1-тиркеме

*(Кыргыз Республикасынын Өкмөтүнүн 2019-жылдын 24-июлундагы № 369 токтомуна)*

**2019-2023-жылдарга Кыргыз Республикасынын киберкоопсуздук СТРАТЕГИЯСЫ**

## I. Киришүү

Бүгүнкү күндө маалыматтык-коммуникациялык технологиялар (мындан ары - МКТ) дүйнөлүк экономиканы жана ага көз каранды болгон багыттар менен сегменттерди өнүктүрүү динамикасын аныктаган кыйла кеңири тараган, өзөктүү глобалдуу технологиялардын бири болуп калды.

Маалыматтык технологиялардын жана байланыштын глобалдык тармагынын борбордук негизин Интернет түзөт. Эл аралык электр байланыш бирлигинин маалыматы боюнча 2018-жылдын аягына карата глобалдуу тармакка дээрлик 3,9 млрд. адамдын жетүү мүмкүнчүлүгү бар. Интернет технологиясын жайылтуу тенденциясы жыл сайын өсүүдө жана Эл аралык электр байланыш бирлигинин болжолу боюнча 2023-жылы дүйнө элинин 70 пайызы интернетке жетүүгө мүмкүндүк алат.

Маалыматтык-коммуникациялык технологиялар экономикалык, чарбалык, башкаруучу жана башка иштин бардык тармагында бизнес-процесстерди аналогдон санариптик форматка глобалдык өзгөрткүчтүн ролун аткарууда, айрым жарандардын, бизнестин, мамлекеттин деңгээлинде, ошондой эле эл аралык деңгээлде ар тараптуу аракеттенүүнү трансформациялоого көмөктөшөт.

Санариптештирүүнүн глобалдык тенденциясы жогору болгон кошумча наркты түзүүдө ар кандай процесстердин, бүтүмдөрдүн жана башка аракеттенүүнүн убакыттык, материалдык, административдик жана башка чыгымдарын кыскартат.

Кыргыз Республикасы аталган шартта улуттук экономиканы санариптик трансформациялоого жана жарандардын азыркы санариптик сервистерге жетүүсүн камсыздоого өзү кадам таштоодо. Ушул Стратегиянын алкагында санариптик экономиканы куруу Кыргыз Республикасынын кыска жана узак мөөнөттүү келечектеги өнүгүшүнүн зарыл шарты жана улуттук артыкчылыгы катары каралат. Кыргыз экономикасынын санариптик трансформациялоо стратегиясынын алгачкы пайдубалы Кыргыз Республикасынын Коопсуздук кеңешинин 2018-жылдын 14-декабрындагы № 2 чечими менен жактырылган "Санарип Кыргызстан 2019-2023" Санариптик трансформациялоо концепциясынын (мындан ары - Концепция) алкагында калыптанат.

Аталган Концепциянын алкагында жана улуттук экономиканы санариптик трансформациялоонун мүмкүн болуучу башка демилгелеринде коюлган милдеттерди чечүү жана максаттарга жетүү үчүн зарыл шарт болуп тийиштүү инфраструктуралардын, сервистердин жана бизнес-процесстердин коопсуздугун камсыздоо эсептелет. Мында маалыматтык-коммуникациялык технологияларды жана санариптик экономиканы өнүктүрүү белгилүү тобокелдиктер менен коркунучтарды алып келе тургандыгын түшүнүү керек. Бирок азыркы учурда Кыргыз

Республикасында базалык шарттар түзүлгөн эмес, аларсыз санариптик трансформациялоо коопсуздугун, атап айтканда маалыматтык технологиялардын, жалпысынан байланыштын улуттук тармагын өнүктүрүү мүмкүн эмес. Анын ичинде:

- доктриналык негизди түзүүчү жана киберкоопсуздукту камсыздоо жаатындагы мамлекеттик саясат үчүн бирдиктүү "координаталар системасы" катары каралуучу алкактык документ жок;

- ченемдик укуктук актылар системасында жана киберкоопсуздукту камсыздоо саясатында олуттуу кемчиликтер бар (компьютердик инциденттерге, Кыргыз Республикасынын олуттуу маалыматтык инфраструктурасынын коопсуздугун камсыздоого, киберкоопсуздукту камсыздоо жаатындагы эл аралык кызматташтыкка таасир этүү системасынын жана ыкманын жоктугу);

- ченемдик укуктук актылардын системасы жана аларда берилген маалыматтык технологиялардын жана маалыматтык-коммуникациялык технологиялардын чөйрөсүн жөнгө салуу ыкмалары мамлекеттик саясаттын багыттарында анын толук эместиги жана маалыматтык-коммуникациялык технологиялардын, киберкоопсуздуктун өнүгүүсүнүн актуалдуу тенденцияларынан артта калгандыгы байкалат (компьютердик кылмыштуулукка каршы аракеттенүү, маалыматты коргоо жаатындагы жөнгө салуу, маалыматтык технологиялар жаатындагы техникалык стандартташтыруу);

- компьютердик гигиенанын жана санариптик сабаттуулуктун керектүү деңгээлин камсыздоого, ошондой эле жалпысынан киберкоопсуздук чөйрөсүндө мамлекеттик саясатты ишке ашыруучу түрдүү субъекттердин (мамлекеттик жарандык кызматкерлердин, укук коргоо органдарынын кызматкерлеринин) потенциалын өстүрүү ыкмасы бир калыпка салынган эмес.

Аталган көйгөйлөрдү чечүү жана кемчиликтерди жоюу үчүн киберкоопсуздукту камсыздоонун улуттук системасын куруу боюнча иштин стратегиялык багыттарын жана принциптеринин системасын түзүү зарыл, булар ушул жааттагы Кыргыз Республикасынын мамлекеттик саясатын калыптандыруу жана ишке ашыруу үчүн негиз болуп берет. Мында эл аралык тажрыйбаны, мыкты практикаларды жана сунуштарды эске алуу менен Кыргыз Республикасынын өзгөчө шарттарына жараша аракет кылуу керек, аталган шарттарга төмөнкүлөр кирет:

- Кыргыз Республикасынын кургакта жайгашуусу, деңизге чыга албагандыгы, региондогу маалыматтык-телекоммуникациялык инфраструктуранын салыштырмалуу начар өнүккөндүгү;

- маалымат коопсуздугу жаатындагы Кыргыз Республикасынын мыйзамдарынын, техникалык жөнгө салуу системасынын жана мамлекеттик институттарынын СССРден бери келе жаткан жарым-жартылай тарыхый уланмалуулугу жана постсоветтик мейкиндиктин интеграциялык форматтарына тарыхый жактан шартталган багыт алуусу. Бул өзгөчөлүк киберкоопсуздуктун түшүнүк аппаратына, маалыматтык технологиялар жана байланыш жаатындагы маалыматты криптографиялык коргоонун жана техникалык стандартташтыруунун каражаттарын жөнгө салууга карата ыкмаларды иштеп чыгуунун маанилүүлүгүн күчөтөт, ал жөнгө салуунун тарыхый калыптанган системасын бузбастан, Кыргыз Республикасынын мамлекеттик саясатын мыкты эл аралык практикага жана тажрыйбага ылайык келтирүүгө мүмкүндүк берет;

- маалыматты криптографиялык коргоо каражаттарын тестирлөө жана сертификациялоо, ЕАЭБ форматынын алкагында мамлекеттер аралык электрондук аракеттенүүнү уюштуруу маселелеринде Кыргыз Республикасынын көз карандылыгы. Бул фактор мындай маселелерди өз алдынча чечүү үчүн Кыргыз Республикасынын улуттук ресурстарын жана институттук механизмдерин түзүү зарылдыгын шарттайт;

- Кыргыз Республикасындагы маалыматтык технологиялар жана байланыш тармактарынын каражаттарынын жана чечимдеринин, анын ичинде киберкоопсуздук багытындагы ички рыноктун кыйла аз көлөмү жана программалык-аппараттык продукциянын чет элдик жөнөтүүчүлөрүнө толук көз карандылыгы. Бул жагдай маалыматтык технологиялар чөйрөсүндөгү ташып келинген продукцияны улуттук сертификациялоо системасын өнүктүрүү, ошондой эле техникалык бейтараптыкты жана суверенитетти сактоо үчүн анын кемчиликтерин жана декларацияланбаган мүмкүндүктөрүн тестирлөө боюнча милдеттин маанилүүлүгүн жогорулатат.

