«ХАЛЫК БАНК КЫРГЫЗСТАН» ААК МААЛЫМАТТЫК КООПСУЗДУК САЯСАТЫ

МАЗМУНУ

«Халык Банк Кыргызстан» ААК маалыматтык коопсуздукту камсыздоо маселелерине өзгөчө көңүл бурат, маалыматтык коопсуздукту башкаруу системасын, маалыматтык коопсуздук коркунучтарынан коргоо үчүн колдонулуучу каражаттарды жана ыкмаларды дайыма өркүндөтүп турат, ошондой эле маалыматты коргоо жаатында компетенттүүлүктү колдоо үчүн Банктын кызматкерлерин жогорку деңгээлде үзгүлтүксүз окутууну камсыздайт.

Бул документ эл аралык «Маалыматтык технологиялар – Коопсуздукту камсыздоо ыкмалары - Маалыматтык коопсуздукту башкаруу системалары - Талаптар» ISO 27001:2013 стандартынын талаптарына ылайык иштелип чыккан жана Банктын корпоративдик веб-сайтында жалпыга ачык жарыялоо үчүн арналган.

Документ маалыматтык коопсуздукту камсыз кылуу көйгөйүнө болгон көз караштар системасын, маалыматты коргоо боюнча негизги принциптерин, багыттарын жана талаптарын баяндайт жана Банк Башкармалыгы тарабынан бекитилген Маалыматтык коопсуздук саясатынын (мындан ары - Саясат) негизги бөлүмдөрүн камтыйт.

Саясаттын ченемдик укуктук негизин Кыргыз Республикасынын мыйзамдарынын жоболору жана маалыматтык системаларды жана маалыматтык коопсуздукту, ошондой эле маалыматтык коопсуздукту башкаруунун эл аралык стандарттарын колдонуу маселелери боюнча Кыргыз Республикасынын Улуттук банкынын талаптары түзөт.

Саясаттын жоболору Банктын бардык кызматкерлери, стажёрлор, практиканттардын аткаруусу үчүн милдеттүү болуп саналат, ошондой эле Банктын маалымат системаларына жана ал Банк жана алардын ишмердиги менен түздөн-түз байланышкан тиешелүү бөлүгүндөгү документтерине кирүү мүмкүнчүлүгү бар кардарларга жана башка үчүнчү жактарга маалымат үчүн жеткирилиши керек.

Саясат бардык маалыматтык системаларды жана документтерди камтыйт, алардын ээси жана колдонуучусу Банк болуп саналат. Маалыматтык коопсуздукту камсыздоо – Банктын коммерциялык ишмердигин ийгиликтүү ишке ашыруу үчүн зарыл шарт болуп саналат. Маалымат банктын эң маанилүү активдеринин бири болуп саналат.

Саясаттын бардык жоболорунун ага кирүүгө багытталган негизги максаты, аларды болтурбоо же алардын кесепеттерин минималдаштыруу аркылуу маалыматтын коопсуздугуна коркунуч жарата турган окуялардан болуучу зыянды минималдаштыруу болуп саналат.

Маалыматтык коопсуздук өздүк максат болуп саналбайт, аны камсыздоо Банктын болгон маалыматтык ресурстарына карата мүмкүн боло турган ар кандай коркунучтар менен байланышкан тобокелдиктерди жана экономикалык жоготууларды төмөндөтүү үчүн керек.

