксатсыз жеткиликтүүлүк – субъекттин маалыматка, объектке жеткиликтүүлүгү, анын укуктук режиминин талаптарын, жеткиликтүүлүктү эрежелерин бузуу менен кирүү;

Объект – системанын пассивдүү компоненти, маалыматтык системанын ресурсунун бирдиги, ага жеткиликтүүлүк мүмкүндүктү чектөө эрежелери менен жөнгө салынат;

Коргоо объекти - маалыматты коргоонун белгиленген максатына ылайык коргоону камсыз кылуу зарыл болгон маалымат же маалымат сактагыч же маалымат процесси;

Уюштуруучу коргоо чаралары – бул маалыматтарды иштетүү системасынын иштешинин процесстерин жөнгө салуучу чаралар, анын ресурстарын пайдалануу, персоналдын ишмердүүлүгү, ошондой эле пайдалануучулардын система менен өз ара иштешүү тартиби, ошондой эле пайдалануучулардын система менен өз ара иштешүүсүн эң кыйындатуу же коопсуздук коркунучтарынын жана анда таралып жаткан маалыматтын мүмкүндүгүн жоюу үчүн жөнгө салуучу чаралар;

Пароль (сырсөз) – адамдардын тар чөйрөсүнө (бир адамга) белгилүү деп эсептелген жана маалыматка, имаратка, аймакка жеткиликтүүлүктү чектөө коюу үчүн колдонулуучу кызматтык сөз;

Пайдалануучу – маалыматка жеткиликтүүлүктүн белгиленген укуктарына жана эрежелерине ылайык анын менчик ээсинен же ортомчусунан алынган маалыматарды пайдалануучу субъект;

Административдик маалыматтарды жеткирип берүүчүлөр - административдик максаттарда чогулган маалыматтарды расмий статистиканы жүргүзүүчүлөргө берүүчү мамлекеттик органдар жана жергиликтүү өз алдынча башкаруу органдары;

Өндүрүш - расмий статистиканы түзүү максатында маалыматтарды топтоо, иштетүү, талдоо жана сактоо менен байланышкан иштин бардык түрлөрү;

Иштеп чыгуу – расмий статистиканы жүргүзүү жана жайылтуу үчүн пайдалануучу статистикалык усулдарды, концепцияларды, стандарттарды жана жол-жоболорду түзүү, күчтөндүрүү жана өркүндөтүү боюнча иш;

Жумушчу станция - колдонмо маселелерди чечүүгө арналган локалдык тармактын курамындагы стационардык же портативдүү компьютер;

Жеткиликтүүлүктү чектөө – субъекттердин белгилүү бир системадагы объекттерге жеткиликтүүлүк укуктарын жөнгө салуучу эрежелердин

жыйындысы;

Ресурстарга жетүүнү чектөө – системалык ресурстарды пайдалануунун тартиби, мында субъекттер белгиленген эрежелерди так сактоо менен объекттерге жетүү мүмкүнчүлүгүнө ээ болушат;

Жашыруун маалымат – компьютер жана байланыш объектилеринде, телекоммуникацияларда, ошондой эле расмий жана мамлекеттик сырлар катары эсептелген маалыматтарды камтыган башка маалыматтык ресурстар, маалыматтык-акустикалык жана электр сигналдары, физикалык талаалар, материалдык маалымат сактагычтар, маалымат массивдери жана маалымат базалары түрүндөгү маалыматтык ресурстар;

Сервердик жай - сервердик, активдүү жана пассивдүү тармактык (телекоммуникациялык) жабдууну жана түзүмдөштүрүлгөн кабелдик системалардын жабдууларын жайгаштырууга арналган жай;

Маалыматтык коопсуздук системасы – маалыматтык коопсуздугун камсыз кылуу үчүн арналган укуктук (мыйзамдык) жана административдик мүнөздөгү атайын чаралардын, уюштуруу иш-чараларынын, коргоонун физикалык жана техникалык (программалык жана аппараттык) түзмөктөрүн жана Улуттук статистика комитетинин атайын персоналдын жыйындысы (комплекси).

Криптографиялык маалыматты коргоо түзмөктөрү - криптографиялык кайра түзүү алгоритмдерин, шифрлөө ачкычтарын түзүүнү, калыптандырууну, бөлүштүрүүнү же башкарууну ишке ашыруучу программалык камсыздоо же аппараттык-программалык комплекси;

Маалыматтык коопсуздук куралы – техникалык, программалык камсыздоо, затты жана/же маалыматты коргоо үчүн иштелип чыккан же колдонулган материал;

Субъект – системанын активдүү компоненти (пайдалануучу, процесс, программа), анын иш-аракеттери жеткиликтүүлүктү чектөө эрежелери менен жөнгө салынат;

Маалыматтык мамилелердин субъекттери – мамлекеттик органдар, мамлекет, мамлекеттик, коомдук же коммерциялык уюмдар (ассоциациялар) жана ишканалар (юридикалык жактар), жеке жарандар (жеке жактар) жана маалыматты биргелешип иштетүү максатында өз ара аракеттенген башка субъекттер;

Жеке маалыматтар субъекти (субъект) - тиешелүү жеке маалыматтар таандык болгон адам;

Техникалык (аппараттык жана программалык) коргоо түзмөктөрү – маалыматты коргоо функцияларын (өз алдынча же башка түзмөктөрү менен айкалыштырган) ар кандай электрондук түзмөктөрү жана атайын программалар (пайдалануучуларды аныктоо жана аутентификациялоо, ресурстарга жеткиликтүүлүктү чектөө, окуяларды каттоо, маалыматты криптографиялык жабуу ж.б.);

Кибер коопсуздук боюнча техникалык документтер - мамлекеттик маалыматтык системалардын базасында камтылган маалыматтын бүтүндүгүн (анын ичинде аутенттүүлүгүн жана айныбастыгын), жеткиликтүүлүгүн жана купуялуулугун камсыз кылуу процесстери менен байланышкан саясатты,

эрежелерди, коргоо чараларын белгилөөчү документтер;

Коркунуч – объектинин иштөө режиминин атайылап же кокусунан (байкабастан) бузулушу жана корголгон маалыматтын же объектинин башка ресурстарынын касиеттерин бузуу максатында кооптуу таасир тийгизүүчү факторлорду ишке ашыруу боюнча реалдуу же потенциалдуу мүмкүн болгон иш-аракеттер;

Маалыматтык коопсуздукка коркунуч – бул маалымат ээсине же пайдалануучусуна зыян келтирген жашыруундуктун, актыктын, маалыматтын болушунун, ошондой эле анын мыйзамсыз кайталанышынын бузулушуна алып келиши мүмкүн болгон потенциалдуу окуя, иш-аракет, процесс же кубулуш;

Маалыматтын аялуулугу – анын жашыруундугунун, бүтүндүгүн, жеткиликтүүлүгүн бузууга же анын мыйзамсыз көбөйтүүгө алып келиши мүмкүн болгон ар кандай туруксуздаштыруучу факторлордун таасирине кабылышы;

Физикалык коргоо чаралары – маалыматтык системанын корголгон маалыматына жана башка ресурстарына потенциалдуу бузуучулардын кирүү жана кирүү жолдорунда физикалык тоскоолдуктарды түзүү үчүн атайын иштелип чыккан механикалык, электр же электрондук-механикалык түзүлүштөрдүн жана түзүлүштөрдүн ар кандай түрлөрү, ошондой эле техникалык визуалдык байкоо жана байланыш жана коопсуздук сигнализациясынын түзмөктөрү;

Маалыматтын бүтүндүгү – маалыматтын анын бузулбаган формада, бурмаланбаган түрдө (айрым туруктуу абалга карата өзгөрүүсүз) болушунан турган касиети;

Маалыматты коргоонун максаты – маалыматтык системанын компоненттерине жагымсыз таасир этүүнүн, ошондой эле маалыматты ачыкка чыгаруунун (агып кетүүнүн), бурмалоонун (модификациялоонун), жоготуунун (жеткиликтүүлүк деңгээлин төмөндөтүүнүн) же мыйзамсыз нускалоонун жардамы менен маалыматтык мамилелердин субъекттерине келтирилген зыяндын (тикелей же кыйыр, материалдык, моралдык же башка) алдын алуу же азайтуу.

II. Улуттук статистика комитетинин маалыматтык коопсуздук системасын түзүүнүн негизги принциптери, максаттары жана милдеттери

4. Улуттук статистика комитетинин маалыматтык коопсуздук системасын түзүүнүн негизги принциптери

Маалыматтык коопсуздук саясаты системасы маалыматтык коопсуздукту камсыз кылуунун комплекстүү системаларын түзүүнүн негизги принциптерин, маалыматтык коопсуздукка коркунучтарды коргоо жана ага каршы туруу үчүн уюштуруу-техникалык методдордун жана заманбап аппараттык жана программалык каражаттардын өзгөчөлүктөрүн жана мүмкүнчүлүктөрүн эске алуу менен түзүлгөн.

Маалыматтык коопсуздукту камсыз кылуунун натыйжалуу системасы маалыматтын кыймылы жана белгиленген ченемдик талаптардын сакталышы

менен байланышкан процесстердин учурдагы абалы жөнүндө адекваттуу жана ар тараптуу маалыматтын, ошондой эле чечим кабыл алууга тиешелүү кошумча маалыматтын болушун талап кылат.

Улуттук статистика комитетинин маалыматтык коопсуздук системасын түзүү жана анын иштеши төмөнкү негизги принциптерге ылайык жүзөгө ашырылууга тийиш:

1) мыйзамдуулук принциби, ал төмөнкүлөрдү болжолдойт:

– электрондук башкаруу, мамлекеттик маалыматтык системалардын маалыматтык коопсуздугун камсыз кылуу жаатындагы колдонуудагы мыйзамдарга, ошондой эле маалыматтык коопсуздук боюнча башка ченемдик укуктук актыларга ылайык Улуттук статистика комитетинин коргоо чараларын жүзөгө ашыруу жана маалыматтык коопсуздук системасын иштеп чыгуу;

– Улуттук статистика комитетинин маалыматтык коопсуздук системасын өз компетенциясынын чегинде, маалымат менен иштөөдө укук бузууларды табуунун жана бөгөт коюунун уруксат берилген методдорун колдонуу менен түзүү жана башкаруу;

2) ырааттуулук принциби – Улуттук статистика комитетинде маалыматтык коопсуздукту камсыз кылуу көйгөйөүн түшүнүү жана чечүү үчүн маанилүү болгон өз ара байланышкан, өз ара аракеттенүүчү жана убакыттын өтүшү менен өзгөрүп туруучу элементтерди, шарттарды жана факторлорду эске алуу менен Улуттук статистика комитетинде маалыматты коргоо системасын түзүүгө системалуу мамилени билдирет.