## II. Киберкоопсуздук стратегиясынын негизги принциптери

1. Инсандын, коомдун жана мамлекеттин кызыкчылыктарынын балансын сактоо. Бул Стратегияны ишке ашыруунун баштапкы субъекти жана пайда табуучусу болуп Кыргыз Республикасынын жарандары эсептелет. Стратегиянын максаттарына жетүү үчүн материалдык жана финансылык ресурстарды бошотуу жана иш жүзүндө натыйжалуу ишке ашыруу маалыматтык технологиялар жана байланыш тармагындагы мамлекеттик-жеке менчик аракеттенүү механизмдерин өнүктүрүүнүн, ошондой эле киберкоопсуздукту камсыздоо жаатындагы демилгелерди өнүктүрүү үчүн ченемдик укуктук жана башка административдик тоскоолдуктарды азайтуунун эсебинен камсыздалат.

2. Комплекстүү мүнөзү. Стратегиянын алкагында Кыргыз Республикасынын киберкоопсуздукту камсыздоо жаатындагы мамлекеттик саясаттын комплекстүү, бирдиктүү жана өтмө системасын түзүүнүн пайдубалы камсыз кылынат:

1) мамлекеттик саясаттын комплекстүү мүнөзү бардык негизги багыттар, бардык секторлор боюнча киберкоопсуздукту камсыздоо милдетин камтыйт, мында бул багыттар жана секторлор өз алдынча эмес, өз ара байланышта каралат;

2) мамлекеттик саясаттын бирдиктүү мүнөзү коюлган маселелерди чечүүдө Кыргыз Республикасынын министрликтеринин жана ведомстволорунун жалпы координациясын жана иштешин, ошондой эле мамлекеттик органдардын жана жеке сектордун, академиялык жана инженердик-техникалык коомдордун, өкмөттүк эмес уюмдардын ортосундагы тыгыз аракеттенүүсүн болжолдойт;

3) мамлекеттик саясаттын өтмө мүнөзү жалпысынан алганда өз алдынча жарандан тартып мамлекетке чейинки бардык деңгээлде чараларды иштеп чыгууну жана ишке ашырууну билдирет.

3. Кооптуу маалыматтык инфраструктуранын коопсуздугун камсыздоонун артыкчылыгы. Кыргыз Республикасынын кооптуу маалыматтык инфраструктуранын киберкоопсуздугун камсыздоо киберкоопсуздукту камсыздоо жаатындагы мамлекеттик саясатты түзүүнүн жана ишке ашыруунун негизги звеносу болуп эсептелет. Ошол эле мезгилде бул жааттагы системалык ыкмалардын жана ченемдик укуктук базанын жоктугу ата мекендик экономиканы санариптик трансформациялоо процессинде киберкоопсуздукту камсыздоого кыйла олуттуу тоскоолдук болууда. Ушул жааттагы мамлекеттик саясатты ийгиликтүү ишке ашыруунун маанилүү шарттары төмөнкүлөр: критерийлер жана өлчөнүүчү параметрлер системасынын негизинде кооптуу маалыматтык инфраструктуранын объекттерин так аныктоо; жеке сектор менен бирге активдүү иш алып баруу, кооптуу маалыматтык инфраструктуранын киберкоопсуздугун камсыздоо боюнча чаралардын жана талаптардын комплекстүү системасын түзүү. Мында маалымат системаларындагы маалыматтын жеткиликтүүлүгүн, бүтүндүгүн жана купуялыгын камсыздоо, ошондой эле компьютердик чабуул жана компьютердик инцидент болгон шартта кооптуу маалыматтык инфраструктурадагы объекттердин туруктуулугун жана үзгүлтүксүз иштөөсүн камсыздоо башкы милдет болуп саналат.

"Инцидентти алдын алуу - инцидентти башкаруу - инциденттен кийин калыбына келтирүү" байланышында ченемдик, уюштуруу, техникалык жана башка чаралар менен ресурстардын эсебинен инциденттерди алдын алууга артыкчылык берилет.

4. Стратегиянын максаттарын социалдык-экономикалык өнүгүүнүн, анын ичинде Кыргыз Республикасынын улуттук экономикасын санариптик трансформациялоонун жалпы милдеттерине коштоо жана ылайык келтирүү. Жарандардын, коомдун жана мамлекеттин киберкоопсуздугун камсыздоо өз алдынча милдет катары Кыргыз Республикасындагы маалыматтык технологиялар жана байланыш тармагын өнүктүрүүнүн жалпы контекстине ылайык келип, Кыргыз Республикасындагы маалыматтык технологиялар жана байланыш тармагын өнүктүрүү деңгээлин көтөрүү, электрондук башкаруу кызматы жана электрондук документтерди жүгүртүү сервистерин өркүндөтүү, ошондой эле Концепцияны жүзөгө ашыруу боюнча мамлекеттик саясаттын ажырагыс бөлүгү катары ишке ашырылууда. Киберкоопсуздукту камсыздоого зарыл ресурстарды инвестициялоо Кыргыз Республикасынын экономикасынын санариптик трансформациялоо поцесстерин токтотпошу керек.

5. Этап-этабы менен өтүү жана ресурстук чектөөлөрдү эсепке алуу. Кыргыз Республикасынын киберкоопсуздугунун стратегиясы жана аны ишке ашыруу боюнча иш-аракеттер планы 2023-жылга чейинки чекте этап-этабы менен милдеттерди бөлүштүрүүнү, милдеттерге артыкчылык берүүнү, башталгыч этаптагы болгон ресурстук чектөөлөрдү эсепке алууну карайт. Биринчи кезекте киберкоопсуздук жаатындагы мамлекеттик саясатты ишке ашыруу үчүн зарыл болгон Кыргыз Республикасынын институттарынын, мыйзамдарынын жана жөнгө салуу концепцияларынын системасындагы негизги кемчиликтердин ордун толтуруу талап кылынат (киберкоопсуздуктун түшүнүк аппараты, кооптуу маалыматтык инфраструктуранын коопсуздугун камсыздоо жаатындагы ченемдик укуктук актылар, компьютердик инциденттерге жооп берүүнүн улуттук системасынын уюштуруу-укуктук негиздери, киберкоопсуздукту камсыздоо жаатындагы мамлекеттик саясатты ведомстволор аралык координациялоо системасы, эл аралык кызматташтык жаатындагы техникалык стандартташтыруу жана демилгелер системасын өнүктүрүү жана башкалар). Финансылык, материалдык-техникалык жана адам ресурстары боюнча чектөөлөр бир катар милдеттерди ишке ашырууну кыйла кийинки мезгилге жылдырат (компьютердик инциденттерге жооп берүү борборлорунун терең тармактык адистешүүсү, өздүк криптографиялык стандарттар системасын өнүктүрүү, Кыргыз Республикасынын өздүк киберкоргонуу системасын түзүү, Интернет, маалыматтын чоң көлөмү, бөлүштүрүлгөн реестрлер сыяктуу санариптик инфраструктуранын жаңы багыттары үчүн киберкоопсуздуктун адистештирилген саясатын иштеп чыгуу жана башкалар).

6. Колдонуудагы ченемдик укуктук актыларга карата интеграция жана уланмалуулук. Кыргыз Республикасында түзүлүп калган маалыматтык коопсуздукту камсыздоо жаатындагы мамлекеттик саясаттын максаттары, мазмуну жана принциптеринин ортосундагы карама-каршылыктын болбогону маанилүү шарт болуп эсептелет. Бул Стратегияда маалыматтык технологиялар бөлүгүндөгү техникалык стандартташтыруу жана техникалык жөнгө салуу жаатындагы саясаттын колдонулуп жаткан негиздерин жокко чыгаруунун же кайра карап чыгуунун зарылдыгын жаратпайт, ошондой эле Кыргыз Республикасы катышкан, мыйзамда белгиленген тартипте күчүнө кирген эл аралык келишимдердин жана колдонулуп жаткан ченемдик укуктук актылардын учурдагы системасына каршы келбейт.

7. Киберкоопсуздукту камсыздоо жаатындагы эл аралык кызматташтыктын артыкчылыктуу ролу жана көп вектордуу мүнөзү. Стратегияда киберкоопсуздукту

камсыз кылуу жаатындагы эл аралык кызматташтыктын ар кандай форматтарына жана жумушчу процесстерине Кыргыз Республикасынын активдүү катышуусу каралган. Мындай кызматташтыкта Кыргыз Республикасынын негизги принциби болуп анын көп вектордуу мүнөзү жана саясаттан максималдуу алыстыгы эсептелет.