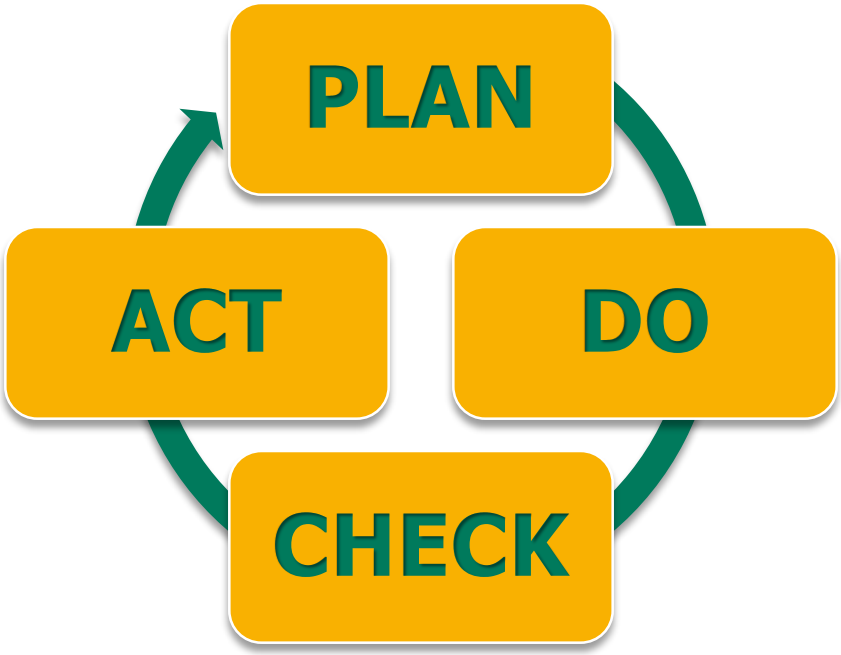
Ушул максатта маалыматтын негизги касиеттерин сактоо зарыл, атап айтканда:

- жеткиликтүүлүк – ага карата тиешелүү ыйгарым укуктары бар субъекттердин маалыматка өз убагында тоскоолдуксуз жетүү жөндөмдүүлүгү менен мүнөздөлүүчү касиет;
- купуялуулук – бул маалыматка жетүүгө ээ болгон субъекттердин чөйрөсүнө чектөөлөрдү киргизүү зарылдыгын көрсөтүүчү жана көрсөтүлгөн маалыматты ага жетүүгө ыйгарым укугу жок субъекттерден жашыруун сактоо жөндөмдүүлүгү менен камсыздала турган касиет;
- бүтүндүк – маалыматтын бузулбаган (анын кандайдыр бир туруктуу абалына карата болгон өзгөрүүсүз) түрдө болушунан турган касиети.

Ишенимдүү маалыматты коргоону түзүү процесси эч качан бүтпөйт. Маалыматтык коопсуздуктун жетишээрлик ишенимдүү системасын камсыз кылуу максатында анын параметрлерин туруктуу түрдө жөнгө салуу, тышкы жана ички чөйрөдөн келип чыккан жаңы коркунучтарды чагылдыруу үчүн көнүктүрүү зарыл.

Мындай зарылчылыктын жаралышына жараша стандарттарга, жол-жоболорго же Саясатка өзгөртүүлөрдү киргизүү учурунда эч кандай тоскоолдук болбошу керек.

Ушул жобого ылайык, маалыматтык коопсуздукту башкаруу циклинин төмөнкү этаптары аныкталган (PDCA модели: Plan-Do-Check-Act).



PLAN – Пландоо (иштеп чыгуу) - тобокелдиктерди талдоо, Банктын жалпы стратегиясына жана милдеттерине ылайык натыйжаларды алуу үчүн тобокелдиктерди тескөөгө жана маалыматтык коопсуздукту өркүндөтүүгө кирген Саясатты, максаттарды, милдеттерди, процесстерди, жол-жоболорду, программалык-аппараттык каражаттарды аныктоо;
DO – Ишке ашыруу (ишке киргизүү жана иштетүү) – Саясатты, контролдоо механизмдерин, процесстерди, жол-жоболорду, программалык-техникалык каражаттарды ишке ашыруу жана иштетүү;
CHECK – Текшерүү (мониторинг жана талдоо) – баалоо жана ал анда колдонулса, саясатка, максаттарга жана практикалык тажрыйбага ылайык процесстерди аткаруу мүнөздөмөлөрүн өлчөө, маалыматтык ресурстардын коопсуздугуна таасир этүүчү тышкы жана ички факторлордун өзгөрүүлөрүн талдоо, талдоо үчүн жетекчиликке отчет берүү;
ACT – Корректировкалоо (коштоо жана өркүндөтүү) – маалыматтык коопсуздук системасын үзгүлтүксүз өркүндөтүүнү камсыз кылуу максатында, маалыматтык коопсуздуктун абалына, жетекчиликтин талаптарына, башка факторлорду ички жана тышкы текшерүүлөрдүн натыйжаларына негизделген түзөтүүчү жана алдын алуучу чараларды көрүү.