Коргоо тутумун түзүүдө Улуттук статистикалык комитетинин маалымат системанын бардык кыйла аялуу жерлери, ошондой эле укук бузуучулардан (өзгөчө квалификациялуу чабуулчулардан) келип чыгуучу коркунучтардын мүнөзү, мүмкүн болгон объекттери жана багыттары, бөлүштүрүлгөн системаларга кирүү жолдору жана маалыматка уруксатсыз кирүү жолдору эске алынууга тийиш;

3) комплекстүүлүк принциби маалыматтык системаларды коргоо ыкмаларын жана каражаттарын комплекстүү пайдалануу жана коркунучтарды ишке ашыруунун бардык олуттуу (маанилүү) мүмкүнчүлүктөрүн жабуучу жана анын айрым компоненттеринин бириккен жерлеринде алсыз жерлерди камтыбаган коргонуунун бүтүн системасын түзүүнү билдирет;

4) үзгүлтүксүздүк принциби, Улуттук статистика комитетинин жетекчилигинен баштап, маалыматтык коопсуздукту камсыз кылуу бөлүмдөрүнө чейин, Улуттук статистика комитетинин баш ийген ведомстволук жана аймактык органдары тарабынан Улуттук статистика комитетинин бардык деңгээлдеринде туруктуу жүзөгө ашырылуучу маалыматтык коопсуздукту камсыз кылуу боюнча ишти болжолдойт жана бул процессте Улуттук статистика комитетинин ар бир кызматкеринин катышуусун билдирет;

5) ***өз убагында болуу принциби*** маалыматтын коопсуздугун камсыз кылуу чараларынын алдын алуучу мүнөзүн, башкача айтканда, маалыматты комплекстүү коргоо боюнча милдеттерди коюуну жана жалпысынан маалыматтык системаларды жана алардын маалыматты коргоо системаларын иштеп чыгуунун алгачкы стадияларында маалыматтык коопсуздукту камсыз кылуу чараларын ишке ашырууну билдирет;

6) ***өркүндөтүүнүн үзгүлтүксүздүгү принциби,*** уюштуруу жана техникалык чечимдердин, кадрдык курамдын улануучулугунун негизинде маалыматты коргоо чараларын жана каражаттарын, Улуттук статистика комитетинин маалыматтык системасынын жана аны коргоо системасынын иштешин талдоонун негизинде, маалыматты коргоо чараларындагы жана каражаттарындагы, коргоо боюнча ченемдик талаптардагы өзгөрүүлөрдү, бул жааттагы алдыңкы технологияларды жана тажрыйбаны эске алуу менен дайыма өркүндөтүүнү билдирет;

7) ***акылга сыярлык жетиштүүлүк*** *(экономикалык максатка ылайыктуулук)* ***принциби***, маалыматтын коопсуздугун камсыз кылууга сарптоолордун деңгээлинин маалыматтык ресурстардын баалуулугуна жана аларды ачыкка чыгаруудан, жоготуудан, агып кетүүдөн, жок кылуудан жана бурмалоодон келип чыгышы мүмкүн болгон зыяндын чоңдугуна ылайык келишин билдирет;

8) ***жеке жоопкерчилик принциби***, маалыматтык коопсуздукту жана маалыматты иштеп чыгуу тутумун камсыз кылуу үчүн жоопкерчиликти ар бир кызматкерге өзүнүн ыйгарым укуктарынын чегинде жүктөөнү билдирет;

9) ***ыйгарым укуктарды минималдаштыруу принциби,*** бул кызматкерге анын кызматтык милдеттерин аткаруу үчүн зарыл болгон учурда жана көлөмдө гана пайдалануучуларга кызматтык зарылчылыкка ылайык кирүүгө минималдуу укуктарды берүүнү билдирет;

10) ***статистикалык купуялуулук принциби*** төмөнкү маалыматтарга карата колдонулат:

– бирден үч бирдиктен турган жыйынды көрсөткүчтөр, мында бирдик жеке, юридикалык жакты же үй чарбасын билдирет, эгерде бул бирдиктердин бири кыйыр түрдө идентификацияланса; өзгөчө учурларда үчтөн ашык бирдиктен турган агрегаттык көрсөткүчтөр, эгерде бул бирдиктердин бири кыйыр түрдө идентификацияланышы мүмкүн болсо, Улуттук статистика комитетинин төрагасы тарабынан жашыруун деп жарыяланышы мүмкүн;

– Кыргыз Республикасынын мамлекеттик сырларды же банк иши чөйрөсүндөгү мыйзамдарына ылайык мамлекеттик сыр же банктык сыр деп жарыяланган маалыматтар;

11) ***кызыкчылыктардын кагылышын четтетүү принциби*** кызматкерлердин милдеттерин так бөлүштүрүүнү жана кызматкерлердин жоопкерчилигинин чөйрөсү кызыкчылыктардын кагылышына жол берген жагдайларды четтетүүнү болжолдойт;

12) ***өз ара аракеттенүү жана кызматташуу принциби***, ал Улуттук статистика комитетинде жагымдуу атмосфераны түзүүнү билдирген өз ара аракеттенүү жана кызматташуу принциби, анда кызматкерлер маалыматтык коопсуздукту камсыз кылуу процессиндеги өз ролун түшүнүшөт жана бул процесске катышышат, ошол эле учурда маалымат менен иштөөнүн жогорку маданиятына ээ болушат жана белгиленген эрежелерди аң-сезим менен сакташат жана маалыматтык коопсуздукту камсыз кылуу бөлүмүнүн ишине көмөк көрсөтүшөт;

13) тутумунун ***коргоо тутумунун ийкемдүүлүк принциби,*** маалыматтык

коопсуздук тышкы чөйрөнүн жана Улуттук статистика комитетинин ички шарттарынын өзгөрүүсүнө жооп берүү жөндөмдүүлүгүн камсыз кылат, алар төмөнкүлөрдү камтыйт:

– Улуттук статистика комитетинин уюштуруу жана штаттык түзүмүн өзгөртүү;

– корпоративдик реструктуризациялоо, биригүү жана кошулуу;

– колдонуудагы маалыматтык системаларды өзгөртүү же принципиалдуу түрдө жаңысын киргизүү;

– жаңы техникалык каражаттар;

– иштин жаңы түрлөрү; жаңы кызматтар, буюмдар.

14) алгоритмдердин жана коргоо механизмдеринин ачыктык принциби, коргоо түзүмдүк уюштуруунун жана анын подсистемаларынын иштөө алгоритмдеринин жашыруундуулугунун эсебинен гана камсыз кылынбашы керек экендигинен турат;

15) ***коргоо куралдарын колдонуунун жөнөкөйлүгү принциби*** коргоо механизмдери жана ыкмалары интуитивдик жана колдонууга оңой болушу керек дегенди билдирет;

16) ***негиздүүлүк жана техникалык ишке ашыруу принциби*** маалыматтык технологиялардын, техникалык жана программалык камсыздоонун, маалыматты коргоонун каражаттары менен чараларынын заманбап алдыңкы технологиялардын деңгээлинде ишке ашырылышы, маалыматтык коопсуздуктун жана экономикалык максатка ылайыктуулуктун белгиленген деңгээлине жетүү көз карашынан негиздүү болушу, ошондой эле маалыматтык коопсуздук боюнча белгиленген ченемдерге жана талаптарга ылайык келиши керек дегенди билдирет;

17) ***маалыматтык ресурстардын коопсуздугун камсыз кылуу*** боюнча иштин конкреттүү түрүнө кыйла даярдалган, практикалык иш тажрыйбасы жана бул жаатта кызмат көрсөтүү укугуна лицензиясы бар адистештирилген уюмдарды маалыматты коргоо чараларын иштеп чыгууга жана ишке ашырууга тартууну камтыган адистештирүү жана кесипкөйлүк;

18) ***милдеттүү көзөмөлдөө,*** белгиленген эрежелерди бузуу аракеттерин милдеттүү жана өз убагында аныктоону жана бөгөт коюуну, маалыматтык коопсуздукту камсыз кылуунун колдонулган системаларынын жана түзмөктүрүнүн негизинде, бул системалардын жана түзмөктүрдүн натыйжалуулугун баалоо критерийлерин жана ыкмаларын өркүндөтүүнү билдирет.

Улуттук статистика комитетинин ыйгарым укуктуу кызматкерлери же Улуттук статистика комитетинин маалыматтык коопсуздугун камсыз кылуу боюнча жооптуу бөлүм (адам) тарабынан аныкталган маалыматтык коопсуздук системадагы кемчиликтер тиешелүү деңгээлдеги жетекчилерге токтоосуз маалымдалып, өз убагында, ыкчам четтетилиши керек.

Улуттук статистика комитетинин жетекчилиги маалыматтык коопсуздук системасында аныкталган бардык көйгөйлөрдүн жыйынтыктаган отчетторун мезгил-мезгили менен алып турушу керек.

5. Маалыматтык коопсуздукту камсыз кылуу системасынын негизги максаттары жана милдеттери

Улуттук статистика комитетинин маалыматтык коопсуздук системасы маалыматты иштеп чыгуу жана сактоо учурунда, байланыш каналдары боюнча маалыматтарды берүүдө, жеткиликтүүлүгү чектелген маалыматтарды ачыкка чыгаруучу жашыруун сүйлөшүүлөрдү жүргүзүүдө, техникалык жана программалык каражаттарды пайдаланууда маалыматты коргоо боюнча уюштуруучулук, программалык жана техникалык каражаттардын жана чаралардын комплексин карайт.

Улуттук статистика комитетинин маалыматтык коопсуздук системасынын негизги максаттары болуп төмөнкүлөрдү камсыз кылуу саналат:

1) Улуттук статистика комитетинин маалыматтык мамилелеринин объектилерин жана субъекттерин маалыматка, аны алып жүрүүчүлөргө, кайра иштетүү жана берүү процесстерине кокустан же атайылап таасир этүү аркылуу аларга мүмкүн болуучу материалдык, физикалык, моралдык же башка зыян келтирүүдөн коргоо;

2) маалыматтык ресурстарды уурдоодон, жоготуудан, агып кетүүдөн, жок кылуудан, бурмалоодон же уруксатсыз кирүүдөн жана өзгөчө таасирлерден коргоо;

3) оперативдүү жана башка тобокелдиктердин деңгээлин (Улуттук статистика комитетинин аброюна шек келтирүүчү тобокелдиктер, укуктук тобокелдиктер ж.б.) минималдаштыруу аркылуу маалыматты иштеп чыгууда, сактоодо жана байланыш каналдары боюнча берүүдө техникалык каналдар аркылуу агып кетүүдөн коргоо.