## III. Максаты жана милдеттери

8. Бул Стратегиянын жана Иш-аракеттер планынын максаты кибермейкиндикте жарандардын, ишкердиктин жана мамлекеттин маанилүү турмуштук кызыкчылыктарын коргоого мүмкүндүк берген коопсуздуктун тиешелүү деңгээлин камсыздоо үчүн киберкоопсуздуктун ата мекендик системасын жана саясатын калыптандыруу жана Кыргыз Республикасынын туруктуу социалдык-экономикалык өнүгүшүн, анын ичинде экономиканын санариптик трансформациялоосун камсыздоо болуп саналат.

9. Стратегия "Санарип Кыргызстан 2019-2023" санариптик транформациялоо концепциясын ишке ашыруу боюнча "жол картасынын" иш-чаралар комплекси менен байланышта ишке ашырылат.

10. Стратегиянын жана Иш-чаралар планынын милдеттери төмөнкүлөр:

1) Кыргыз Республикасынын киберкоопсуздугун камсыздоонун бирдиктүү системасынын жана саясатынын негизин калыптандыруу;

2) киберкоопсуздук жаатында бирдиктүү түшүнүктүк жана методикалык аппаратты калыптандыруу;

3) компьютердик инциденттердин алдын алуунун, жооп берүүнүн жана башкаруунун ата мекендик системасын калыптандыруунун жана өнүктүрүүнүн эсебинен Кыргыз Республикасынын маалыматтык инфраструктура объекттеринде компьютердик инциденттердин санын кыскартуу жана кесепеттерин азайтуу;

4) маалыматты коргоо каражаттарын жана маалыматты криптографиялык коргоо каражаттарын тестирлөө жана сертификаттоо системасынын уюштуруу-техникалык жана ченемдик укуктук негизин калыптандыруу;

5) киберкоопсуздук жана маалыматты коргоо жаатында улуттук стандарттардын системасын модернизациялоо;

6) киберкоопсуздукту камсыздоо жаатында Кыргыз Республикасынын мамлекеттик саясатын ишке ашыруу үчүн кадрдык потенциалдын деңгээлин жогорулатуу.

11. Коюлган маселелерди чечүүнүн натыйжасында кооптуу маалыматтык инфраструктуранын объекттерин резервдөөнү, компьютердик инциденттердин жана компьютердик чабуулдардын шартында кооптуу маалыматтык инфраструктуранын объекттеринин үзгүлтүксүз иштөөсүн жана мындай объекттерде олуттуу компьютердик инциденттерди болтурбоону кошо алганда кооптуу маалыматтык инфраструктуранын коопсуздугун камсыздоого мүмкүн; компьютердик кылмыштуулукка каршы күрөшүү жаатында мыйзамдарды өркүндөтүүнүн, компьютердик кылмыштарды териштирүүнүн, бул жаатта эл аралык кызматташтыкты активдештирүүнүн эсебинен маалыматтык-коммуникациялык технологияларды пайдалануу менен жасалуучу мыйзамсыз иш-аракеттердин (компьютердик кылмыштардын) санын кыскартуу жана зыян келтирилишин азайтууга болот.

## IV. Негизги түшүнүктөр

12. Стратегияда төмөнкүдөй терминдер жана аларга тиешелүү аныктамалар колдонулат:

**маалымат мейкиндиги** - маалыматтык инфраструктурага жана маалыматка таасир этүүчү, анын ичинде жеке жана коомдук аң-сезимге таасир этүүчү маалыматты калыптандыруу, түзүү, кайра түзүү, өткөрүп берүү, пайдалануу, сактоого байланышкан иштин комплекстүү чөйрөсү;

**кибермейкиндик** - маалымат мейкиндигиндеги иштин чөйрөсү, ал маалыматтык-телекоммуникациялык тармактардын (Интернет глобалдык маалыматтык-телекоммуникациялык тармагын кошо алганда) жана маалыматтык инфраструктуранын башка түрү аркылуу ишке ашырылуучу адамдардын, программалык камсыздоонун жана сервистердин бирге аракеттенүүсүнүн ар кандай формаларынын эсебинен түзүлөт;

**киберкоопсуздук** - коопсуздукту камсыздоо каражаттарынын, стратегияларынын, принциптеринин, коопсуздук кепилдигин, тобокелдерди жана камсыздандырууну башкаруу ыкмаларын, кесиптик даярдыктын, практикалык тажрыйбанын жана технологиялардын жыйындысын колдонуунун эсебинен камсыздалуучу маалыматтык инфраструктуранын объекттериндеги маалыматтын бүтүндүгүн (бул бирдейликти жана туруктуулукту камтышы мүмкүн), жеткиликтүүлүк жана купуялык касиеттерин сактоо;

**маалыматтык инфраструктура** - маалыматты калыптандыруу, түзүү, кайра түзүү, өткөрүп берүү, пайдалануу жана сактоо үчүн, ошондой эле технологиялык процесстерди башкаруу үчүн колдонулуучу технологиялык процесстерди башкаруунун маалыматтык системаларынын, маалыматтык-телекоммуникациялык тармактардын жана автоматташтырылган системалардын жыйындысы;

**Кыргыз Республикасынын кооптуу маалыматтык инфраструктурасы** - мамлекеттик башкаруу жана мамлекеттик электрондук кызмат көрсөтүүлөр секторунда, саламаттык сактоо, транспорт, телекоммуникация жана байланыш тармактарында, кредиттик-финансы чөйрөсүндө, коргонуу секторунда, отун өнөр жайында, электр энергиясын генерациялоо жана бөлүштүрүү тармагында, тамак-аш өнөр жайында жана тоо-кен өнөр жайында иштөөчү мамлекеттик маалыматтык системалардын, мамлекеттик маалыматтык-телекоммуникациялык тармактардын жана технологиялык процесстерди башкаруунун автоматташтырылган системаларынын жыйындысы;

**Кыргыз Республикасынын кооптуу маалыматтык инфраструктурасынын объекттери** - мамлекеттик башкаруу жана мамлекеттик электрондук кызмат көрсөтүүлөр секторунда, саламаттык сактоо, транспорт, телекоммуникация жана байланыш тармактарында, кредиттик-финансы чөйрөсүндө, коргонуу секторунда, отун өнөр жайында, электр энергиясын генерациялоо жана бөлүштүрүү тармагында, тамак-аш өнөр жайында жана тоо-кен өнөр жайында иштөөчү мамлекеттик маалыматтык системалар, мамлекеттик маалыматтык-телекоммуникациялык тармактар жана технологиялык процесстерди башкаруунун автоматташтырылган системалары (мындан ары - мамлекеттик системалар);

**компьютердик чабуул** - маалымат системаларына, маалыматтык-телекоммуникациялык тармактарга, байланыш каражаттарына жана технологиялык процесстерди башкаруунун автоматташтырылган системаларына алардын иштөөсүн бузуу жана (же) алар иштеп чыгуучу маалыматтын коопсуздугун бузуу максатында программалык же программалык-аппараттык каражаттар менен максаттуу таасир этүү;

**компьютердик инцидент** - маалыматтык инфраструктуранын объектинин иштөөсүн бузуу же токтотуу жана (же) мындай объект иштеп чыгуучу маалыматтын, анын ичинде компьютердик чабуул менен чакырылган коопсуздугун бузуу окуясы.

## V. Киберкоопсуздукту камсыздоо жаатындагы мамлекеттик саясатты түзүү ишинин негизги багыттары

### 5.1. Киберкоопсуздукту камсыздоо чараларынын бирдиктүү системасын түзүү

13. Кыргыз Республикасынын киберкоопсуздугун камсыздоо чөйрөсүндөгү мамлекеттик саясаттын комплекстүү, бирдиктүү жана өтмө системасын куруу боюнча маселелерди чечүүнүн алкагында 2023-жылга чейинки убакыттын чегинде төмөнкүдөй чаралар ишке ашырылат:

1) Киберкоопсуздукту камсыздоо жаатындагы мамлекеттик саясатты калыптандыруу жана ишке ашыруу маселелери боюнча ведомстволор аралык өз ара аракеттенүүнү бекемдөө.

Кыргыз Республикасынын мамлекеттик саясатынын бирдиктүү системасын түзүү үчүн тармактык мамлекеттик органдардын киберкоопсуздук коркунучтары жана инциденттери тууралуу маалымат алмашуу, киберкоопсуздукту камсыздоо чараларын ишке ашырууга баа алуу жана берүү, жөнгө салуунун ведомстволук ыкмаларынын учурдагы өнүгүүсү жана башка маселелердин системалуу аракеттенүүсүн жөнгө салуу зарыл.