Банктын маалыматтык коопсуздук системасын куруу жана анын иштеши төмөнкү негизги принциптерге ылайык жүргүзүлүшү керек:

- мыйзамдуулук – маалыматтык коопсуздукту камсыз кылуу үчүн кабыл алынган бардык иш-аракеттери колдонуудагы мыйзамдардын негизинде, Банктын маалыматтык коргоо объекттерине тийгизиле турган терс таасирлерди аныктоо, эскертүү, локалдаштыруу жана бөгөттөөнүн мыйзам тарабынан жол берилген бардык ыкмаларын колдонуу менен жүргүзүлөт;
- бизнеске карата багыттуулук – маалыматтык коопсуздук негизги ишмердикти колдоо процесси катары каралат. Маалыматтык коопсуздукту камсыз кылуу боюнча бардык чаралар Банктын ишине олуттуу тоскоолдуктарды жаратпашы керек;
- үзгүлтүксүздүк – маалыматтык коопсуздук системаларын тескөө каражаттарын колдонуу, Банктын маалыматтык коопсуздугун камсыз кылуу боюнча бардык иш-чараларды ишке ашырууда Банктын учурдагы бизнес-процесстерин үзгүлтүксүз же токтотуусуз жүргүзүлүшү керек;
- комплекстүүлүк – маалыматтык ресурстардын бүткүл жашоо циклинин ичинде, аларды пайдалануунун бардык технологиялык этаптарында жана бардык иштөө режимдеринде алардын коопсуздугун камсыз кылуу;
- негиздүүлүк жана экономикалык максаттуулук – коргоонун колдонулуу мүмкүнчүлүктөрү жана каражаттары илимдин жана техниканын өнүгүүсүнүн тиешелүү деңгээлинде ишке ашырылууга, коопсуздуктун берилген деңгээлинин көз карашынан негизделүүгө жана коюлган талаптарга жана стандарттарга дал келүүгө тийиш. Бардык учурларда маалыматтык коопсуздук чараларынын жана системаларынын наркы тобокелдиктин бардык түрлөрүнөн мүмкүн боло турган зыяндын көлөмүнөн аз болушу керек;
- артыкчылык – маалыматтык коопсуздукка реалдуу, ошондой эле потенциалдуу коркунучтарды баалоо учурунда маанилүүлүк даражасы боюнча Банктын бардык маалыматтык ресурстарын категорияларга бөлүү (ранжирлөө);

- керектүү билим жана эң аз артыкчылык деңгээли – колдонуучу артыкчылыктын минималдуу деңгээлин жана анын ыйгарым укуктарынын чегинде ишин аткаруу үчүн ал зарыл болгон маалыматтарга гана жетүү алат;
- адистештирүү – техникалык каражаттарды иштетүү жана маалыматтык коопсуздук чараларын ишке ашыруу Банктын кесиптик даярдалган адистери тарабынан жүргүзүлүшү керек;
- маалымдуулук жана жеке жоопкерчилик – бардык деңгээлдеги жетекчилер жана аткаруучулар маалыматтык коопсуздуктун бардык талаптары тууралуу билиши керек жана бул талаптарды аткаруу жана маалыматтык коопсуздуктун белгиленген чараларын сактоо үчүн жеке жоопкерчиликте болушу керек;
- өз ара аракеттенүү жана координациялоо – маалыматтык коопсуздук чаралары Банктын тиешелүү түзүмдүк бөлүмдөрүнүн өз ара мамилелеринин, коюлган максаттарга жетүү үчүн алардын күч-аракеттерин координациялоонун, ошондой эле тышкы уюмдар, кесиптик бирикмелер (ассоциациялар) жана коомдоштор, мамлекеттик органдар, юридикалык жана жеке жактар менен зарыл болгон байланыштарды түзүүнүн негизинде жүргүзүлөт;
- тастыктоочулук – маанилүү документтер жана бардык жазуулар – маалыматтык коопсуздук боюнча талаптардын аткарылышын жана аны уюштуруу системасынын натыйжалуулугун тастыктоочу документтер, ыкчам жетүү жана калыбына келтирүү мүмкүнчүлүгү менен түзүлүшү жана сакталышы керек.