Маалыматтын көрсөтүлгөн касиеттерин коргоонун жана камсыз кылуунун негизги максатына жетүү үчүн Улуттук статистика комитетинин маалыматтык коопсуздук системасы төмөнкү милдеттерди натыйжалуу чечүүнү камсыз кылууга тийиш:

– маалыматтык коопсуздукка коркунучтардын булактарын, маалыматтык мамилелердин кызыкдар субъекттерине зыян келтирүүгө, Улуттук статистикалык комитеттин маалымат системасынын түзүк иштешин бузууга көмөктөшүүчү себептерди жана шарттарды өз убагында аныктоо, баалоо жана болжолдоо;

– жашыруун иштер жүргүзүлүп жаткан имараттарга жана жайларга жана маалымат иштетилүүчү (сакталган, берилүүчү) маалымат-коммуникациялык түзүлүштөргө, ошондой эле түздөн-түз маалымат жана байланыш түзмөктөрүнүн өзүнө кирүүнү чектөө;

– маалыматтык коопсуздукка коркунучтарга жана терс тенденцияларга ыкчам жооп кайтаруу механизмин түзүү;

– жеке жана юридикалык жактардын укукка каршы аракеттеринен келтирилген зыянды азайтуу жана локалдаштыруу үчүн шарттарды түзүү, маалыматтык коопсуздукту бузуунун терс таасирин азайтуу жана кесепеттерин жоюу;

– Улуттук статистика комитетинин маалымат системасынын иштөө

процессине ыйгарым укуксуз адамдардын кийлигишүүсүнөн коргоо максатында аткаруучулардын (пайдалануучулардын, Улуттук статистика комитетинин кызматкерлеринин) ишке, документтерге жана маалыматтарга кирүүсүнө уруксат берүү системасын ишке ашыруу;

– Улуттук статистика комитетинин маалыматына, техникалык каражаттарына, программалык камсыздоосуна жана башка ресурстарына пайдалануучулардын жеткиликтүүлүгүн дифференциациялоо, чектөө (бул ресурстарга гана жетүү жана алар менен конкреттүү пайдалануучулар өздөрүнүн кызматтык милдеттерин аткаруу үчүн зарыл болгон операцияларды гана жүргүзүү мүмкүнчүлүгү);

– маалымат алмашууга катышкан пайдалануучулардын аутентификациясын камсыз кылуу (маалыматты жөнөтүүчү менен алуучунун аныктыгын тастыктоо);

– системаны уруксатсыз программаларды, анын ичинде зыяндуу программаларды киргизүүдөн коргоо;

– документтерди, маалымат массивдерин эсепке алуу, пайдалануучулардын, Улуттук статистика комитетинин кызматкерлеринин аракеттерин каттоо, колдонуучулардын, Улуттук статистика комитетинин кызматкерлеринин жана уруксаты жок адамдардын уруксатсыз кирүүсүн жана аракеттерин көзөмөлдөө;

– ачык ачкыч инфраструктурасын ишке ашыруу, ачык байланыш каналдары боюнча компьютердик технологиялар менен иштетилген жана берилүүчү чектелген маалыматты криптографиялык коргоо;

– документтерди жана компьютердик сактагычтарды, ачкычтарды (негизги документтерди) ишенимдүү сактоо жана алардын жүгүртүүсүн, уурдоону, алмаштырууну жана жок кылууну болтурбоо, коопсуз сактоо, ошондой эле байланыш каналдары боюнча кайра иштетүү, сактоо жана берүү учурунда чектелген маалыматты техникалык каналдар аркылуу агып кетүүдөн коргоону камсыз кылуу.

III. Маалыматтык мамилелердин негизги субъекттери жана объекттери

6. Улуттук статистика комитетинин маалыматтык мамилелеринин негизги субъекттери

Улуттук статистика комитетинин маалыматтык коопсуздугун камсыз кылууда маалыматтык мамилелердин субъекттери болуп төмөнкүлөр саналат:

1) маалыматтык ресурстардын менчик ээси катары Улуттук статистика комитети;

2) Улуттук статистика комитетинин маалыматтык коопсуздугун камсыз кылууга жооптуу бөлүм (адам);

3) маалымат алмашууга катышкан борбордук аппараттын бөлүмдөрү, Улуттук статистика комитетинин баш ийген ведомстволук жана аймактык органдары;

4) Улуттук статистика комитетинин борбордук аппаратынын, баш ийген

ведомстволук жана аймактык органдарынын жетекчилиги жана кызматкерлери, аларга жүктөлгөн функцияларга жана ыйгарым укуктарга ылайык;

5) юридикалык жана жеке жактар, үй чарбалары, алар жөнүндө маалыматтар Улуттук статистика комитетинин маалыматтык системасында топтолот, сакталат жана иштетилет;

6) Улуттук статистика комитетинин өз функцияларын аткаруусун камсыз кылууга тартылган башка юридикалык жана жеке жактар (консультанттар, иштеп чыгуучулар, кызмат көрсөтүү үчүн тартылган уюмдар ж.б.).

7. Коргоо объектилери

Улуттук статистика комитетинин маалыматтык коопсуздук системасынын негизги объекттери болуп төмөнкүлөр саналат:

– жеткиликтүүлүгү чектелген маалыматтык ресурстар, баштапкы маалымат базалары, кокусунан жана уруксатсыз таасирлерге жана алардын коопсуздугунун бузулушуна сезгич болгон башка маалыматтык ресурстар, ошондой эле формасына жана түрүнө карабастан Улуттук статистика комитетинин иши үчүн зарыл болгон аны берүү формасына жана түрүнө карабастан купуя маалыматтары бар статистикалык база;

– Улуттук статистика комитетинин маалыматтык системасында маалыматты иштеп чыгуу процесстери, маалыматтык технологиялар, регламенттер жана маалыматты чогултуу, иштеп чыгуу, сактоо жана берүү жол-жоболору, системанын маалыматтык ресурстарын пайдалануу жана техникалык тейлөөнү жүзөгө ашырган иштеп чыгуучулардын жана пайдалануучулардын кызматкерлери жана Улуттук статистика комитетинин кызматкерлери;

– маалыматтык инфраструктура, анын ичинде маалыматтарды иштеп чыгуу жана талдоо системаларын, аны иштеп чыгуунун, берүүнүн жана көрсөтүүнүн техникалык жана программалык камсыздоо, анын ичинде маалыматтык алмашуу жана телекоммуникация каналдары, маалыматты коргоо системаларын жана түзмөктөрүн, Улуттук статистика комитетинин маалыматтык чөйрөсүнүн сезгич элементтери жайгашкан объекттерди жана жайларды камтыган маалыматтык инфратүзүмдү камтыйт.

8. Коргоо, маалыматтык байланыштын негизги объекттеринин түзүмү, курамы жана жайгашуусу

Улуттук статистика комитетинин маалыматтык чөйрөсү – Улуттук статистика комитетинин борбордук аппаратынын, баш ийген ведомстволук жана аймактык органдарынын маалыматтык чакан системаларынын Улуттук статистика комитетинин бирдиктүү маалыматтык системасына бириктирүүчү бөлүштүрүлгөн түзүм болуп саналат.

Улуттук статистика комитетинин маалымат чөйрөсүнүн негизги өзгөчөлүктөрүнө төмөнкүлөр кирет:

– маалыматтык системанын компоненттерин кеңири аймактык бөлүштүрүлүшү;

– маалыматты иштеп чыгуунун жана берүүнүн көп сандагы техникалык каражаттарынын бирдиктүү системага бириктирүү;

– Улуттук статистика комитетинде маалыматты иштеп чыгуунун автоматташтырылган системаларын колдонуу чөйрөсүн олуттуу кеңейтүү;

– чечиле турган милдеттердин жана түрлөрүнүн ар кандай түрлөрү, иштетилүүчү маалыматтар, маалыматтарды автоматташтырылган статистикалык иштетүү режимдери;

– маалыматтарды автоматташтырылган иштетүүнүн негизинде кабыл алынган чечимдердин олуттуу маанилүүлүгү жана жоопкерчилиги;

– ар кандай максаттагы, таандыктагы жана купуялуулук деңгээлиндеги маалыматтарды бирдиктүү маалымат базаларына бириктирүү;

– Улуттук статистика комитетинин ишинин үзгүлтүксүздүгүн камсыз кылуу зарылчылыгы;

– расмий статистиканы пайдаланууучулардын категорияларынын ар түрдүүлүгү.

Мындай шарттарда маалыматтын аялуулугу кескин жогорулайт жана Улуттук статистика комитетинин маалыматтык чөйрөсүнүн маанилүү элементтеринин бири болуп корпоративдик маалымат системасы болуп калат, мында ар кандай пайдаланууучулар тарабынан пайдаланылуучу чыгарылуучу маалыматтардын олуттуу көлөмү иштетилет жана топтолот.

9. Коргоого алынуучу маалыматтык ресурстардын категориялары

Улуттук статистика комитети таралышы чектелген маалыматтарды (кызматтык, жашыруун, жеке маалыматтар) жана ачык маалыматты камтыган маалыматтарды жүгүртүүнү жүзөгө ашырат.

Улуттук статистика комитетинин бардык маалыматтык жана маалыматтык ресурстары Улуттук статистика комитетинин маалыматтык чөйрөсүндө көрсөтүлүшүнө жана жайгашкан жерине карабастан корголууга тийиш.

Улуттук статистика комитетинин маалыматтык коопсуздугунун аныкталган коркунучтарын эске алуу менен коргоо режими Улуттук статистика комитетинин маалыматтык чөйрөсүндө айланган маалыматты жана анын инфраструктурасын маалыматтын ээлерине же Улуттук статистика комитетине зыян келтирүүгө алып келүүчү табигый же жасалма мүнөздөгү кокустуктан же атайылап жасалган таасирлерден коргоонун ыкмаларынын жана чараларынын жыйындысы катары түзүлүүгө тийиш.

Расмий статистиканы өндүрүүгө, статистикалык талдоо жүргүзүүгө жана статистикалык кызмат көрсөтүүлөргө, анын ичинде Кыргыз Республикасынын расмий статистика чөйрөсүндөгү мыйзамдары менен жөнгө салынган бардык иш-аракеттерге арналган маалыматтар статистикалык максаттарда гана пайдаланылууга тийиш.