Буга байланышкан маселе киберкоопсуздук маселелерин иштеп чыгуу үчүн бирге иш жүргүзүү, киберкоопсуздукту камсыздоо жаатындагы мамлекеттик саясаттын көп деңгээлдүү маселелерин өз убагында иштеп чыгуу жана чечүү максатында аткаруу жана мыйзам чыгаруу бийлигинин ортосунда диалог жүргүзүүнүн жана аракеттенүүнүн түз каналдарын жөнгө салуу болуп саналат.

Натыйжалуу өз ара аракеттенүүнү камсыздоо максатында Кыргыз Республикасынын Өкмөтүнө караштуу консультациялык жана координациялык аянтча каралууда, ал төмөнкү функциялардын аткарылышын камсыздоого тийиш:

а) кызыкдар мамлекеттик органдардын же ишканалардын, мекемелердин жана менчигинин түрүнө карабастан башка уюмдардын киберкоопсуздук чөйрөсүндөгү өз ара аракеттенүүсүн координациялоо жана жакшыртуу;

б) киберкоопсуздук жана кооптуу маалыматтык инфраструктуранын коопсуздугун камсыздоо боюнча бирдиктүү саясатты калыптандыруу;

в) киберкоопсуздукту ички мамлекеттик деңгээлде камсыздоо жаатындагы саясаттын маселелери боюнча позицияны макулдашуу жана талкуулоо, белгилөө жана сунуштоо;

г) Кыргыз Республикасынын Жогорку Кеңешине жана Кыргыз Республикасынын Президентине ченемдик укуктук актылардын, уюштуруу-техникалык жана башка чаралардын жоболорунун, ошондой эле киберкоопсуздукту камсыздоо жаатында мамлекеттик саясаттын алкагындагы иш-чаралардын аткарылышы тууралуу отчётторду үзгүлтүксүз берип туруу;

д) Кыргыз Республикасынын аткаруу бийлигинин органдарынын ортосунда киберкоопсуздукту камсыздоо жаатындагы мамлекеттик саясатты ишке ашыруу маселелери боюнча маалымат алмашууга жана башка өз ара аракеттенүүгө көмөк көрсөтүү;

ж) Кыргыз Республикасынын Киберкоопсуздук стратегиясынын жана аны ишке ашыруу, координациялоо, өнүктүрүү, толуктап иштеп чыгуу жана ушул документтерди жаңылоо боюнча Иш-аракеттер планынын аткарылышын контролдоо;

2) мамлекеттик бийлик органынын улуттук коопсуздукту камсыздоо маселелерин тейлеген киберкоопсуздукту камсыздоо жаатындагы ыйгарым укуктуу органды аныктоо:

а) профилдик регуляторду аныктоо ага киберкоопсуздукту камсыздоо жаатындагы аткаруучу бийлик органдарынын бардык функциялары жана милдеттери биригет дегенди түшүндүрбөйт - ар бир ведомство өзүнүн ыйгарым укуктарына ылайык киберкоопсуздук жаатындагы өзүнүн жоопкерчилигинин секторун сактайт.

Ошону менен бирге киберкоопсуздукту камсыздоо жаатындагы ыйгарым укуктуу орган төмөнкү маселелер боюнча жооптуу:

а) инсандын, коомдун жана мамлекеттин киберкоопсуздугун камсыздоо боюнча саясатты аныктоо;

б) кооптуу маалыматтык инфраструктуранын объекттерин коргоого карата белгиленген талаптарды сактоону камсыздоо, кооптуу маалыматтык инфраструктуранын объекттеринин операторлору менен өз ара аракеттенүү, кооптуу маалыматтык инфраструктуранын коопсуздугун камсыздоо системасын мындан ары өнүктүрүүнү, анын ичинде Кыргыз Республикасынын ченемдик укуктук актыларын иштеп чыгууну жана ишке ашырууну координациялоо;

в) компьютердик инциденттерге жооп берүү боюнча Улуттук борбордун ишин контролдоо жана координациялоо;

г) компьютердик инциденттерге жооп берүү боюнча борборлордун ишин координациялоо (жеке, финансылык жана башка);

д) Кыргыз Республикасынын мамлекеттик органдарынын жана жеке сектор уюмдарынын катышуусунда үзгүлтүксүз кибер окууларды өткөрүү ишин уюштуруу жана камсыздоо;

е) Кыргыз Республикасынын ченемдик укуктук актыларында белгиленген ыйгарым укуктардын алкагында эл аралык кызматташтыкты жүргүзүү;

ж) Кыргыз Республикасынын Өкмөтүнө Кыргыз Республикасынын коопсуздугун камсыздоо чөйрөсүндөгү тобокелдиктердин жана киберкоркунучтардын өсүү динамикасы тууралуу маалымдоо, ошондой эле негизги киберкоопсуздук инциденттер, анын ичинде кооптуу маалыматтык инфраструктурадагы инциденттер жана Кыргыз Республикасына тийгизүүчү кесепеттери тууралуу маалымдоо;

з) маалыматтык жана киберкоопсуздукту камсыздоо боюнча координациялык борбордун ишин уюштуруу жана камсыздоо;

и) компьютердик инциденттерге жооп берүү боюнча улуттук борбордун жана Кыргыз Республикасынын компьютердик инциденттерге жооп берүү боюнча башка (жеке, финансылык жана башка) борборлорунун ортосунда өз ара аракеттенүүнү уюштуруу.

3) улуттук коопсуздук маселелерин тейлеген Кыргыз Республикасынын маалыматтык жана киберкоопсуздукту камсыздоо боюнча координациялык борборду түзүү. Маалыматтык жана киберкоопсуздукту камсыздоо боюнча координациялык борбордун иши жана иштөө модели төмөнкүдөй параметрлерге дал келиши мүмкүн:

а) маалыматтык жана киберкоопсуздукту камсыздоо боюнча координациялык борбор мамлекеттик органдар, бизнес жана эксперттик коомчулук арасында киберкоопсуздукту камсыздоо маселелери боюнча ведомстволор аралык координациялоонун жана маалымат алмашуунун негизги механизми болуп саналат;

б) маалыматтык жана киберкоопсуздукту камсыздоо боюнча координациялык борбор киберкоопсуздук чөйрөсүндөгү инциденттердин жана коркунучтардын бирдиктүү базасын топтоо, талдоо жана калыптандыруу ишин жүргүзөт;

в) маалыматтык жана киберкоопсуздукту камсыздоо боюнча координациялык борбор мамлекеттик органдардын жана башка кызыкдар тараптардын, анын ичинде Кыргыз Республикасынын маалыматтык технологиялар жана байланыш тармагынын уюмдарынын, ошондой эле кооптуу маалыматтык инфраструктуранын объекттеринин операторлорунун ортосундагы киберкоопсуздукту камсыздоо жаатындагы мамлекеттик саясатты ишке ашыруу жана практикалык өз ара аракеттенүү маселелери боюнча диалог үчүн аянтча болот.

Маалыматтык жана киберкоопсуздукту камсыздоо боюнча координациялык борбордун аянтчасында киберкоопсуздукту камсыздоо жаатындагы мамлекеттик саясатты ишке ашыруу маселелери боюнча диалогду уюштуруу үчүн бардык кызыкдар тараптардын өкүлдөрүнүн, анын ичинде төмөнкүлөрдүн өкүлдөрүнүн катышуусунда үзгүлтүксүз талкуулар уюштурулууда:

а) профилдик мамлекеттик органдардын;

б) киберкоопсуздукту камсыздоо жаатындагы мамлекеттик саясатты ишке ашырууга катышкан Кыргыз Республикасынын мамлекеттик уюмдарынын жана техникалык түзүмдөрдүн;

в) Кыргыз Республикасынын жеке секторунун, анын ичинде маалыматтык технологиялар жана байланыш секторунун, ошондой эле маалыматтык технологиялар жана байланыш секторунун тармактык ассоциацияларынын;

г) академиялык чөйрөнүн, инженердик-техникалык коомчулуктун жана иш чөйрөсү маалыматтык технологиялар жана байланыш секторун камтыган Кыргыз Республикасынын өкмөттүк эмес уюмдарынын.