Банкта маалыматтык коопсуздукту камсыз кылуунун негизги объекттери болуп төмөнкү элементтер таанылат:

- банктык сырга, Банктын коммерциялык сырына, Банктын чендүү иштешин камсыз кылуу үчүн зарыл болгон ар кандай башка маалыматтарга (мындан ары - корголуучу маалымат) карата колдонуудагы мыйзамдарга жана Банктын ички ченемдик документтерине ылайык аларга киргизилген маалыматтарды камтыган маалыматтык ресурстар;

- корголуучу маалыматты кайра иштеп чыгуу, берүү жана сактоо жүргүзүлө турган маалыматташтыруу каражаттары жана системалары (эсептөөчү техника, маалыматтык-эсептөө комплекстери, тармактар, системалар);
- Банктын автоматташтырылган системасынын программалык каражаттары (операциялык системалар, маалыматтар базаларын башкаруу системалары, башка жалпы системалык жана колдонмо программалык камсыздоо), алардын жардамы менен корголуучу маалымат кайра иштетилет;
- маалыматтык ресурстарды башкаруу жана пайдалануу менен байланышкан Банк процесстери;
- корголуучу маалыматты кайра иштетүү каражаттары жайгашкан жайлар;
- Банктын кызматкерлеринин иш бөлмөлөрү жана кеңселери, жабык сүйлөшүүлөрдү жана кеңешмелерди өткөрүү үчүн арналган Банк жайлары;
- корголуучу маалыматка жетүүгө уруксаты бар, Банк персоналы;
- ачык маалыматты кайра иштетип чыгуучу, бирок корголуучу маалымат кайра иштетилип жаткан жайларда жайгаштырылган техникалык каражаттар жана системалар.

Корголууга жаткан маалымат болушу мүмкүн:

- кагазга жазылган маалымат;
- электрондук түрдө болгон маалымат (эсептөөчү техника каражаттарынын жардамы менен иштетилиши, берилиши жана сакталышы, техникалык каражаттардын жардамы менен жазылышы жана кайра чыгарылышы мүмкүн болгон);
- телефон, телефакс, телекс боюнча ж.у.с. электрдик сигналдар түрүндө берилиши мүмкүн болгон маалымат;
- кеңешмелерди жана сүйлөшүүлөрдү жүргүзүү учурунда аба чөйрөсүндө жана курчап турган конструкцияларда акустикалык жана термелүү сигналдар түрүндө болгон маалымат.

Маалыматтык коопсуздуктун коркунучтары болуп маалыматтын башкы касиеттеринин бузулуусунун потенциалдуу мүмкүнчүлүгү түшүнүлөт.

Маалыматтык коопсуздуктун коркунучтары төмөнкүлөргө бөлүнөт:

- кокустуктан – табигый кырсыктар, көңүл бурбоо менен кетирилген каталар, аппараттык жана программалык каражаттардын ж.б. каталары;
- атайылап жасалган, б.а. маалыматтарды бурмалоо же жок кылуу, маалыматтарды кыянаттык менен колдонуу, компьютердик кылмыштар ж.б.

Маалыматтык коопсуздук коркунучтарынын санына төмөнкүлөр кирет (бирок алар менен чектелбейт):

- банктык сырды, Банктын коммерциялык сырын жана башка корголуучу маалыматты түзгөн маалыматтын жоголушу;
- корголуучу маалыматты бурмалоо (уруксатсыз өзгөртүү, жасалмалоо);
- маалыматтын сыртка чыгып кетүүсү (утечка) – башка бөтөн адамдар корголуучу маалымат менен уруксатсыз таанышуусу (уруксатсыз кирүү, көчүрүү, уурдоо ж.б.);
- маалыматтык ресурстарды уруксатсыз пайдалануу (кыянаттык, алдамчылык ж.у.с.);
- маалыматтын бөгөттөлүшүнүн, жабдуулардын же программалардын иштебей калышынын, жумушчу станциялардын, серверлердин, активдүү тармактык жабдуулардын, маалымат базасын башкаруу системаларынын, бөлүштүрүлгөн эсептөө тармактарынын операциялык системаларынын иштешинин бузулушу, вирустардын, табигый кырсыктардын, форс-мажордук жагдайлар жана башка кыянат аракеттердин таасирлеринин натыйжасында маалыматка жетүүгө мүмкүн эместик.