10. Улуттук статистика комитетинин маалыматтык коопсуздукту камсыз кылуу бөлүмүнүн негизги укуктары жана функциялары

Маалыматтык коопсуздук тутумунун натыйжалуу иштешин уюштуруу боюнча милдеттерди ишке ашырууну Улуттук статистика комитетинин маалыматтык коопсуздугун камсыз кылуу үчүн жооптуу бөлүмү (жооптуу адам) тарабынан камсыз кылынат, ага төмөнкүдөй негизги милдеттер жүктөлөт:

– маалыматтык-коммуникациялык технологиялардын активдерин эсепке алуу жана талдоо;

– маалыматтык коопсуздук инфратүзүмүнүн элементтерин түзүү жана өнүктүрүү боюнча иштерди координациялоо;

– мамлекеттик электрондук башкаруунун инфраструктурасынын реестринде маалыматтык системаны каттоо;

– Улуттук статистика комитетинин маалымат тутумунун программалык камсыздоонун эталондук нускаларынын, баштапкы программалык коддордун (эгерде бар болсо), лицензиялык программалык камсыздоонун орнотууларынын комплексинин, башкаруунун электрондук инфраструктурасынын элементтеринин техникалык документтеринин электрондук көчүрмөлөрүнүн жана Улуттук статистика комитетинин маалымат системасынын сакталышын көзөмөлдөө;

– ыйгарым укуктуу мамлекеттик орган, маалыматтык системасынын операторлору, башка мамлекеттик органдар, жергиликтүү өз алдынча башкаруу органдары, уюмдар менен электрондук башкаруу жана маалыматтык коопсуздук чөйрөсүндөгү долбоорлорду ишке ашыруу маселелери боюнча өз ара аракеттенүү;

– маалыматтык коопсуздук саясатын ишке ашыруу, Улуттук статистика комитетинин маалымат системасынын колдонуудагы компоненттерин түзүү жана андан ары өнүктүрүү процессинде коопсуздук системаларына талаптарды калыптандыруу;

– маалыматты комплекстүү коргоо боюнча Улуттук статистика комитетинин бардык бөлүмдөрүнүн иш-чараларын уюштуруу жана иштерин координациялоо;

– Улуттук статистика комитетинин маалыматтык коопсуздугунун учурдагы абалына ички аудит жана талдоо жүргүзүү;

– көрүлгөн чаралардын жана маалыматтык коопсуздукту камсыз кылуу чараларынын натыйжалуулугун көзөмөлдөө жана баалоо.

Ошондой эле Улуттук статистика комитетинин маалыматтык коопсуздукту камсыз кылуу чөйрөсүндөгү бул бөлүмдүн негизги функцияларына төмөнкүлөр кирет:

– маалыматтык коопсуздук (киберкоопсуздук) боюнча техникалык документтердин талаптарынын аткарылышын көзөмөлдөө;

– маалыматтык коопсуздукту документтештирүүнү көзөмөлдөө (киберкоопсуздук);

– маалыматтын купуялуулугун, жеткиликтүүлүгүн жана бүтүндүгүн камсыз кылуу боюнча чечимдерди даярдоо;

– маалыматтык коопсуздук системасын пайдаланууга кабыл алууга

катышуу;

– маалыматтык коопсуздукту (кибер коопсуздукту) камсыз кылуу бөлүгүндө активдерди башкарууну көзөмөлдөө;

– программалык камсыздоону пайдалануунун мыйзамдуулугун көзөмөлдөө;

– орнотулган маалыматтык коопсуздук системаларынын иштешин камсыз кылууну көзөмөлдөө;

– маалыматтык коопсуздук тутумунун иштешине байкоо жүргүзүү;

– маалыматтык коопсуздукту камсыз кылуу маселелеринде Улуттук статистика комитетинин кызматкерлерине методикалык жардам көрсөтүү;

– администраторлорунун, серверлердин жана тармактык түзүлүштөрдүн иш-аракеттерин көзөмөлдөө;

– пайдалануучулардын жана тейлөө кызматкерлеринин маалымат менен иштөөнүн белгиленген эрежелерин сактоосуна көзөмөлдөө жүргүзүү;

– Улуттук статистика комитетинин жетекчилигинин көрсөтмөсү боюнча маалымат жана жабдуулар менен иштөө эрежелерин бузуу фактылары боюнча кызматтык иликтөөнү уюштуруу;

– маалыматтык-коммуникациялык технологиялар чөйрөсүндөгү тобокелдиктерди башкарууну көзөмөлдөө;

– маалыматтык коопсуздук (киберкоопсуздук) окуяларын каттоону көзөмөлдөө;

– маалыматтык коопсуздуктун тышкы аудитин уюштуруу (киберкоопсуздук);

– Улуттук статистика комитетинде маалыматтык коопсуздуктун (киберкоопсуздуктун) талаптарын сактоого көзөмөлдөө жүргүзүү;

– маалыматтык ресурстарга жана системанын компоненттерине уруксатсыз кирүүгө аракет жасалганда же коопсуздук тутумунун иштөө эрежелери бузулган учурда чараларды көрүү;

- маалыматтык коопсуздук маселелери боюнча маалыматтарды чогултуу, топтоо, анализдөө жана системалаштыруу.

Ага жүктөлгөн милдеттерди чечүү үчүн Улуттук статистика комитетинин маалыматтык коопсуздугун камсыз кылуу боюнча жооптуу бөлүмү (адам):

– Улуттук статистика комитетинин маалыматтык тутумунун техникалык каражаттары орнотулган бардык жайларга кирүү укугуна жана ага түздөн-түз коркунуч келип чыккан учурда маалыматты иштеп чыгууну токтотууга укуктуу;

– Улуттук статистика комитетинин маалыматтык системасынын жаңы компоненттерин колдонуудагы компоненттердин катарына киргизүүгө тыюу салууга укуктуу, эгерде алар маалыматты коргоо талаптарына жооп бербесе жана бул маалыматтын коопсуздугуна олуттуу коркунучтар ишке ашырылган учурда олуттуу кесепеттерге алып келиши мүмкүн болсо;

– маалыматтык коопсуздукту (киберкоопсуздукту) камсыз кылуу маселелерине тиешелүү ченемдик укуктук актыларды, анын ичинде Улуттук статистика комитетинин маалыматтык системасын пайдалануучулардын бул чөйрөдөгү ишин жөнгө салуучу документтерди иштеп чыгуунун зарылдыгын аныктайт;

– Улуттук статистика комитетинде маалыматтык технологияларды колдонуунун бардык маселелери боюнча Улуттук статистика комитетинин маалыматтык системасын пайдалануучулардан маалымат ала алат;

– жаңы маалыматтык технологияларды иштеп чыгууда жана иштеп чыгууда маалыматтык коопсуздукту камсыз кылуу маселелери боюнча техникалык чечимдерди иштеп чыгууга катышат;

– маалыматтык коопсуздук талаптарын ишке ашыруунун сапатын баалоо үчүн иштелип чыккан маалыматтык технологияларды тестирлөөгө (сыноого) катышат;

– маалыматтык коопсуздукту камсыз кылуу маселелери боюнча Улуттук статистика комитетинин маалымат тутумун пайдалануучулардын ишин көзөмөлдөйт;

– зарылчылыкка жараша Улуттук статистика комитетинин жетекчилиги менен макулдашуу боюнча Улуттук статистика комитетинин баш ийген ведомстволук жана аймактык органдарына карата жерлеринде текшерүүлөрдү жүргүзөт.

IV. Маалыматтык ресурстардын коопсуздугунун талап кылынган деңгээлин камсыз кылуунун чаралары, ыкмалары жана түзүлүштөрү

11. Маалыматтык коопсуздук системасынын маселелерин чечүүнү камсыз кылуунун негизги жолдору жана чаралары

Улуттук статистика комитетинин маалыматтык коопсуздугун камсыз кылуу режимин түзүү боюнча чаралардын комплекси төмөнкүлөрдү камтыйт:

1) Улуттук статистика комитетинде маалыматтык коопсуздукту камсыз кылуунун уюштуруу-укуктук режимин белгилөө (зарыл ченемдик документтерди иштеп чыгуу, кызматкерлер менен иштөө, иш кагаздарын жүргүзүү эрежелери);

2) Улуттук статистика комитетинин корпоративдик маалыматтык системасынын маалыматтык ресурстарына уруксатсыз аракеттердин (жеткиликтүүлүктүн) алдын алуу боюнча уюштуруу жана программалык-техникалык иш-чаралар;

3) кокустан же атайылап таасир тийгизүүдөн кийин чектелген пайдалануудагы маалымат ресурстарын коргоо каражаттарынын жана системаларынын иштешин көзөмөлдөө боюнча комплекстүү иш-чаралар;

4) Улуттук статистика комитетинин маалыматтык коопсуздугун камсыз кылуу боюнча жооптуу бөлүмдүн (адамдын) Улуттук статистика комитетине тиешеси жок башка уюштуруу түзүмдөрүнө тиешеси бар адамдардын Улуттук статистика комитетине киришине жол бербөө (аныктоо) боюнча ыкчам комплекстүү иш-чаралар;

5) маалыматтарды коопсуз иштетүүнү жана сактоону камсыз кылуу боюнча иш-чаралар.

Ушуга ылайык, иш-чаралардын аткарылышы төмөндөгүлөрдү камсыз кылуу менен толук кандуу:

– Улуттук статистика комитетинин корголуучу маалыматтык системасынын бардык ресурстарын (маалыматтарды, тапшырмаларды, документтерди, байланыш каналдарын, серверлерди, автоматташтырылган жумушчу станцияларды) так эсепке алуу;

– корпоративдик маалыматтык системанын программалык жана техникалык жабдуларын тейлөөнү жана модификациялоону жүзөгө ашырган кызматкерлердин иш-аракеттерин журналга жазуу;

– маалыматтык коопсуздукту камсыз кылуу маселелери боюнча Улуттук статистика комитетинин уюштуруу-тескөөчү документтеринин талаптарынын толуктугу, реалдуу максатка ылайыктуулугу жана шайкештиги;

– маалыматтын жана аны иштетүү процесстеринин коопсуздугун камсыз кылуу боюнча практикалык чараларды уюштуруу жана ишке ашыруу үчүн жооптуу кызмат адамдарын (кызматкерлерин) окутуу;

– ар бир кызматкерге (пайдалануучуга) Улуттук статистика комитетинин маалыматтык ресурстарына жетүү үчүн функционалдык милдеттерин аткаруу үчүн зарыл болгон минималдуу ыйгарым укуктарды берүү;

– маалыматтык коопсуздук маселелери боюнча Улуттук статистика комитетинин маалыматтык системасынын бардык пайдалануучуларынын жетишээрлик так билүүсү жана уюштуруучулук-тескөөчү документтердин талаптарын так аткаруусу;

– Улуттук статистика комитетинин маалыматтык ресурстарына ээ болгон ар бир кызматкердин өзүнүн функционалдык милдеттеринин чегинде жасаган аракеттери үчүн жеке жоопкерчиликти;

– Улуттук статистика комитетинин маалыматтык чөйрөсүнүн элементтеринин коопсуздуктун талап кылынган деңгээлин үзгүлтүксүз камсыз кылуу, техникалык каражаттардын ашыкча болушун (резервдөөнү) жана массивдердин жана сактоочу каражаттардын кайталоону камсыз кылуу;

– системалык ресурстарды коргоонун физикалык-техникалык (аппараттык жана программалык) жабдуларын пайдалануу жана аларды пайдалануну үзгүлтүксүз (оперативдүү, үзгүлтүксүз административдик, эксплуатациялык-техникалык жактан) колдоо;

– Улуттук статистика комитетинин маалыматтык ресурстарын пайдалануучулардын маалыматтык коопсуздуктун талаптарын сактоосуна натыйжалуу көзөмөлдөө;

– Улуттук статистика комитетинин бөлүмдөрүнүн тышкы уюмдар менен өз ара аракеттенүүсүндө (маалымат алмашуу менен байланышууларда) ушул уюмдар тарабынан да, ошондой эле Улуттук статистика комитетинин кызматкерлеринин жана башка үчүнчү жактардын мыйзамсыз аракеттеринен да Улуттук статистика комитетинин кызыкчылыктарын юридикалык жактан коргоо;

– ыйгарым укуктуу пайдалануучулар үчүн маалыматтын жана ага байланыштуу ресурстардын жеткиликтүүгү;

– Улуттук статистика комитетинин маалымат тутумдарына уруксатсыз, анын ичинде кокусунан кирүүнү болтурбоо; жеке маалыматтарды, кызматтык же мамлекеттик сырды түзгөн маалыматтарды жок кылууга, өзгөртүүгө, бөгөт

коюуга, көчүрүүгө, таркатууга, ошондой эле башка уруксатсыз аракеттерге алып келе турган мүмкүчулуктөргө жол бербөө;

– Улуттук статистика комитетинин корпоративдик маалыматтык системасына зыяндуу программаларды киргизүүгө жол бербөө;

– жумуштан тышкаркы жана дем алыш күндөрү Улуттук статистика комитетинин корпоративдик маалымат тутумуна чектөөлөрдү киргизүү.