Маалыматтык жана киберкоопсуздукту камсыздоо боюнча координациялык борборго операциялык-техникалык функциялар жүктөлөт, анын ичинде:

а) киберкоопсуздуктун олуттуу инциденттери же мындай инциденттердин жогорку тобокелдиктери болгон учурда Компьютердик инциденттерге жооп берүү боюнча улуттук борбор менен бирдикте калкка, мамлекеттик органдарга жана жеке менчик уюмдарга ыкчам маалымдоо;

б) мамлекеттик органдардан, жарандардан, жеке менчик уюмдардан киберкоопсуздукту камсыздоо жана тобокелдиктерди башкаруу маселелери боюнча кайрылууларды жана суроо-талаптарды кабыл алуу; маалымат берүү жана аталган суроо-талаптар боюнча түшүндүрмөлөрдү чыгаруу;

в) берилген ыйгарым укуктарга ылайык Кыргыз Республикасы кошулган өз ара аракеттенүү форматтарынын жана механизмдеринин алкагында Кыргыз Республикасынын эл аралык өнөктөштөрү менен киберкоопсуздук маселелери боюнча маалымат алмашуу жаатында өз ара аракеттенүү;

г) маалыматтык-коммуникациялык технологиялар жана киберкоопсуздук жаатындагы мамлекеттик-жеке менчик өнөктөштүктүн катышуучулары менен өз ара аракеттенүүнүн жана маалыматтык-ресурстук колдоонун аянтчасы;

д) өз компетенциясынын чегинде башка милдеттерди аткаруу.

### 5.2. Кыргыз Республикасынын кооптуу маалыматтык инфраструктурасынын коопсуздугун камсыздоо

14. Бул Стратегиянын милдеттеринин бири Кыргыз Республикасынын кооптуу маалыматтык инфраструктурасынын коопсуздугун камсыздоонун бирдиктүү системасын түзүү болуп саналат.

15. Бул чөйрөдөгү мамлекеттик саясат төмөнкүдөй жолдор менен ишке ашырылат:

1) кооптуу маалыматтык инфраструктуранын объекттери иштеген секторлорду, тармактарды жана иш чөйрөлөрүн аныктоо, анын ичинде төмөнкү секторлор менен чөйрөлөрдөгү мамлекеттик системалар:

- мамлекеттик башкаруу жана мамлекеттик электрондук кызмат көрсөтүүлөр сектору;

- саламаттык сактоо чөйрөсү;

- транспорт тармагы;

- телекоммуникация жана байланыш тармагы;

- кредиттик-финансылык чөйрө;

- коргонуу сектору;

- отун өнөр жайы;

- генерация жана электр энергиясын бөлүштүрүү тармагы;

- тамак-аш өнөр жайы;

- тоо-кен өнөр жайы;

2) объекттердин кооптуу маалыматтык инфраструктурага таандыгын аныктоого мүмкүндүк берген критерийлер менен параметрлерди иштеп чыгуу жана бекитүү.

Критерийлер потенциалдуу кесепеттерди өзүнө камтыйт, алар объекттин коргонуу жөндөмү, социалдык-экономикалык, социалдык-саясий жана башкаруу чөйрөсүндөгү ишинин бузулушуна алып келиши мүмкүн.

Параметрлер маалыматтык инфраструктуранын айрым объектин кооптуу маалыматтык инфраструктуранын объекти катары анын маанилүүлүгүн аныктоого категориялоо үчүн зарыл. Маанилүүлүк параметрлери объекттин функцияларынын тибине жараша өзгөрүлүп турат, бирок өлчөнүүчү сандык мүнөзгө ээ жана объекттин ишинин көрсөткүчтөрүнүн Кыргыз Республикасынын экономикалык активдүү калкынын ошол белгилүү бир объектинин кызмат көрсөтүүсүн камтыган же көз каранды болгон үлүшүнө байланыусуна негизделет.

Бул милдетти чечүү үчүн 2023-жылдын аягына чейин кооптуу маалыматтык инфраструктуранын коопсуздугу жөнүндө Кыргыз Республикасынын Мыйзамын иштеп чыгуу жана кабыл алуу, ошондой эле аталган Мыйзамдын жоболорун ишке ашырууну камсыздаган мыйзам алдындагы ченемдик актылардын системасын түзүү зарыл.

16. Кооптуу маалыматтык инфраструктуранын операторлору үчүн алардын объекттеринин коопсуздугун камсыздоо боюнча милдеттүү талаптарды белгилөө керек, анын ичинде:

а) ишти камсыздаган кооптуу маалыматтык инфраструктуранын объекттерин резервдөө боюнча талаптарды, анын ичинде ресурстарды резервдөөнүн сандык көрсөткүчтөрүн жана алардын маалыматтык инфраструктураларынын негизги түйүндөрү үчүн "ыкчам резервди";

б) кооптуу маалыматтык инфраструктуранын объекттеринин коопсуздугун камсыздоо саясатын иштеп чыгуу жана макулдашуу боюнча талаптарды, алар өзүнө кооптуу маалыматтык инфраструктуранын белгилүү бир объекттерине коркунуч келтирүүчү моделдерди түзүүнү, компьютердик инциденттерди болтурбоо, башкаруу жана кийинки калыбына келтирүү пландарын иштеп чыгууну камтыйт;

в) компьютердик кол салууларды болтурбоо жана табуу каражаттарын, ошондой эле компьютердик чабуулдарды болтурбоо жана табуу, кооптуу маалыматтык инфраструктуранын объекттеринин коопсуздугун камсыздоочу башка каражаттарды орнотуу жана колдонуу боюнча талаптарды;

г) кооптуу маалыматтык инфраструктура объекттеринин операторлорунун штаттык түзүмүндөгү киберкоопсуздукту камсыздоо боюнча түзүмдүк бөлүмдөрдү уюштурууга талаптарды;

д) кооптуу маалыматтык инфраструктуранын объекттеринин операторлору тарабынан Компьютердик инциденттерге жооп берүү боюнча улуттук борборду кооптуу маалыматтык инфраструктуранын объекттериндеги олуттуу компьютердик инциденттерди кошуп алганда компьютердик инцидент фактылары тууралуу милдеттүү түрдө маалымдоо, ошондой эле Компьютердик инциденттерге жооп берүү боюнча улуттук борбор менен коркунучтар жана начар корголгондугу тууралуу үзгүлтүксүз маалымат алмашууну камсыздоо боюнча талаптарды.

### 5.3. Компьютердик инциденттерди алдын алуунун, жооп берүүнүн жана башкаруунун улуттук системасын түзүү

17. Кыргыз Республикасынын маалыматтык инфраструктуранын объекттеринде компьютердик инциденттердин кесепеттерин кыскартуу жана минималдаштыруу боюнча маселелерди чечүүнүн алкагында Кыргыз Республикасынын компьютердик инциденттерди алдын алуунун, жооп берүүнүн жана башкаруунун улуттук системасы түзүлөт. Бул системанын борбордук звенолору төмөнкүлөр болот:

а) маалыматтык жана киберкоопсуздукту камсыздоо боюнча координациялык борбор;

б) киберкоопсуздукту камсыздоо чөйрөсүндөгү ыйгарым укуктуу мамлекеттик органдын компьютердик инциденттерге жооп берүү борбору (Компьютердик инциденттерге жооп берүү боюнча улуттук борбор);

в) компьютердик инциденттерге жооп берүү боюнча борборлордун инфраструктурасы (менчик, финансылык жана башка);

г) мамлекеттик органдардын жана менчик сектор уюмдарынын, анын ичинде кооптуу маалыматтык инфраструктуранын объекттеринин операторлорунун катышуусунда үзгүлтүксүз киберокууларды өткөрүү боюнча иштерди уюштуруу.

18. Мындай системаны түзүү жана жайылтуу үчүн төмөнкү чараларды көрүү зарыл:

1) ушул Стратегияны ишке ашыруунун алкагында компьютердик инциденттердин алдын алуу, жооп берүү жана башкаруу боюнча иш төмөнкүлөргө мүмкүндүк берет:

- эл аралык тажрыйбаны эске алуу менен (анын ичинде CC-CERT, AP-CERT, US-CERT, IMPACT-ITU, FIRST, FIN-CERT РФ) киберкоопсуздук инциденттерин классификациялоо системасын иштеп чыгуу жана ишке киргизүү. Классификациялоо системасы практикалык критерийлерге таянууга тийиш (инциденттин жүрүшүндө бузулган системаны калыбына келтирүү үчүн убакыт; инциденттин жыйынтыгында системанын ишинин бузулуу даражасы; инциденттин потенциалдуу же болбосо анык кесепеттери - маалыматтын жайылышы, маалыматтын жок болушу, физикалык инфраструктурага келтирилген зыяны ж.б.);