Аталган коркунучтардын таасиринин натыйжасында Банктын маалыматтык коопсуздугунун абалына жана анын чендүү иштешине таасир этүүчү төмөнкүдөй терс кесепеттер жаралышы мүмкүн:

- корголуучу маалыматтын сыртка чыгып кетиши (утечка) же жайылтылышы менен байланышкан финансылык жоготуулар;
- жоголгон маалыматты жок кылуу жана кийин калыбына келтирүү менен байланышкан финансылык жоготуулар;
- Банктын ишин үзгүлтүккө учуратуудан келтирилген зыян жана ал өзүнүн милдеттенмелерин аткарууга мүмкүн эместик менен байланышкан жоготуулар;
- бир жактуу маалыматтын негизинде башкаруучулук чечимдерди кабыл алуудан келтирилген зыян;
- Банктын жетекчилигинде объективдүү маалыматтын жоктугунан келтирилген зыян;
- Банктын кадыр-баркына келтирилген зыян;
- зыяндын башка түрү.

Маалыматтык коопсуздукту бузгандар төмөнкүдөй түрдө классификацияланат:

- ички бузуучулар – маалыматтык коопсуздук режимин билбестен же кыянаттык менен бузган Банктын кызматкерлери;
- тышкы бузуучулар – Банк менен эмгек мамилелери боюнча байланышы жок (анын ичинде стажерлор жана практиканттар), бейбаш же кыянаттык менен Банктын маалыматтык ресурстарына зыян келтирүүгө жөндөмдүү аракеттерди жасаган адамдар.

Бузуучунун коркунучтуулугу көбүнчө ага жеткиликтүү болгон маалыматтык ресурстардын саны жана маанилүүлүгү менен аныкталат. Ушуга жараша, эң кооптуу категориялар болуп, жогорку жана орто звенодогу менеджерлер, маалымат ресурстарынын администраторлору жана кардарлардын жана финансылык маалыматтардын чоң көлөмү менен иштеген адамдар эсептелиши мүмкүн.

Ички бузуучулардын негизги типтери:

- «окутулбаган (сабатсыз)/шалаакы кызматкер» – билбестиктен же кыянаттык жасоого ою жок, бирок өзүнүн шалаакылыгынан бузулуштарга жол берген Банктын кызматкери;
- «атаандаш кызматкер» – жеке кастыктан же башка себептер боюнча башка кызматкерге зыян келтирүүгө аракет жасаган Банктын кызматкери. Анын иш-аракеттеринин натыйжасында анын «максаты» гана эмес, бүтүндөй Банк жабыркашы мүмкүн;
- «кызыкдар бузуучу» – үчүнчү тараптын Банкка карата мыйзамсыз аракеттерин жасоого же өзүнүн пайдасы үчүн кызыкдар болгон Банктын кызматкери. Эреже боюнча, ал Банк менен эмгек мамилелерин андан ары да улантууга кызыкдар жана аны түздөн-түз компроматтай турган аракеттерди жасабайт. Эң ыктымалдуу бузуу - маалыматтын сыртка чыгып кетиши (өз пайдасы үчүн кызыкдар - финансылык алдамчылык болгон учурда);

- «тажрыйбалуу кылмышкер» – үчүнчү жактардын кызыкчылыгында укукка каршы аракеттерди жасоо максатында жумушка кирген Банктын кызматкери. Банк менен андан аркы эмгек мамилелерине иш жүзүндө кызыкдар эмес;
- «иштен бошонуучу кызматкер» – аны менен эмгек мамилелерин токтоткон, өз ара дооматы жок Банктын кызматкери. Ал ага түздөн түз жетүүгө мүмкүнчүлүгү бар маалыматтын сыртка чыгып кетүү ыктымалдуулугу бар;
- «таарынган кызматкер» – өзүнүн эмгек ишмердигинин параметрлерине кескин нааразы болгон же болбосо, Банктын жетекчилиги ал кызматкердин ишине ачык эле нааразы болгон вариант катары Банктын кызматкери. Бардык, ал тургай логикасы жок бузуулар, өзгөчө эмгектик мамилелерди бузуу учурунда мүмкүн.