12. Маалыматты коргоону камсыз кылуунун уюштуруу-укуктук режими

Маалыматты коргоонун уюштуруу-укуктук чараларына маалыматтарды иштеп чыгуу тутумунун иштөө процесстерин, анын ресурстарын пайдаланууну, Улуттук статистика комитетинин кызматкерлеринин ишин жөнгө салуучу уюштуруу мүнөзүндөгү чаралар, ошондой эле колдонуучулардын система менен өз ара аракеттенүүсүнүн тартиби коопсуздук коркунучтарын ишке ашыруу мүмкүнчүлүгүн кыйла оорлотуучу же болтурбоочу же аларды ишке ашырууда жоготуулардын өлчөмүн азайтуучу чаралар кирет.

Уюштуруу-укуктук режим маалыматтардын коопсуздугунун укуктук базасын түзүүнү жана колдоону, атап айтканда, уюштуруу-тескөө документтерин иштеп чыгууну жана кабыл алууну карайт:

1) Жашыруун маалымат жөнүндө жобо

Аталган жобо купуя маалыматты (кызматтык жана мамлекеттик сырлар, жеке маалыматтар, расмий статистиканы өндүрүүчүлөрдүн карамагында болгон жеке маалыматтар) түзгөн маалыматтар менен иштөөнүн тартибин, маалыматтарды иштеп чыгууга жол берилген кызматкерлердин милдеттерин жана жоопкерчиликтерин, кызматтык жана мамлекеттик сырды түзгөн маалыматтарды камтыган материалдарды мамлекеттик жана коммерциялык мекемелерге жана уюмдарга берүүнүн тартибин жөнгө салат.

2) жашыруун маалыматты түзгөн маалыматтардын тизмеси.

Тизме жашыруун, чектелген маалымат катары классификацияланган маалыматтарды, корголуучу маалыматка жетүү боюнча чектөөлөрдү камсыз кылуунун деңгээлин жана мөөнөттөрүн аныктайт.

3) Улуттук статистика комитетинин маалыматтык коопсуздук саясатынын талаптарын деталдуу чагылдырган маалыматтык коопсуздукту (кибер коопсуздукту) камсыз кылуу жаатындагы ченемдик документтердин, жумушчу формалардын, журналдардын, өтүнмөлөрдүн, протоколдордун жана башка документтердин, анын ичинде аткарылган жол-жоболорду жана иштерди каттоо жана тастыктоо үчүн пайдаланылуучу электрондук документтердин.

4) маалыматтын коопсуздук режимин белгилөө боюнча буйруктардын жана тескемелердин:

– кызматкерлерге купуя маалымат жана чектелген маалыматтар менен иштөөгө уруксат берүү жөнүндө;

– Улуттук статистика комитетинин корпоративдик маалымат системасында таркалышы чектелген маалыматтар менен жашыруун маалыматтар менен иштөө үчүн жооптуу администраторлорду жана адамдарды дайындоо жөнүндө.

5) кызматкерлердин нускамаларын жана функционалдык милдеттерин:

– коопсуздукту жана кирүүнү көзөмөлдөө режимин уюштуруу боюнча;

– иш кагаздарын жүргүзүүнү уюштуруу боюнча;

– корпоративдик маалыматтык системасынын маалыматтык ресурстарын башкаруу боюнча;

– башка ченемдик документтер.

13. Маалыматты жана маалыматтык активдерди коргоо боюнча уюштуруу-техникалык иш-чаралар

Техникалык (аппараттык жана программалык) коргоо чаралары ар кандай электрондук түзүлүштөрдү жана маалымат системасын коргоо функцияларын аткарган (өз алдынча же башка каражаттар менен айкалышкан) атайын программаларды колдонууга негизделген.

1) Маалыматтык активдерди коргоону камсыз кылуу үчүн Улуттук статистика комитетинин маалыматтык коопсуздугун камсыз кылуу боюнча жооптуу бөлүмү (адам) төмөнкүлөргө көзөмөлдөөнү жүзөгө ашырат:

– активдерди инвентаризациялоо;

– кызмат адамдарына активдерди бекитүү жана киберкоопсуздук активдерин башкаруу боюнча чараларды ишке ашыруу үчүн алардын жоопкерчилигинин көлөмүн аныктоо;

– киберкоопсуздук боюнча техникалык документтерде активдерди пайдалануу жана кайтаруу, активдерди идентификациялоо, классификациялоо жана маркировкалоо тартибин жөнгө салуу.

2) Улуттук статистика комитетинде маалыматтык коопсуздукту бузуу окуяларына көзөмөлдү жүргүзүү үчүн:

а) маалыматтык коопсуздукту бузуу менен байланышкан окуяларга мониторинг жүргүзүлөт жана мониторингдин натыйжаларына, жыйынтыктарына талдоо жүргүзүлөт;

б) маалыматтык коопсуздуктун абалына байланыштуу окуялар катталат жана окуяларды каттоо журналдарын талдоо жолу менен эреже бузуулар аныкталат, анын ичинде:

– операциондук системалардын окуялар журналдары;

– маалыматтар базасын башкаруу системасынын иш–чараларын каттоо журналдары;

– антивирустук коргоо окуяларынын журналдары;

– колдонмо программалык камсыздоо окуяларын каттоо журналдары;

– телекоммуникациялык жабдуулардын окуяларын каттоо журналдары;

– маалымат системасына кол салууну аныктоо жана алдын алуу системасынын окуяларын каттоо журналы;

– контентти башкаруу системанын окуяларын каттоо журналдары;

в) окуяларды каттоо журналдарынын убактысын убакыт булагынын инфраструктурасы менен синхрондоштуруу камсыз кылынат;

г) окуяларды каттоо журналдары кибер коопсуздук боюнча техникалык

документтерде көрсөтүлгөн мөөнөттүн ичинде, бирок үч жылдан кем эмес сакталат жана үч айдан кем эмес ыкчам жетүүдө болот;

д) ыйгарым укуктуу мамлекеттик орган тарабынан бекитилүүчү маалыматтык коопсуздукту (кибер коопсуздукту) камсыз кылууга, электрондук башкаруу боюнча Улуттук статистика комитетинин инфратүзүмүнүн элементтеринин корголушуна жана коопсуз иштешине мониторинг жүргүзүү эрежелеринде аныкталган жазуулардын форматтарына жана түрлөрүнө ылайык түзүлүүчү программалык камсыздоо окуяларын каттоо журналдары жүргүзүлөт;

е) окуяларды каттоо журналдарын кийлигишүүдөн жана уруксатсыз кирүүдөн коргоо камсыз кылынат; системалык администраторлордо журналдарды өзгөртүүгө, алып салууга жана өчүрүүгө ыйгарым укуктардын болушуна жол берилбейт; жашыруун маалымат системалары үчүн журналдардын резервдик сактагычын түзүү жана жүргүзүү талап кылынат;

ж) киберкоопсуздуктун инциденттери жөнүндө маалымдоонун, билдирүүнүн жана киберкоопсуздуктун инциденттерине чара көрүүнүн формалдуу, расмий жол-жоболорун киргизүү камсыз кылынат.

3) Улуттук статистика комитетинин маалымат системасындагы өтө маанилүү процесстерди ички жана тышкы коркунучтардан коргоо максатында:

– маалыматты кайра иштетүү жабдулар менен байланышкан активдердин үзгүлтүксүз иштешин жана функционалдуулугун калыбына келтирүүнү камсыз кылуу үчүн иш-чаралар планы иштелип чыгат, сыналат жана ишке ашырылат;

– Улуттук статистика комитети тарабынан бекитилген киберкоопсуздуктун инциденттерине жана өзгөчө (кризистик) кырдаалдарга пайдалануучулардын чара көрүү тартиби жөнүндө нускама Улуттук статистика комитетинин кызматкерлеринине жеткирилет.

Маалыматтарды кайра иштетүү жабдулары менен байланышкан активдердин үзгүлтүксүз иштешин камсыз кылуу жана ишке жарамдуулугун калыбына келтирүү боюнча иш-чаралардын планы үзгүлтүксүз жаңыртылып турууга тийиш.

4) Маалыматтык коопсуздук (киберкоопсуздук) боюнча техникалык документтер Улуттук статистика комитетинин жана анын түзүмдүк бөлүмдөрүн өз ишинде жетекчиликке ала турган документтештирилген эрежелер, жол-жоболор жана көрсөтмөлөр түрүндө түзүлөт.

Киберкоопсуздук боюнча техникалык документтер Улуттук статистика комитетинин жетекчилигинин чечими менен бекитилет жана Улуттук статистика комитетинин бардык кызматкерлерине жеткирилет.

Маалыматтык коопсуздук (киберкоопсуздук) боюнча техникалык документтер анда камтылган маалыматтарды талдоо жана актуалдаштыруу максатында эки жылда бир жолудан кем эмес кайра каралып турат.

5) Улуттук статистика комитетинин кызматкерлеринин маалыматтык коопсуздугун камсыз кылуу боюнча функционалдык милдеттери жана маалыматтык коопсуздук боюнча техникалык документтердин талаптарын аткаруу боюнча милдеттери кызматтык нускамаларга жана/же эмгек келишиминин шарттарына киргизилет.

Маалыматтык коопсуздук боюнча техникалык документтерде маалыматтык коопсуздукту камсыз кылуу жаатында милдеттенмелери бар Улуттук статистика

комитетинин кызматкерлерин иштен бошотуудагы жол-жоболордун мазмуну да аныкталат.