- классификациялоонун негизинде киберкоопсуздук инциденттеринин деңгээлинин шкаласы түзүлөт, ал маалымат системаларын, анын ичинде мамлекеттик органдардын жана кооптуу маалыматтык инфраструктуранын объекттерин коргоого талаптардын системасын иштеп чыгууда зарыл инструмент болуп эсептелет. Шкаланын жогорку деңгээлине таандык инциденттер киберкоопсуздуктун олуттуу инциденттеринин катарына кирет. Олуттуу инциденттерди болтурбоо жана кесепеттерин жоюу чараларын камсыздоо, ошондой эле мындай инциденттердин фактылары тууралуу маалымдоо

инциденттердин башка категорияларына (деңгээлдерине) салыштырмалуу субъекттердин кеңири аймагы үчүн милдеттүү болуп саналат;

- компьютердик инциденттерге жооп берүү борборлорунун CC-CERT, FIRST жана компьютердик инциденттерге жооп берүү жаатындагы мыкты эл аралык тажрыйбага жана иш стандарттарына ылайык келүүсүнө мүмкүндүк берген башка эл аралык форматтардын аккредитациясын алуу (24x7x365 иштөө моделин жана компьютердик инциденттер тууралуу келип түшкөн билдирүүгө жооп берүүнүн минималдуу убактысын кошкондо);

- Компьютердик инциденттерге жооп берүү боюнча улуттук борбор менен бирге маалымат алмашууну уюштуруу жана башка өз ара аракеттенүү боюнча кооптуу маалыматтык инфраструктуранын объекттерине коюлуучу талаптарды иштеп чыгуу жана бекитүү. Алсак талаптарда кооптуу маалыматтык инфраструктуранын объекттеринде болгон компьютердик инциденттер тууралуу милдеттүү маалымдоо системасын түзүү каралууга тийиш.

Бекитилген талаптардын системасы төмөнкүлөргө багытталат:

а) компьютердик инцидент, компьютердик чабуул жана кооптуу маалыматтык инфраструктуранын объекттерине киберкоопсуздук коркунучун жаратуучу башка киберкоопсуздук түшүнүктөрүнүн жана аныктамаларынын системасын түзүүгө;

б) кооптуу маалыматтык инфраструктуранын объекттеринин операторлоруна маалыматтык жана киберкоопсуздукту камсыздоо боюнча координациялык борборго компьютердик инциденттер тууралуу маалымат жана отчёт берүү жаатындагы талаптарды иштеп чыгууга жана бекитүүгө;

в) кооптуу маалыматтык инфраструктуранын объекттеринин операторлору тарабынан толукталуучу, ошондой эле менчик уюмдар жана адамдар тарабынан толуктоого ачык болгон маалыматтык жана киберкоопсуздукту камсыздоо боюнча координациялык борборго караштуу компьютердин начар корголгондугу жана зыяндуу программалык камсыздоо тууралуу маалыматтардын бирдиктүү репозиторийин түзүүгө;

г) маалыматтык жана киберкоопсуздукту камсыздоо боюнча координациялык борбордун аянтчасында Кыргыз Республикасынын аймагында электр байланышы жана маалыматтык инфраструктуранын иштеши бузулуп, өзгөчө кырдаал түзүлгөндө иш-аракеттер планын иштеп чыгууга. Окуу планын жана окуунун жүрүшүндө иштелип чыккан коркунуч келтирүүчү моделдерди жана өзгөчө кырдаалдардын сценарийлерин актуалдаштырууга жана жаңылоого.

### 5.4. Компьютердик кылмыштуулукка каршы аракеттенүү

19. Стратегия өнүгүп жаткан жогорку технологиялык кылмыштуулукка, анын ичинде Кыргыз Республикасынын аймагында, ошондой эле чет өлкөлөрдө айрым адамдарга, уюмдарга жана мамлекетке карата жүргүзүлгөн трансчек аралык компьютердик кылмыштуулукка каршы аракеттенүү зарылдыгынан келип чыгат. Стратегиянын алкагында заманбап компьютердик кылмыштуулукка каршы аракеттенүүдө төмөнкүлөргө басым жасалат.

а) Кыргыз Республикасынын Жазык кодексинде киберкылмыштуулук менен күрөшүүдөгү эл аралык ыкмага ылайык компьютердик кылмыштардын курамынын криминалдашуусун бекитүүнүн зарылдыгы;

б) Кыргыз Республикасынын Жазык-процесстик кодексинде компьютердик криминалистиканын методдору менен каражаттарын бекитүү, Кыргыз Республикасынын Жазык-процесстик кодексине жана тиешелүү ченемдик укуктук актыларга санариптик далилдөө түшүнүгүн киргизүү, анын критерийлерин,

мүнөздөмөсүн жана белгилөө ыкмаларын сыпаттоо жана баяндоо. Башка далилдер сыяктуу эле санариптик далилдөөнүн юридикалык күчүн таануу;

в) компьютердик кылмыштардын курамынын криминалдашуусу жана аларды териштирүү, Кыргыз Республикасынын аймагынан компьютердик кылмыш жасоого шектелген же чет өлкөнүн аймагында андай кылмыш жасоого шектелген адамдарды трансчек аралык берүү боюнча улуттук мыйзамдардын шайкештигин камсыздоо;

г) санариптик далилдерди жыйноого жана Кыргыз Республикасынын укук коргоо органдары үчүн санариптик далилдер боюнча соттук экспертиза жүргүзүүгө жеке компанияларды тартуу мүмкүндүгүн кароо.

### 5.5. Маалыматты коргоонун, анын ичинде маалыматты криптографиялык коргоонун улуттук системасын түзүү

20. Стратегиянын алкагында маалыматты криптографиялык коргоо жаатында Кыргыз Республикасынын комплекстүү жана бирдиктүү мамлекеттик саясатын түзүү максаты көздөлүүдө. Калыптандырылуучу жана жүргүзүлүп жаткан саясат криптографиялык алгоритмдердин жана функциялардын техникалык стандартташтыруу деңгээлиндеги маалыматты коргоо каражаттарын, анын ичинде Кыргыз Республикасынын мамлекеттик органдарынын бизнес-процесстеринде колдонулган маалыматты криптографиялык коргоо каражаттарын тестирлөө жана сертификациялоо системасын түзүү деңгээлиндеги мамилени макулдашуу жана милдеттерди бөлүштүрүү принцибине таянат.

Маалыматты криптографиялык коргоо жаатындагы техникалык стандартташтыруу деңгээлинде эл аралык стандарттарга шайкеш келген Кыргыз Республикасынын стандарттары кабыл алынууга тийиш. Мында Кыргыз Республикасынын кабыл алынуучу стандарттары эл аралык таанылган жана колдонулуучу криптографиялык алгоритмдердин математикалык параметрлерин сыпаттайт.

Маалыматты коргоо каражаттарын жана маалыматты криптографиялык коргоо каражаттарын тестирлөө жана сертификациялоо деңгээлинде маалыматты, анын ичинде Кыргыз Республикасынын мамлекеттик органдарынын административдик жол-жоболорунда колдонулуучу маалыматты коргоо каражаттарына коюлуучу талаптарды иштеп чыгууну камсыздоо зарыл. Кыргыз Республикасынын кооптуу маалыматтык инфраструктуранын объекттеринде маалыматты криптографиялык коргоо каражаттарын тестирлөө жана сертификациялоо системасы киргизилүүгө тийиш. Бул багытта биринчи кезекте маалыматты коргоо каражаттарын, анын ичинде маалыматты криптографиялык коргоо каражаттарын тестирлөөчү сыноо борборлорунун системасын (лаборатория) түзүү зарыл. Кыргыз Республикасында мындай системаны түзүүнүн принциби болуп мамлекеттик-жеке өнөктөштүк, анын ичинде интеллектуалдык жана материалдык каражаттарды, ошондой эле жеке сектордун компетенция борборлорун Кыргыз Республикасынын аймагында колдонулуучу маалыматты криптографиялык коргоо каражаттары үчүн тестирлөөчү сыноо борборлорунун системасын (лаборатория) түзүү жана өнүктүрүү процессине кошуу эсептелет.

21. Кыргыз Республикасынын маалыматты криптографиялык коргоо жаатындагы мамлекеттик саясатынын маанилүү элементи болуп маалыматтарды коргоо каражаттарын, анын ичинде Кыргыз Республикасынын аймагындагы сыноо борборлорунда (лабораторияларда) мындай каражаттарды тестирлөөнүн жыйынтыгында алардын инженердик-техникалык корголушу боюнча маалыматты криптографиялык коргоо каражаттарын сертификациялоону жүргүзгөн уюмдардын системасын түзүү эсептелет.

22. Стратегиянын алкагында маалыматты коргоо каражаттарын сертификациялоо боюнча мамлекеттик уюмдардын минималдуу керектүү санын түзүү болжолдонот.