Тышкы бузуулчулардын негизги типтери (бул бөлүмдө азыркы учурдагы маалыматтык коопсуздук боюнча адистер коомдоштугуна кабыл алынган терминология колдонулат):

- «Script Kiddie» же «Башталгыч» – жалпыга белгилүү аярлуу келген бардык маалыматтык ресурсту бузуп кирүүгө кызыкдар адам. Ал Банктын гана маалыматтык ресурстарын бузууга багытталган эмес, коргоонун олуттуу каражаттары табылган учурда ал чабуулду оңой эле токтотот. Эреже боюнча, бузуунун кеңири жайылган ыкмаларын колдонот, өз каражаттарын иштеп чыгарбайт;
- «Black hat» – «Кара хакер» – «Script Kiddie»ден айырмаланып, белгилүү бир ресурсту өжөрлүк менен бузуп кирет, коргоо системаларын айланып өтүүнү «намыс иши» катары эсептейт, чабуулдун жөнөкөй каражаттарын иштеп чыга алат. Өзүн-өзү ишенимдүү көрсөтүү максатында же жеке кызыкчылыгын көздөөгө аракеттенет, өзүнүн кызматын кылмыштуу түзүмдөргө сатып жибериши мүмкүн;
- «Консультант» – маалыматтык ресурстарга жетүү мүмкүнчүлүгү бар сервис компаниясынын кызматкери. Эреже боюнча, тейленүүчү маалыматтык системанын алкагында, уруксатсыз ишти көрсөтүүнүн ар кандай сценарийлери болушу мүмкүн болгон;

- «Elite hacker» же «Гуру» – маалыматтык системаларды бузуу боюнча жогорку квалификациялуу адис. Эреже катары, ал криминалдык түзүмдөрдүн же атаандаш уюмдардын «буюртмасы менен» иштейт. Биринчи учурда, бул финансылык алдамчылык жасоого, экинчи учурда – же маалыматтын сыртка чыгып кетишине же сервердин жеткиликтүү эместигине жана кардарлардын көзүнчө Банкка компрометация жасоого максатталат. Анын арсеналында атайын программалык-техникалык камсыздоонун толук спектри бар, ошондой эле социалдык инженерия ыкмаларын колдонот;
- «Өнөктөш» – Банктын маалыматтык системаларына кирүү мүмкүнчүлүгү бар өнөктөш уюмдун же туунду уюмунун кызматкери. Ички бузуучунун бардык типтерин аныктоого болот, ал, адатта, башкарууга көнбөйт жана Банкта кабыл алынган маалыматтык коопсуздук талаптары тууралуу азыраак билет;
- «Стажер/практикант» – эреже боюнча, маалыматка жана маалымат системаларына жетүүгө мүмкүнчүлүгү чектелген, бирок ал туруктуу Банктын аймагында жүрөт жана маалыматты кыйыр түрдө же социалдык инженерия ыкмалары менен ала алат. Бул стажерди/практикантты жетектеген Банк кызматкери өз милдеттерине шалаакы мамиле жасаганда гана олуттуу зыян келтириши мүмкүн;
- «Кардар» – Банктын аралыктан (дистанциялык) банктык тейлөө сервистерине жетүү мүмкүнчүлүгү бар Банктын кардары. Ушул тейлөө сервистери туура эмес пайдаланылса, идентификациялык маалыматтар жоголсо, же банктык маалыматтык ресурстарга кирүү мүмкүнчүлүгү чектелген болсо да, ага кире алса, тышкы бузуучулардын биринчи үч тиби катары аракет жасашы мүмкүн.

Банктын маалыматтык коопсуздугун камсыз кылуу боюнча негизги чаралар болуп төмөнкүлөр саналат:

- административдик-укуктук жана уюштуруучулук чаралар;
- физикалык коопсуздук чаралары;
- программалык-техникалык чаралар.

АДМИНИСТРАТИВДИК УКУКТУК ЖАНА УЮШТУРУУЧУЛУК ЧАРАЛАР ТӨМӨНКҮЛӨРДҮ КАМТЫЙТ (бирок алар менен чектелбейт):

- Кыргыз Республикасынын мыйзамдарынын жана ВНДБнын талаптарынын аткарылышын контролдоо;
- Саясатты колдоочу эрежелерди, методикаларды жана нускамаларды иштеп чыгууну, ишке киргизүүнү жана аткарылышын контролдоо;
- бизнес-процесстердин Саясаттын талаптарына шайкеш келишин контролдоо;
- маалыматтык системалар жана маалыматтык коопсуздук талаптары менен иштөөгө Банктын кызматкерлерине маалымат берүү жана окутуу;
- инциденттерге, кесепеттерди локалдаштырууга жана минималдаштырууга чара көрүү;
- маалыматтык коопсуздуктун жаңы тобокелдиктерин талдоо;
- жамаатта моралдык-ишкердик климатка байкоо жүргүзүү жана жакшыртуу;
- өзгөчө кырдаалдар жаралган учурда иш-аракеттерди аныктоо;
- Банктын кызматкерлерин жумушка кабыл алууда жана бошотууда профилактикалык иш-чараларды жүргүзүү.