Кызматтан бошотууда же эмгек келишиминин шарттарына өзгөртүүлөрдү киргизүүдө Улуттук статистика комитетинин кызматкеринин маалыматка жана маалыматты иштеп чыгуу жабдуларга жетүү укугу:

– физикалык жана логикалык кирүү мүмкүндүгүн, кирүү идентификаторлорун, Улуттук статистика комитетинин иштеп жаткан кызматкери катары идентификациялоочу кол тамгаларды, документтерди камтыйт;

– жокко чыгарылат же эмгек келишиминин шарттарына өзгөртүүлөр киргизилгенде өзгөртүлөт.

6) Мамлекеттик маалыматтык системаларды жана башка электрондук башкаруу объекттерин иштетүүдө маалыматтык коопсуздукту камсыз кылуу максатында Улуттук статистика комитети төмөнкүлөргө талаптарды белгилейт:

– идентификациялоо ыкмаларын;

– маалыматты криптографиялык коргоонун колдонулуучу түзмөктөрүн;

– жеткиликтүүлүгүн жана каталарга туруктуулукту камсыз кылуу жолдорун;

– маалыматтык коопсуздукка, коргоого жана коопсуз иштешине мониторинг жүргүзүүнү;

– маалыматтык коопсуздукту камсыз кылуу инструменттерин жана системаларын колдонуу;

– иштелип жаткан же сатып алынган колдонмо программалык камсыздоо төмөнкү инструменттерди колдонууну талап кылат:

- пайдалануучуларды идентификациялоо жана аутентификациялоо, зарыл болгон учурда электрондук кол тамга жана каттоо күбөлүктөрү менен;
- жеткиликтүүнү башкаруу;
- бүтүндүктү көзөмөлдөө;
- киберкоопсуздукка таасир этүүчү колдонуучунун аракеттерин журналга каттоо;
- онлайн транзакцияларды коргоо;
- маалыматты сактоодо жана иштетүүдө тиешелүү деңгээлдеги маалыматты криптографиялык коргоо каражаттарын пайдалануу менен маалыматты криптографиялык коргоо;
- программалык камсыздоонун маанилүү окуяларын журналга каттоо.

7) Коргоонун техникалык жабдулары төмөнкүдөй негизги милдеттерди чечүү үчүн да жооп берет:

– ысымдардын же атайын аппараттык жабдулардын жардамы менен пайдалануучуларды идентификациялоо жана аутентификациялоо;

– пайдалануучулардын жайларга, физикалык жана логикалык түзүлүштөргө кирүүсүн жөнгө салуу жана башкаруу;

– компьютердик вирустардын киришинен жана зыяндуу программалардын кыйратуучу таасиринен коргоо;

– пайдалануучунун бардык аракеттерин коопсуз журналда каттоо, каттоонун бир нече деңгээлдеринин болушу;

– файл сервериндеги маалыматтарынын коргоо тутумунун анда жайгашкан маалыматтар менен иштөө кызматтык милдеттерине кирбеген пайдалануучулардын кирүүсүнөн коргоо.

14. Маалыматтарды коопсуз иштетүү жана сактоо

1. Улуттук статистика комитетинин борбордук аппаратынын бөлүмдөрү, Улуттук статистика комитетинин расмий статистикалык маалыматтарды өндүрүүнү жүзөгө ашыруучу баш ийген ведомстволук жана аймактык органдары төмөнкүлөргө милдеттүү:

1) жеке маалыматтарды коргоону камсыз кылууга;

2) жашыруун жалпыланган көрсөткүчтөрдү жана статистикалык маалыматтарды алар чыгарылганга чейин коргоону камсыз кылууга;

3) ыйгарым укуктуу эмес, уруксаты жок адамдардын маалыматтарга жетүүсүн болтурбоо боюнча ченемдик-укуктук, административдик, техникалык жана уюштуруучулук чараларды көрүүгө.

2. Улуттук статистика комитетинин борбордук аппаратынын бөлүмдөрү, расмий статистика өндүрүшүн ишке ашыруучу Улуттук статистика комитетинин баш ийген ведомстволук жана аймактык органдары жеке маалыматтар чөйрөсүндөгү Кыргыз Республикасынын мыйзамдарына ылайык статистикалык максаттарга жетүү үчүн зарыл болгон мезгил ичинде идентификаторлору бар жеке маалыматтарды иштеп чыгууну жана сактоону жүргүзөт.

Маалыматтарды чогултуунун кагаз жана электрондук формаларында пайдаланылуучу жана Улуттук статистика комитетинде расмий статистиканы өндүрүүчүлөргө берилген администрациялык маалыматтарда камтылган идентификаторлор аларды администрациялык маалыматтарды берүүчүлөр менен макулдашуу боюнча статистикалык максаттарда пайдалануунун зарылдыгы жок болгон учурдан тартып жок кылынат.

3. Маалыматты кызматтык пайдалануу, жашыруун маалымат, маалыматтык системалардын маалымат базаларында камтылган жеке маалыматтардын атайын категориялары үчүн коргоо максатында Кыргыз Республикасынын мыйзамдарында белгиленген коопсуздуктун тиешелүү деңгээлиндеги маалыматты криптографиялык коргоо жабдуларына карата техникалык талаптарга ылайык параметрлери бар маалыматты криптографиялык коргоо жабдуларды (программалык же аппараттык) колдонулат.

15. Маалыматташтыруу объекттерин физикалык коргоо жана режимдик талаптар

Имараттарды, жайларды, объектилерди жана маалымат жабдуларын физикалык жактан коргоо Улуттук статистика комитетинин маалыматтык коопсуздугун камсыз кылуу үчүн жооптуу бөлүм (адам) тарабынан тиешелүү күзөт постторун, техникалык коопсуздук жабдуларын же болбосо аларды

болтурбоочу же башка ыкмаларды орнотууну камсыз кылуу жолу менен уюштурулууга тийиш. Алардын милдеттерине уруксаты жок адамдардын киришин жол бербөөгө, документтерди жана маалымат алып жүрүүчүлөрдү, маалыматтык жабдулардын өздөрүн уурдоону олуттуу татаалдаштырууга, ошондой эле көзөмөлдөгү (корголуучу) зонанын ичинде маалыматты алуунун техникалык жабдулардын болушун жокко чыгарууга шарттарды түзү боюнча маселер кирет.

Маалыматташтыруу объекттерин (Улуттук статистика комитетинин маалымат системасынын компоненттерин) физикалык жактан коргоо төмөнкүлөрдү камтыйт:

1) объектиге күзөт-өткөрүү режиминин системасын жана уруксат берүүнү көзөмөлдөө системасын уюштуруу;

2) чектелген маалыматты сактоо үчүн арналган жайларга кирүүгө кошумча чектөөлөрдү киргизүү (коддук жана электрондук кулпулар, уруксат берүү карточкалары ж.б.);

3) корголуучу объекттин көзөмөлдөнүүчү аймагын визуалдык жана техникалык көзөмөлдөө; коопсуздук жана өрт сигнализациясын колдонуу.

Чектелген маалымат менен иштөөдө коопсуздук режимдик талаптарын сактоо төмөнкүлөрдү камтыйт:

1) чектелген пайдалануудагы маалыматтык ресурстарга жеткиликтүүлүктү чектөө;

2) корпоративдик маалыматтык системанын ресурстарына жеткиликтүүлүктүнү чектөө;

3) кызматкерлердин чектелген пайдалануудагы маалыматтар менен таанышуусун эсепке алууну жүргүзүү;

4) кызматкерлердин функционалдык милдеттерине чектелген пайдалануудагы маалыматарды ачыкка чыгарбоо, сактоо жана коргоо боюнча милдеттенмелерди киргизүү;

5) жеке маалыматтардын идентификаторлорун, маалыматты материалдык сактагычтарды жок кылууну уюштуруу;

6) кызматтык жайларды сейфтер, кагаз жана башка маалымат сактоочуларды сактоо үчүн шкафтар менен камсыздоо;

7) жашыруун маалымат талкуулана турган жайларды акустикалык жактан коргоону камсыз кылуу.

16. Техникалык көзөмөлдөө иш-чаралары

Улуттук статистика комитетинде маалыматтык коопсуздукту камсыз кылуу үчүн:

1) маалыматтык коопсуздук (киберкоопсуздук) боюнча техникалык документтерде төмөнкүлөр аныкталат жана иш-аракеттеди жүзөгө ашырууда колдонулат:

– серверлерге жана жумушчу станцияларга программалык камсыздоону орнотуу, жаңыртуу жана алып салуу эрежелери;

– системанын программалык камсыздоого өзгөртүүлөр киргизилген учурда программалык камсыздоону өзгөртүүнү башкаруу жана талдоо жол-

жоболору;

– Улуттук статистика комитетинин кызматкерлеринин жумушчу станцияларын жайгаштыруу ыкмалары;

– жумушчу станцияларды электр менен жабдуу системасындагы бузулуулардан жана инженердик коммуникациялардын иштөөсүнүн бузулушунан улам келип чыккан башка бузулуулардан коргоо жолдору;

– үзгүлтүксүз жеткиликтүүлүктү жана бүтүндүктү камсыз кылуу үчүн жумушчу станцияларды тейлөөнүн жол-жоболору жана мезгилдүүлүгү;

– ар кандай тышкы тобокелдиктерди эске алуу менен Улуттук статистика комитетинин чегинен тышкары жайгашкан мобилдик пайдалануучулардын жумушчу станцияларын коргоо жолдору;

– жумушчу станцияларды кайра пайдаланууда же сактагычтарды эксплуатациядан чыгарууда маалыматты кепилдүү жок кылуунун ыкмалары;

– жумушчу станцияларды жумуш ордунан башка жакка чыгаруу эрежелери;

2) жумушчу станцияларды маалыматтык технологиялар маселелеринде компетенттүү бөлүнүш тарабынан туруктуу негизде конфигурацияларды текшерүү менен эсепке алуу жүргүзүлөт;

3) лицензияланууучу программалык камсыздоолор лицензиялары болгон шартта гана колдонулат жана сатып алынат;

4) жумушчу станцияларда ички контурдун локалдык тармагын сырттан алыстан башкаруунун программалык же аппараттык жабдулардын орнотууга жана колдонууга жол берилбейт; ички контурдун локалдык тармагынын чегинде дистанциялык башкарууга мындай аралыктан жетүүнү берүүнүн шарттарын жана тартибин (буйрук, жобо, нускама) аныктаган Улуттук статистика комитетинин ченемдик укуктук актысында түздөн-түз каралган учурларда гана жол берилет;

5) Улуттук статистика комитетинин кызматкерлеринин жумушчу станцияларынын жана мобилдик компьютерлеринин пайдаланылбаган киргизүү – чыгаруу порттору өчүрүлөт же жабылат;

6) Кызматтык пайдалануу үчүн маалыматты коргоо максатында маалыматтык системанын маалымат базасында камтылган купуя маалыматтар, жеке маалыматтардын атайын категориялары, маалыматты криптографиялык коргоо жабдуларына (коопсуздуктун тиешелүү деңгээлиндеги) карата белгиленген техникалык талаптарга ылайык параметрлер менен криптографиялык маалыматты коргоо каражаттары (программалык же аппараттык каражаттар) колдонулат.