### 5.6. Кыргыз Республикасынын мамлекеттик секторунда киберкоопсуздукту камсыздоо боюнча бирдиктүү ыкманы түзүү

23. Маалымат мейкиндиги менен кибермейкиндиктин катышын аныктоо жагында Стратегия "Маалыматтык технология. Коопсуздукту камсыздоо методдору. Киберкоопсуздук боюнча колдонмо көрсөтмөлөр" ИСО/МЭК 27032:2012 (ISO/IEC 27032:2012) эл аралык стандартында баяндалган өңүткө таянат.

Киберкоопсуздукту аныктоо жагында Стратегия "МСЭ электр байланышын стандартташтыруу сектору (04/2008). X серия: Маалымат берүү тармактары, ачык системалардын жана коопсуздуктун өз ара байланышы" X.1205 рекомендацияларында баяндалган № 17 (SG-17) МСЭ-Т изилдөө тобунун иштерине таянат.

24. Кыргыз Республикасынын жеке киберкоопсуздук системасын жана саясатын калыптандыруу боюнча практикалык милдеттерден улам, ошондой эле мыкты чет өлкөлүк практиканы жана эл аралык тажрыйбаны (анын ичинде сунушталган ISO стандарттарын жана Эл аралык электр байланыш уюмунун рекомендациясын) эске алып, ушул Стратегия маалыматтык инфраструктуранын объекттеринде маалыматтын бүтүндүгүн, жеткиликтүүлүгүн жана купуялыгын сактоо сыяктуу киберкоопсуздук маселелеринен тартып коомдук жана жеке аң-сезимге контенттин таасири, маалымат таймашы жана маалыматтык-психологиялык операциялар жагында маалыматтык коопсуздук маселелерин бөлүү принцибинен келип чыгат. Бул принципке ылайык:

а) ушул Стратегия Кыргыз Республикасынын мыйзамдарына ылайык киберкоопсуздук маселелерин гана камтыйт;

б) Стратегияда коомдук жана жеке ан-сезимге контенттин таасири, маалымат таймашы жана маалыматтык-психологиялык операциялар, ошондой эле мамлекеттик маалымат саясатын жана жалпыга маалымдоо каражаттарына карата саясатты түзүү жана ишке ашыруу жагында маалыматтык коопсуздукту камсыздоого байланышкан иштин терминдери, чакырыктары, тобокелдиктери, милдеттери жана багыттары каралбайт;

в) киберкоопсуздукту камсыздоо жаатындагы саясат ушул Стратегияга ылайык Кыргыз Республикасынын мамлекеттик саясатынын өз алдынча жана көз карандысыз багытын камтыйт, ал мамлекеттик маалымат саясатынын жана маалыматтык коопсуздукту камсыздоо жаатындагы саясаттын өнүгүүсүн эске алуу менен ишке ашырылат;

г) ушул Стратегия, ошондой эле анда түптөлгөн принциптер маалыматтык коопсуздукту камсыздоо боюнча мамлекеттик саясатты чектебейт.

25. Киберкоопсуздукту камсыздоо чөйрөсүндөгү мамлекеттик саясаттын чараларын практикалык ишке ашыруунун деңгээлин жана сапатын жогорулатуу боюнча милдеттерди чечүү үчүн жеке маалыматтарды иштеп чыгуу жаатындагы көзөмөлдөө саясаты күчөтүлөт, ошондой эле жеке маалыматтар боюнча ыйгарым укуктуу мамлекеттик органды түзүү аркылуу жеке маалыматтарды иштеп чыгуу чөйрөсүндө бирдиктүү талаптар белгиленет.

26. Стратегиянын алкагында жеке маалыматтарды коргоо чөйрөсүндөгү мыйзамдардын талаптарын сактабаган учурда жеке мүнөздөгү маалыматтарды иштеп чыгуу субъекттерин жоопкерчиликке тартуу укуктары менен 2019-жылдан кечиктирбей ыйгарым укуктуу мамлекеттик органды түзүү каралууда.

27. Кыргыз Республикасынын мамлекеттик секторунун маалыматтык системаларынын коопсуздугун камсыздоо үчүн киберкоопсуздук аудитин үзгүлтүксүз жүргүзүү каралууда; мындай аудитти жүргүзүүгө Кыргыз Республикасында катталган менчик компаниялар, улуттук коопсуздук маселесин тескеген ыйгарым укуктуу мамлекеттик орган менен милдеттүү түрдө макулдашуудан кийин тартылышы мүмкүн. Категориялаштыруунун жыйынтыгы боюнча кооптуу маалыматтык инфраструктуранын объекттеринин тизмесине кирген мамлекеттик маалыматтык инфраструктураларга да мамлекеттик сатып алуу жол-жобосунун алкагында сатып алынган программалык-аппараттык продукциянын (пентест) начар корголгондугуна милдеттүү тестирлөө жол-жобосу белгиленет.

### 5.7. Эл аралык кызматташтык жана техникалык стандартташтыруу

28. Кыргыз Республикасы 2019-2023-жылдарда киберкоопсуздук жана маалыматтык коопсуздук жаатындагы техникалык стандартташтыруу боюнча негизги жумуш аянтчаларында өзүнүн катышуусун бекемдейт.

29. ISO/МЭК, IEEE тармактык стандарттарды, ЕАЭБ өлкөлөрүнүн стандарттарын, ошондой эле Интернет долбоорлоо боюнча жумушчу топтун (IETF) документтерин кошуп алганда киберкоопсуздук жана маалыматтык коопсуздук жаатындагы эл аралык стандарттарга шайкеш келтирүү зарыл. Маалыматтык технологиялардын киберкоопсуздугу жаатындагы ата мекендик стандарттарды эл аралык стандарттарга шайкеш келтирүү деңгээлин жогорулатууга жетишүү зарыл.

Ошондой эле Стандартташтыруу боюнча мамлекеттер аралык комитеттин алкагында кабыл алынган маалыматты криптографиялык коргоонун мамлекеттер аралык стандарттарын жаңылоо жол-жобосун киргизүү максатка ылайыктуу.

### 5.8. Киберкоопсуздукту камсыздоо үчүн потенциалды өстүрүү жана адам ресурстарын чыңдоо

30. Адам потенциалын өстүрүү жаатындагы негизги милдет болуп киберкоопсуздук, компьютердик гигиена жана санариптик сабаттуулук сабактарын системалуу түрдө окутууну Кыргыз Республикасынын мектеп, орто жана жогорку кесиптик билим берүү системасына киргизүү эсептелет. Бул үчүн билим берүүнүн жана билим берүү регламентинин стандарттарын кайра карап чыгуу процесси төмөнкү максатта ишке ашырылат:

а) "киберкоопсуздук" сабагын Кыргыз Республикасынын жогорку билим берүү мекемелеринин техникалык адистиктери үчүн тармактык сабактардын тизмесине киргизүү;

б) "киберкоопсуздук" сабагын Кыргыз Республикасынын орто кесиптик билим берүү мекемелеринин техникалык адистиктери үчүн тармактык сабактардын тизмесине киргизүү;

в) "компьютердик гигиена" жана "санариптик сабаттуулуктун негиздери" сабактарын Кыргыз Республикасынын мектептеги базалык билим берүүнүн окуу программаларына милдеттүү сабак катары киргизүү.

31. Мындан сырткары Стратегияны ишке ашыруу планынын алкагында ата мекендик адистердин техникалык компетенцияларын чыңдоо жана аларды эл аралык техникалык жамааттын ишине тартуу боюнча иш-чаралар каралган.

32. Компьютердик кылмыштуулук менен күрөшүү үчүн потенциалды өстүрүүнүн алкагында өнүктүрүү боюнча региондук жана эл аралык өнөктөштөр менен өз ара аракеттенип атайын, кызматтардын, укук коргоо органдарынын, прокуратура органдарынын, ошондой эле соттордун компьютердик кылмыштуулук фактылары боюнча жазык процесстерин териштирүү жана жүргүзүү көндүмдөрүн

жогорулатуу жаатында кызматкерлерди даярдоо жана квалификациясын жогорулатуу программасын түзүү жана киргизүү болжолдонот.