ФИЗИКАЛЫК КООПСУЗДУК ЧАРАЛАРЫ ТӨМӨНКҮЛӨРДҮ КАМТЫЙТ (бирок алар менен чектелбейт):

- өткөрүүчү жана объект ичиндеги режимдерди уюштуруу;
- корголуучу объекттердин коопсуздук периметрин куруу;
- корголуучу объекттерди күнү-түнү, анын ичинде техникалык коопсуздук каражаттарын колдонуу менен коргоону уюштуруу

- корголуучу объекттердин өрткө каршы коопсуздугун уюштуруу;
- Банктын кызматкерлеринин кирүү мүмкүнчүлүгү чектелген жайларга кирүүсүн контролдоо.

ПРОГРАММАЛЫК-ТЕХНИКАЛЫК ЧАРАЛАР ТӨМӨНКҮЛӨРДҮ КАМТЫЙТ (бирок алар менен чектелбейт):

- лицензияланган программалык камсыздоону жана маалыматтык коопсуздуктун сертификацияланган каражаттарын колдонуу;
- коргоо куралдардын периметрин колдонуу (firewall, IPS и т.п.);
- вируска каршы комплекстүү коргоону колдонуу;
- маалыматтык системаларга орнотулган маалыматтык коопсуздук каражаттарын колдонуу;
- маалыматтын үзгүлтүксүз резервдик көчүрмөсүн камсыз кылуу;
- колдонуучулардын, биринчи кезекте артыкчылыктуу колдонуучулардын укуктарын жана аракеттерин контролдоо;
- криптографиялык маалыматты коргоо системаларын колдонуу;
- аппараттык каражаттардын токтобой иштешин камсыз кылуу;
- маалыматтык системанын маанилүү элементтеринин абалына мониторинг жүргүзүү.

Ушул Саясат жана маалыматтык коопсуздук системасы жалпысынан төмөнкү ченемдик укуктук актыларга жана эл аралык стандарттарга таянат (ушул бөлүмдө жалпысынан Банктын маалыматтык коопсуздук системасын түзүү процессине түздөн-түз таасир этүүчү негизги ченемдик укуктук актылар көрсөтүлөт; ошол эле учурда, мамлекеттик деңгээлде маалыматтык коопсуздукту өнүктүрүүнүн стратегиялык аспектилерин сүрөттөгөн же жеке тиркемелерди/кызматтарды маалыматты коргоо эрежелерин жөнгө салган бир катар документтер бар):

- «Кыргыз Республикасынын Улуттук банкы, банктар жана банк иши жөнүндө» Кыргыз Республикасынын 2016-жылдын 16-декабрындагы № 206 Мыйзамы;
- «Электрондук кол жөнүндө» Кыргыз Республикасынын 2017-жылдын 19-июлундагы № 128 Мыйзамы;
- «Электрондук башкаруу жөнүндө» Кыргыз Республикасынын 2017-жылдын 19-июлундагы №127 Мыйзамы;
- «Жеке маалыматтар жөнүндө» Кыргыз Республикасынын 2008-жылдын 14-апрелиндеги № 58 Мыйзамы;
- Кыргыз Республикасынын Улуттук банк Башкармалыгынын 2021-жылдын 22-декабрындагы № 2021-П-20/72-8-(НПА) токтому менен бекитилген Кыргыз Республикасынын коммерциялык банктарында маалыматтык коопсуздукту камсыз кылуу боюнча талаптар жөнүндө жобосу;
- Кыргыз Республикасынын Өкмөтүнүн 2019-жылдын 24-июлундагы № 369 токтому менен бекитилген 2019-2023-жылдарга Кыргыз Республикасынын киберкоопсуздук стратегиясы;
- Кыргыз Республикасынын Коопсуздук кеңешинин 2018-жылдын 14-декабрындагы № 2 чечими менен жактырылган «Санариптик Кыргызстан 2019-2023» санариптик трансформация концепциясы.
- Кыргыз Республикасынын Өкмөтүнүн 2019-жылдын 3-майындагы № 209 токтому менен бекитилген 2019-2023-жылдарга Кыргыз Республикасынын маалыматтык коопсуздугунун концепциясы;
- Кыргыз Республикасынын Улуттук банкынын «Кыргыз Республикасындагы электрондук акчалар жөнүндө» 2016-жылдын 30-мартындагы № 15/6 жобосу;
- Кыргыз Республикасынын Улуттук банкынын «Кыргыз Республикасынын банктарында тобокелдиктерди тескөө боюнча минималдуу талаптар жөнүндө» 2017-жылдын 15-июнундагы № 2017-П-12/25-8-(НКА) жобосу;