17. Маалыматтык коопсуздук тобокелдиктерин/коркунучтарын башкаруу

Маалыматтык коопсуздук чөйрөсүндөгү тобокелдиктерди/ коркунучтарды башкаруу максатында Улуттук статистика комитети төмөнкүлөрдү жүзөгө ашырат:

1) Улуттук статистика комитети иштин тиешелүү түрлөрүн жүзөгө ашырууда маалыматтык системасындагы маалыматтык коопсуздукка

(киберкоопсуздукка) коркунучтардын тизмесин аныктоо;

2) идентификацияланган жана классификацияланган активдердин тизмесине карата тобокелдиктерди аныктоо, анын ичинде:

– маалыматтык коопсуздуктун коркунучтарын жана алардын булактарын аныктоо;

– коркунучтарды ишке ашырууга алып келиши мүмкүн болгон аялуу жерлерди, алсыздыктарды аныктоо;

– маалыматтын агып чыгуу каналдарын аныктоо;

– кылмышкердин болжолдуу үлгүсүн калыптандыруу;

3) аныкталган тобокелдиктерди кабыл алуу критерийлерин тандоо;

4) маалыматтык коопсуздуктун коркунучтарынын (тобокелдеринин) каталогун түзүү, анын ичинде коркунучтарды (тобокелдиктерди) баалоо (кайра баалоо), потенциалдуу зыяндарды аныктоо;

5) маалыматтык коопсуздукка коркунучтарды (тобокелдиктерди) зыянсыздандыруу же азайтуу боюнча чараларды иштеп чыгуу жана бекитүү.

18. Бөлмө жайларга кирүүнү жөнгө салуу

Улуттук статистика комитетинин маалыматтык системасынын таасирлерге сезгич компоненттери ишенимдүү автоматтык кулпулар, сигнализация каражаттары менен жабдылган жана дайыма кайтарууда же байкоодо турган, бөтөн адамдардын бөлмөгө көзөмөлсүз кирүү мүмкүнчүлүгүн жокко чыгарган жана имараттагы корголгон ресурстардын (документтердин, серверлердин, кирүү реквизиттеринин ж.б.) физикалык сакталышын камсыз кылган жайларда жайгаштырылууга тийиш.

Аппараттык-программалык комплекстин сервердик жабдуулары жана маалыматтарды сактоо системалары сервердик жайда жайгаштырылат.

Сервердик бөлмө терезе тешиктери жок өзүнчө, өтүүгө мүмкүн эмес бөлмөлөрдө жайгашат.

Сервердик жай тышкы электромагниттик нурлануудан ишенимдүү корголот.

Маанилүү жабдууларды техникалык тейлөө сертификатталган техникалык кызматкерлер тарабынан жүзөгө ашырылат.

Чектелген маалыматты иштеп чыгуу учурунда мындай жайларда бул маалымат менен иштөөгө ыйгарым укуктуу Улуттук коопсуздук комитетинин кызматкерлери гана катышууга тийиш.

Чектелген маалыматты иштеп чыгууда зыяратчыларды жайларда кабыл алууга тыюу салынат.

Эгерде жайлар күзөт сигнализациялары, ошондой эле бул каражаттардан сигналдарды кабыл алуунун жана эсепке алуунун автоматташтырылган системасы менен жабдылган болсо, мындай жайларды кайтарууга кабыл алуу жана берүү атайын иштелип чыккан нускамалардын негизинде жүзөгө ашырылат.

19. Кызматкерлердин маалыматтык ресурстарды пайдаланууга жеткиликтүүлүгүн жөнгө салуу

Пайдалануучулардын Улуттук статистика комитетинин маалыматтык системасы менен иштөөгө уруксаты жана анын ресурстарына жетүүсү катуу жөнгө салынууга тийиш.

Чакан системаны пайдалануучулардын курамына жана ыйгарым укуктарына ар кандай өзгөртүүлөр Улуттук статистика комитетинин маалыматтык ресурстарын пайдаланууга жеткиликтүүлүктү камсыз кылуу боюнча ченемдик укуктук актыларга ылайык белгиленген тартипте жүргүзүлүүгө тийиш.

Корпоративдик маалымат системасындагы маалыматтардын негизги пайдалануучулары болуп Улуттук статистика комитетинин борбордук аппаратынын бөлүмдөрүнүн, баш ийген ведомстволук жана аймактык органдарынын кызматкерлери саналат.

Ар бир пайдалануучунун ыйгарым укуктарынын деңгээли төмөнкү талаптарды сактоо менен жекече аныкталат:

– ар бир кызматкер кызматтык милдеттерине ылайык иштөө зарыл болгон маалыматка карата ага белгиленген укуктардан гана пайдаланат. Кошумча маалыматтык ресурстарга жетүү укугун кеңейтүү жана аларга жетүү мүмкүндүгүн берүү милдеттүү түрдө Улуттук статистика комитетинин маалыматтык коопсуздукту камсыздоо бөлүмү менен макулдашылууга тийиш;

– Улуттук статистика комитетинин түзүмдүк бөлүмүнүн жетекчиси өзүнүн кызматтык милдеттерине ылайык, өзүнө баш ийген адамдардын маалыматтарын белгиленген чектерде гана кароого укуктуу.

Улуттук статистика комитетинин маалыматтык системасынын мыйзамдуу пайдалануучулары катары катталган Улуттук статистика комитетинин бардык кызматкерлери маалыматты иштеп чыгуунун белгиленген тартибин, алардын карамагында болгон системанын корголгон ресурстарын, чектелген пайдалануудагы маалыматтарды сактоо, пайдалануу жана берүү эрежелерин бузгандыгы үчүн жеке жоопкерчилик тартууга тийиш.

Ар бир кызматкер ишке кабыл алууда жашыруун, купуя маалыматты, жеке мүнөздөгү маалыматты сактоо боюнча белгиленген талаптарды сактоо жана бузгандыгы үчүн жоопкерчилик жөнүндө милдеттенмеге кол коюуга тийиш.

Улуттук статистика комитетинин маалыматтык системасынын компоненттеринде маалыматтарды иштеп чыгуу маалыматтык коопсуздукту камсыз кылуу боюнча талаптарды камтыган Улуттук статистика комитетинин бекитилген нускамаларына ылайык жүргүзүлүүгө тийиш.

20. Аппараттык жана программалык ресурстарды тейлөө жана модификациялоону жүзөгө ашыруу процесстерин жөнгө салуу

Системанын корголууга тийиш болгон ресурстары (документтер, тапшырмалар, серверлер, программалар) катуу эсепке алынууга тийиш (тиешелүү формулярларды же маалыматтардын адистештирилген базаларын колдонуунун негизинде).

Маалыматтык коопсуздук режимин сактоо максатында, Улуттук статистика комитетинин кызматкерлеринин корпоративдик маалыматтык системасынын ресурстарына жетүү мүмкүн болгон автоматташтырылган жумушчу станцияларынын аппараттык-программалык конфигурациясы ушул пайдалануучуларга жүктөлгөн функционалдык милдеттердин чөйрөсүнө шайкеш келиши керек.

Жашыруун маалымат менен иштеген кызматкерлердин жумуш орундарында колдонулбаган бардык киргизүү/чыгарма түзүлүштөрү мүмкүн болсо өчүрүлүшү керек, тышкы физикалык сактагычта иштөө үчүн керексиз программалык камсыздоо жана маалымат сактагычтардагы маалыматтар жок кылынышы керек.

Кошумча байланыш жабдулар өзгөчө учурларда жана убактылуу чара катары гана колдонулушу мүмкүн.

Мындай түзүлүштөрдү орнотуу Улуттук статистика комитетинин маалыматтык коопсуздугун камсыз кылуу үчүн жооптуу бөлүм (адам) менен макулдашылууга тийиш.

Корпоративдик маалыматтык системасынын компоненттеринде жана Улуттук статистика комитетинин кызматкерлеринин жумуш орундарында Улуттук статистика комитетинин маалыматтык коопсуздугун камсыз кылуу үчүн жооптуу бөлүмдөн (адамдан) гана уруксат алган программалык камсыздоо орнотулушу жана колдонулушу керек.

Улуттук статистика комитетинин корпоративдик маалыматтык системасынын корголушун баалоо жана Улуттук статистика комитетинин маалыматтык системасында маалыматты коргоо системасын түзүү боюнча атайын милдеттерди чечүү үчүн Улуттук статистика комитетинин маалыматтык коопсуздугун камсыз кылууга жооптуу бөлүм (адам) менен макулдашылган атайын программалык камсыздоо колдонулушу мүмкүн.

Маалыматты коргоонун натыйжалуулугуна көзөмөлдөө техникалык каналдар боюнча маалыматтын ага уруксатсыз кирүүсүнөн улам агып кетишин өз убагында табуу жана алдын алуу, ошондой эле маалыматты жок кылууга жана маалымат каражаттарын жок кылууга багытталган мүмкүн болуучу өзгөчө таасирлердин алдын алуу максатында жүзөгө ашырылат.

Көзөмөлдөө Улуттук статистика комитетинин маалыматтык коопсуздукту камсыз кылуу боюнча жооптуу бөлүмү (адам) тарабынан да, ошондой эле иштин ушул түрүнө лицензиясы бар, бул максатта тартылган уюмдар тарабынан да жүргүзүлүшү мүмкүн.

Маалыматты коргоо чараларынын натыйжалуулугун баалоо белгиленген талаптарга ылайыктуулугун техникалык жана программалык көзөмөлдөө

жабдуларын пайдалануу менен жүргүзүлөт.

Улуттук статистика комитетинин тейлөөчү кызматкерлерине эксплуатациялоо учурунда кирүү талап кылынбаган, жашыруун маалыматка жетүү үчүн пайдаланылуучу корпоративдик маалымат системанын жабдуулары жөндөөдөн, оңдоодон жана анын компоненттерине жетүү менен байланышкан башка иштерден кийин жабылууга жана пломбалануу тийиш.

21. Персоналды (кызматкерлерди) тандоо жана даярдоо, пайдалануучуларды окутуу

Улуттук статистика комитетинин маалыматтык системасынын маалыматтарын пайдалануучулар, Улуттук статистика комитетинин борбордук аппаратынын, баш ийген ведомствого караштуу жана аймактык органдарынын кызматкерлери өздөрүнүн ыйгарым укуктарынын деңгээли, ошондой эле Улуттук статистика комитетинде маалыматты иштеп чыгуунун талаптарын жана тартибин аныктаган уюштуруучулук тескөөчү, ченемдик, техникалык документтер менен таанышышы керек.