## VI. Стратегияны ишке ашыруудагы күтүлүүчү жыйынтыктар, жагымдуу өбөлгөлөр жана тобокелдиктер

33. Ушул Стратегиянын жоболорун кабыл алуу жана өз убагында ишке ашыруу төмөнкүлөргө шарт түзөт:

- тармактык программаларды жана ыйгарым укуктуу мамлекеттик органдын, Кыргыз Республикасынын компетенттүү мамлекеттик органдарынын, ишке тартылган коомдук уюмдардын, бизнес-демилгелердин жана жарандардын иш пландарын иштеп чыгуу үчүн институттук жана базалык шарттарды түзүүгө;

- маалыматтык-ресурстук колдоо жана маалыматтык-коммуникациялык технологиялар менен киберкоопсуздукту өнүктүрүү жаатында бардык кызыкдар тараптардын өз ара аракеттенүүсү үчүн аянтча түзүүгө;

- киберкоопсуздукту камсыздоо жаатындагы мыйзамга ылайык жүрүм-турум ченемдерин жана эрежелерин аныктоочу, ошондой эле бул жааттагы мамлекеттик органдардын ишин жөнгө салуучу бирдиктүү түшүнүк аппаратын жана атайын укуктук база түзүүгө;

- киберкоопсуздукту камсыздоо органдарынын системасын түзүүгө, анын ичинде Кыргыз Республикасынын киберкоргонуусунун абалына жооптуу ыйгарым укуктуу мамлекеттик органды аныктоого;

- киберкоопсуздукка аудит жүргүзүүнүн жана контролдоонун бирдиктүү эрежелерин киргизүүгө;

- Кыргыз Республикасынын мыйзамдарына киберкоопсуздук чөйрөсүндөгү кылмыштар үчүн, анын ичинде трансчек аралык компьютердик кылмыштар боюнча жоопкерчилик киргизүү, компьютердик технологияны колдонуу менен мыйзамсыз иштерге далилдерди табуу, топтоо, белгилөө жана берүү методикаларын киргизүүгө жана жакшыртууга;

- кооптуу маалыматтык инфраструктуранын объекттеринин коопсуздугун камсыздоонун бирдиктүү стандарттарын түзүү менен аларды аныктоого, ошондой эле координациялоо жана контролдоо системасын, өзгөчө кырдаал учуруна иш-аракеттер планын түзүүгө;

- маалыматты коргоо каражаттарын жана маалыматты криптографиялык коргоо каражаттарын тестирлөө жана сертификациялоо системасын киргизүүгө;

- Кыргыз Республикасынын мектеп, орто жана жогорку кесиптик билим берүү системасына атайын сабактарды (киберкоопсуздук, компьютердик гигиена жана санариптик сабаттуулук) киргизүүнүн эсебинен адам потенциалын жогорулатууга;

- тоскоолдуктарды жоюу, эл аралык илимий-техникалык жана укуктук кызматташууну өнүктүрүү, киберкоопсуздукту камсыздоо менен байланышкан мамилелерди эл аралык жөнгө салуу механизмдерине Кыргыз Республикасынын толук кандуу катышуусун камсыздоо максатында киберкоопсуздук жаатындагы мыйзамдарды шайкеш келтирүүгө, терминдерди жана түшүнүктөрдү, ошондой эле эл аралык стандарттарды бирдейлештирүүгө;

- өнүктүрүү боюнча региондук, эл аралык өнөктөштөр менен өз ара аракеттенип, атайын кызматтардын, укук коргоо органдарынын, прокуратура органдарынын, ошондой эле судьялардын компьютердик кылмыштар фактылары боюнча жазык процесстерин териштирүү жана жүргүзүү көндүмдөрүн жогорулатуу жаатында кесиптик даярдыгын жана квалификациясын жогорулатуу программаларын түзүүгө жана ишке киргизүүгө.

Жалпысынан аталган жетишкендиктер Кыргыз Республикасынын киберкоопсуздугун ата мекендик камсыздоо системасынын алкагын белгилейт жана киберкоопсуздук системасынын архитектурасын мындан ары өнүктүрүүгө мүмкүндүк берет.

34. Стратегияны ийгиликтүү ишке ашыруу үчүн жагымдуу өбөлгөлөр төмөнкүлөр:

а) маалыматтык-коммуникациялык технологияларды ишке киргизүү, пайдалануу жана өнүктүрүү, алардын коопсуздугун камсыздоо маселелеринде мамлекеттик бийликтин саясий, мыйзам чыгаруу жана административдик органдарынын колдоосу;

б) технологиялык жактан алдыга жылган жана коопсуз Кыргызстанды түптөө боюнча чет өлкөлүк институттардын жана эл аралык уюмдардын өкүлдөрүнөн турган эл аралык өнөктөштөрдүн көмөк көрсөтүүгө кызыкдарлыгы;

в) санариптик транформациялоо боюнча ири долбоорлорду ишке ашырууда Кыргыз Республикасынын киберкоопсуздугун жана техникалык бейтараптуулугун камсыздоо менен байланышкан демилгелерди колдоого жана улантууга жарандык коомдун даярдыгы;

г) маалыматтык технологиялар жаатындагы адистердин көбөйүшү.

35. Стратегияны ишке ашыруу процессиндеги оң өбөлгөлөр менен катар мамлекеттик органдар төмөнкүдөй тобокелдиктерге дуушар болушу мүмкүн:

- Стратегияны ишке ашыруу боюнча белгиленген багыттардан четтөө;

- жүргүзүлүп жаткан өзгөрүүлөрдүн маанилүүлүгүн түшүнбөө, ага ылайык айрым демилгелер менен чечимдерди кабыл алууну кечеңдетүү, балким аларга атайын бөгөт коюу;

- маалыматтык-коммуникациялык технологиялар жаатындагы мамлекеттик жарандык кызматкерлердин, мамлекеттик органдардын жетекчилеринин киберкоргонуу жана киберкоопсуздук маселелериндеги сабатынын жетишсиздиги;

- маалыматтык-коммуникациялык технологиялар жаатында сапаттуу билими, тажрыйбасы бар кесипкөй кадрлардын жетишсиздиги;

- кабыл алынуучу чечимдерге деструктивдүү маанайдагы адамдардын жана уюмдардын бүлдүргүч жооп берүүгө багытталган иши;

- Стратегияны ишке ашырууга байланышкан долбоорлорду чектеп же өз убагында эмес каржылоо;

- телекоммуникациялык тармактардын трансулуттук жана трансчектүү мүнөзү жана алардын эл аралык байланышкандыгы.

## VII. Стратегияны ишке ашырууга мониторинг

36. Стратегияны ишке ашыруу процессине жыл сайын, кийинки отчёттук жылдын 20-декабрынан кечиктирбей мониторинг жана баалоо жүргүзүлөт, жыйынтыгы Кыргыз Республикасынын Өкмөтүнүн Аппаратынын деңгээлинде талкууланат жана анын натыйжасында Кыргыз Республикасынын Премьер-министрине отчёт берилет. Бул Стратегиянын максаттарынан жана милдеттеринен четтеп кетүүгө алдын ала бөгөт коёт жана Иш-чаралар планына зарыл болгон оңдоолорду киргизүүгө мүмкүндүк берет.

37. Азыркы учурда Бириккен Улуттар Уюмунун эл аралык электр байланыш уюму жарыялаган глобалдык киберкоопсуздук индексине ылайык Кыргыз Республикасы дүйнөдө 111-орунду ээлейт. Стратегиянын Иш-чаралар планынын бардык пункттарынын аткарылышы менен 28 позицияга жогорулоо болжолдонууда.

Эстониянын Электрондук башкаруу академиясы жарыялаган улуттук киберкоопсуздук индексине ылайык Кыргызстан дүйнөдө 104-орунду ээлейт. 2023-жылда 18 позицияга жогорулоо пландалууда.

Маалыматтык-коммуникациялык технологияларды өнүктүрүү индексинин рейтингинде Кыргыз Республикасы 109-орунду ээлейт (Бириккен Улуттар Уюмунун эл аралык электр байланыш уюму жарыялаган индекс). Бул рейтингде Стратегияда пландалган бардык иш-чараларды ишке ашырууда 17 позицияга жогорулоо пландалууда.

## VIII. Стратегияны ишке ашыруунун финансылык жана башка ресурстары

38. 2019-2023-жылдарга Стратегияны ишке ашырууга ушул Стратегияны жана "Санарип Кыргызстан 2019-2023" санариптик транформациялоо концепциясын ишке ашыруу боюнча "жол картасын" жүзөгө ашырууга тартылган мамлекеттик органдарга бөлүнгөн, тиешелүү жылга каралган республикалык бюджеттин каражаттары, ошондой эле эл аралык өнөктөш уюмдар тарабынан бөлүнүүчү финансылык каражаттарды кошуп алганда, Кыргыз Республикасынын мыйзамдарына каршы келбеген башка булактардын каражаттары багытталат.