- Маалыматтык коопсуздук боюнча «Маалыматтык технологиялар - Коопсуздук техникалары - Маалыматтык коопсуздукту башкаруу системалары - Талаптар» ISO/IEC 27001:2013 эл аралык стандарты;
- 3.2.1 версиясындагы PCI DSS эл аралык стандарт, (Төлөм карталары тармагынын маалыматтарын коргоо стандарты – төлөм карталары индустриясынын маалыматтарынын коопсуздук стандарты);
- PCI 3DS эл аралык стандарты (Core Security Standard) – төлөм картасын физикалык берүүсүз төлөм функцияларын аткаруучу же көрсөтүүчү уюмдар үчүн коопсуздук стандарты;
- Колдонуучунун коопсуздугун камсыздоочу концепция (CSCF) SWIFT (мындан ары - CSCF SWIFT);

Банкта ченемдик укуктук актылардын талаптарын сактоону, интеллектуалдык менчик укуктарын сактоону, мыйзам менен корголгон жеке маалыматтарды коргоону, криптографиялык каражаттарды колдонуу боюнча чектөөлөрдү сактоону камсыз кылуу үчүн тиешелүү процесстер ишке киргизилди.

ISO/IEC 27001 жана PCI DSS эл аралык стандарттарынын бардык талаптары жана жоболору тиешелүү документтер менен аныктала турган аларды колдонуу жаатында аткаруу үчүн милдеттүү болуп саналат.

Маалыматтык коопсуздуктун каражаттарын жана ыкмаларын иштеп чыгуу жана колдонуу учурунда Банк тарабынан үчүнчү жактар менен түзүлгөн келишимдик милдеттенмелердин жана келишимдердин талаптары эске алынат.

Үчүнчү жактардын Банктын маалыматтык ресурстарына жетүү мүмкүнчүлүгү мындай жеткиликтүүлүктү камсыз кылууда келип чыгышы мүмкүн болгон тобокелдиктерди талдоодон жана жөндүү коргоо чаралары көрүлгөндөн кийин гана ишке ашырылат. Зарыл болгон учурда (атап айтканда, ченемдик укуктук актылардын же эл аралык стандарттардын талаптары бар болсо) Банк контрагенттерди (товарларды жана кызмат көрсөтүүлөрдү берүүчүлөрдү) белгилүү бир талаптарга ылайыктуулугун текшерет (мисалы, көрсөтүлгөн кызматтардын талаптарынын PCI DSS стандартынын талаптарына шайкештигин тастыктаган документтерди текшерүү).

Саясаттын негизинде маалыматтык коопсуздукту камсыз кылуунун конкреттүү эрежелерин жана ыкмаларын, стандарттардын колдонулуу жаатындагы жеке саясатчыларды ж.у.с. жөнгө салуучу бир катар ички ченемдик укуктук документтер иштелип чыгат. Мындай документтер Саясаттын талаптарын толукташы жана кеңейтиши мүмкүн, бирок алар менен карама-каршы келбеши керек.

«ХАЛЫК БАНК КЫРГЫЗСТАН» ААК МААЛЫМАТТЫК КООПСУЗДУК САЯСАТЫ МЕНЕН ТААНЫШКАНЫҢЫЗ ҮЧҮН СИЗГЕ ЫРААЗЫЧЫЛЫК БИЛДИРЕБИЗ