Улуттук статистика комитетинин маалыматтык ресурстары менен иштеген ар бир адам үчүн милдеттүү болгон эрежелерге атайылап же билинбеген төмөнкү аракеттерге тыюу салынат - Улуттук статистика комитетинин маалымат системасынын компоненттеринин түзүк иштешин буза турган, кошумча ресурстук чыгымдарды алып келе турган, сакталган жана иштетилген маалыматтын бүтүндүгүн буза турган, мыйзамдуу пайдалануучулардын, маалыматтык мамилелердин субъекттеринин, жеке маалыматтардын субъекттеринин кызыкчылыктарын буза турган.

Улуттук статистика комитетинин ички маалыматтык системанын бардык маалыматтарын пайдалануучулар Улуттук статистика комитетинин маалыматтык коопсуздугун камсыз кылуу боюнча уюштуруу-тескөөчү документтери менен таанышууга тийиш.

Аларга тиешелүү бөлүгүндө алар маалыматтын коопсуздугун камсыз кылуу боюнча нускамаларды жана жалпы милдеттерди билиши жана так аткарышы керек.

Корголгон маалыматты иштеп чыгууга ыйгарым укуктуу адамдар көрсөтүлгөн документтердин талаптарын жеткирүүдө кол коюга тийиш.

22. Маалыматтык коопсуздук түзмөктөрү

Улуттук статистика комитетинин маалыматтык коопсуздугун камсыз кылуу үчүн төмөнкү коргоо чараларын колдонулат:

1) пайдалануучуларды идентификациялоо жана аутентификациялоо чаралары;

Уруксатсыз адамдардын Улуттук статистика комитетинин маалымат системанын ресурстары менен иштөөсүнө жол бербөө максатында ар бир мыйзамдуу пайдалануучуну (же пайдалануучулардын топторун) тааануу мүмкүнчүлүгүн камсыз кылуу зарыл.

Идентификациялоо үчүн түзүлүштүн ар кандай түрлөрү колдонулушу мүмкүн: магниттик карталар, ачкычтар, негизги койгучтар ж. б.

Түзмөктөрдүн ар кандай түрлөрүн аныктоо үчүн колдонууга болот: магниттик карталар, ачкычтар, негизги тиркемелер ж.б.

Пайдаланууучулардын аутентификациясы да жүргүзүлүшү мүмкүн:

– пайдаланууучулардын атайын түзмөктөрү бар-жогун текшерүү менен (магниттик карталар, ачкычтар, негизги тиркемелер ж.б.);

– сырсөздөр тууралуу билимдерин текшерүү менен;

– атайын биометриялык түзмөктөрдү колдонуу менен пайдаланууучулардын уникалдуу физикалык өзгөчөлүктөрүн жана параметрлерин текшерүү менен.

2) жеткиликтүүлүктү чектөө жабдулары;

Коргоонун техникалык жабдулардын жоопкерчилик зоналары жана милдеттери ушул жабдулардын документтеринде баяндалган алардын мүмкүнчүлүктөрүнө жана эксплуатациялык мүнөздөмөлөрүнө жараша белгиленет.

Жеткиликтүүлүктү чектөөнүн техникалык түзмөктөрү мүмкүн болушунча жеткиликтүүлүктү көзөмөлдөөнүн бирдиктүү системасынын ажырагыс бөлүгү болууга тийиш:

– көзөмөлдөнүүчү аймакка; өзүнчө жайларга (бөлмөлөргө);

– Улуттук статистика комитетинин маалыматтык чөйрөсүнүн компоненттерине жана маалыматтык коопсуздук системанын бөлүктөрүнө (физикалык жеткиликтүүлүк);

– маалымат ресурстарына (документтерге, маалымат сактагычтарга, файлдарга, маалыматтар топтомдоруна, архивдерге, аалымдамаларга ж. б.);

– активдүү ресурстарга (колдонмо программаларга, тапшырмаларга ж.б.);

– операциондук системага, системалык программаларга жана коргоо программаларына.

3) бүтүндүгүн камсыз кылуу жана көзөмөлдөө жабдулары;

Бүтүндүк куралдарына резервдик көчүрүү түзмөктөрү, антивирустук коргоо программалары, операциондук чөйрөнүн жана маалымат базасынын бүтүндүгүн калыбына келтирүү программалары кирет.

Системанын маалыматтык ресурстарынын бүтүндүгүнө көзөмөлдөө жүргүзүү түзмөктөрү системанын ресурстарын өзгөртүүнү же бурмалоону өз убагында аныктоого арналган.

Алар коопсуздук системанын туура иштешин жана сакталган жана иштетилген маалыматтардын бүтүндүгүн камсыз кылууга мүмкүндүк берет.

Берилген кайра иштетүү технологиясы менен аныкталган маалыматтык чөйрөнүн өзгөрбөстүгүн камсыз кылуу үчүн маалыматтын жана коргоо түзмөктөрүн бүтүндүгүнө көзөмөлдөө жүргүзүү жана маалыматты уруксатсыз өзгөртүүдөн коргоо:

– жеткиликтүүлүктү дифференциациялоо түзмөктөрү (үй-жайларга, документтерге, маалыматтарды ташуучуларга, серверлерге, логикалык түзмөктөргө ж.б.);

– электрондук санариптик кол коюу түзмөктөрү; бухгалтердик эсеп

түзмөктөрү;

– текшерүү суммаларды эсептөө түзмөктөрү (колдонулган программалык камсыздоо үчүн).

4) коопсуздук окуяларын ыкчам көзөмөлдөө жана каттоо түзмөктөрү;

Объективдүү көзөмөлдөө инструменттери саясаттын бузулушуна алып келиши жана кризистик жагдайларга алып келиши мүмкүн болгон бардык окуяларды (колдонуучулардын иш-аракеттерин, уруксатсыз кирүү аракеттерин ж.б.) аныктоону жана катталышына камсыз кылууга тийиш.

Каттоо каражаттары менен чогултулган маалыматты талдоо укук бузуулардын жасалгандыгынын фактыларын, алардын мүнөзүн аныктоого, аны иликтөөнүн ыкмасын жана бузуучуну издөөнүн жана кырдаалды оңдоонун ыкмаларын сунуштоого мүмкүндүк берет.

Көзөмөлдөө жана каттоо түзмөктөрү төмөнкүлөрдү камсыз кылууга тийиш:

– коопсуздук окуяларын каттоо журналдарын (системалык журналдарды) жүргүзүү жана талдоо;

– коопсуздук окуяларынын каттоо журналынын кагазга (басма) көчүрмөсүн алуу;

– журналдарды тартипке келтирүү, ошондой эле аларды сактоо мөөнөтүнө чектөөлөрдү белгилөө;

– тартип бузуулар жөнүндө коопсуздуктун администраторуна ыкчам билдирүү.

Коопсуздук окуяларын каттоодо журналга төмөнкү маалыматтар жазылууга тийиш;

– окуянын мезгили (датасы) жана убактысы;
– катталуучу иш-аракетти жүзөгө ашыруучу субъекттин идентификатору;
– иш – аракет (жеткиликтүүлүк түрү).

5) криптографиялык түзмөктөрү.

Улуттук статистика комитетинин корпоративдик маалыматтык системасынын коопсуздук системанын негизги элементтери болуп криптографиялык ыкмалар жана коргоо түзмөктөрү саналат.

Криптографиялык методдорду колдонуунун келечектүү багыты болуп ачык ачкычтарды (PKI - Public Key Infrastructure) колдонуу менен коопсуздук инфраструктурасын түзүү саналат.

Улуттук статистика комитетинин алыскы аймактык органдарынын, Улуттук статистика комитетинин кошумча кеңселеринин жана өнөктөштөрүнүн ортосунда криптографиялык коргоо түзмөктөрүн колдонуунун негизинде коопсуз онлайн өз ара аракеттенүүсүн уюштурууга мүмкүндүк берет:

– Улуттук статистика комитетинин байланыш каналдары аркылуу берилүүчү жашыруун маалыматтарын коргоо;

– Улуттук статистика комитеттин борбордук аппаратынын, баш ийген ведомстволук жана аймактык органдарынын маалымат системасын (ички локалдык компьютердик тармактарды) уруксатсыз тышкы таасирлерден коргоого;

– ресурстарды башкарууну борборлоонун аркасынан Улуттук статистика комитетинин маалыматтык өз ара иштешүүсүн натыйжалуураак кылууга;

– алыскы бөлүмдөрдүн тармактарын башкаруу боюнча чыгымдарды оптималдаштыруу.

Маалыматты берүү учурунда, ошондой эле байланыш каналдары аркылуу купуялуулукту жана коргоону абоненттик шифрлөөнү колдонуу аркылуу да камсыздалууга тийиш.

Бөлүштүрүлгөн маалыматтык ресурстары бар түзүм болуп саналган корпоративдик маалыматтык системада билдирүүлөрдүн бүтүндүгүн жана аныктыгын юридикалык жактан далилдөөнү, ошондой эле пайдаланууучулардын аутентификациясын, абоненттик пункттардын жана билдирүүлөрдү жөнөтүү убактысын тастыктоону камсыз кылган электрондук санариптик кол тамганы түзүү жана текшерүү түзмөктөрүн пайдаланылууга тийиш.

Коргоо түзмөктөрү Улуттук статистика комитетинин маалыматтык системасынын бардык сезгич ресурстарына, алардын түрүнө жана маалымат берүү формасына карабастан колдонулууга тийиш.

V. Акыркы жоболор

23. Улуттук статистика комитетинин маалыматтык системасынын ресурстарын пайдалануунун белгиленген тартибин бузгандыгы үчүн жоопкерчилик

Улуттук статистика комитетинин маалыматтык ресурстарын пайдалануу тартибин жана эрежелерин одоно бузуулар иликтенүүгө тийиш. Күнөөлүүлөргө тийиштүү түрдө таасир этүү чаралары колдонулушу керек.

Улуттук статистика комитетинин маалыматтык ресурстарын пайдалануучулардын маалымат менен коопсуз иштөөнү камсыз кылуунун белгиленген эрежелерин бузуу менен жасаган аракеттери үчүн жоопкерчилигинин көлөмү келтирилген зыян, зыяндуу ниеттиктин бар экендиги жана Улуттук статистика комитетинин жетекчилигин кароосу боюнча аныкталууга тийиш.

24. Улуттук статистика комитетинин маалыматтык коопсуздук саясатына өзгөртүүлөрдү жана толуктоолорду киргизүү

Ушул саясат Улуттук статистика комитетинин төрагасынын буйругу менен бекитилет.

Бул саясатка өзгөртүүлөр жана толуктоолор Улуттук статистика комитетинин жетекчилигинин, Улуттук статистика комитетинин маалыматтык коопсуздугун камсыз кылуу боюнча жооптуу бөлүмдүн (адамдын) демилгеси менен киргизилет жана Улуттук статистика комитетинин төрагасынын буйругу менен бекитилет.