

ЎЗБЕКИСТОН РЕСПУБЛИКАСИ ИИВ МАЛАКА ОШИРИШ ИНСТИТУТИ



АХБОРОТ ХАВФСИЗИГИ СИЁСАТИ БЎЙИЧА

ЎҚУВ ҚЎЛЛАНМА

ТОШКЕНТ-2025

КИРИШ

Ўз вазифаларини бажариш учун Малака ошириш институти ахборот технологиялари инфратузилмасини шакллантиради ва ривожлантиради, шунингдек ахборот-коммуникация технологияларини самарали жорий этади. Институтда ахборот хавфсизлигини таъминлаш вазифаси ахборот тизимларининг ишончли ва узлуксиз ишлашини таъминлаш устувор вазифадир.

Ахборот хавфсизлиги, конфиденциаллик, яхлитлик ва ҳимояланган конфиденциал маълумотларнинг сақланиши нуқтайи назаридан кўриб чиқилади.

Ахборот хавфсизлигига сиёсий, амалиётлар, жараёнлар ва ташкилий тузилмаларни ўз ичига олган чора-тадбирларни амалга ошириш орқали эришилади. Ахборот хавфсизлиги чора-тадбирлари Институт ва унинг инфратузилмаси маълумотларини (ахборотларини) кенг миқёсли таҳдидлардан ҳимоя қилишни таъминлаши, узлуксиз ишлашини таъминлаш, таҳдидларни амалга оширишдан етказиладиган зарарни минималлаштириш, уларнинг таъсирини башорат қилиш ва олдини олиш, ишбилармонлик обрўсини сақлаш ва қонун талабларига жавоб бериш керак.

Институтнинг ахборот хавфсизлиги сиёсати унинг ахборот активларини, Институт инфратузилмасини ҳимоя қилишнинг асосий тамойилларини белгилайди. Бу Институтда ахборот хавфсизлигини бошқариш тизимини (АХБТ) бошқариш ва қуриш бўйича тегишли ҳужжатларни қабул қилиш учун асос бўлиб хизмат қилади. Ушбу ахборот хавфсизлиги сиёсати – ўз фаолиятида олиб борадиган, ахборот хавфсизлиги соҳасидаги ҳужжатлаштирилган кўрсатмалар, қоидалар, жараёнлар ва амалиёт тўпламидир.

АТАМАЛАР ВА ТАЪРИФЛАР

Мазкур ҳужжатда Ўз ДСт 2927:2015 “Ахборот технологиялари. Ахборот хавфсизлиги. Атамалар ва таърифлар” ва Ўз ДСт 1047:2018 “Ахборот технологиялари. Атамалар ва таърифлар” давлат стандартига мувофиқ қуйидаги атамалар ва таърифлардан фойдаланилган:

аутентификатсия қилиш – фойдаланувчи (тармоқ абоненти, хабар жўнатувчи), дастур, қурилма ёки маълумотлар (ахборот, олинадиган хабар, калит)нинг ҳақиқийлигини белгилаш жараёни;

авторизатсия – муайян шахсга ёки шахслар гуруҳига муайян ҳаракатларни амалга ошириш ҳуқуқини бериш;

ахборот хавфсизлиги – ахборот муносабатларининг субектларига номақбул зиёнларни келтириши мумкин бўлган табиий ёки сунъий хусусиятли тасодифий ёки қасддан қилинган таъсирлардан ахборот ва таъминлаб турадиган инфраструктуранинг муҳофаза қилинганлиги;

ахборот хавфсизлиги таҳдидлари – ахборот тизимлари хавфсизлигининг бир ёки бир нечта жиҳатларини бузилишига олиб келадиган потенциал ҳаракатлар ёки ҳодисалар;

ахборот хавфсизлиги инциденти – ахборот хавфсизлигининг ягона воқеаси ёки бир қатор нохуш ёки қутилмаган воқеалари бўлиб, ушбу воқеалар туфайли ахборотни компрометатсия қилиш эҳтимоли ва ахборот хавфсизлигига таҳдидлар эҳтимоли катта бўлади;

ахборот ресурслари – ахборот тизими таркибидаги электрон шаклдаги ахборотлар, маълумотлар банклари, маълумотлар базаси;

ахборот тизими – ахборотларни йиғиш, сақлаш, излаш, ишлаш ва улардан фойдаланиш имконини берувчи ахборот ресурслари, ахборот технологиялари ва алоқа воситаларининг ташкилий тартибга солинган йиғиндиси;

ахборотлаштириш объекти – турли даража ва мақсадлардаги ахборот тизимлари, телекоммуникация тармоқлари, ахборотни қайта ишлаш техник воситалари, бу воситалар ўрнатилган ва эксплуататсия қилинадиган, шунингдек, музокаралар, шу жумладан, конфиденциал музокаралар олиб бориш учун мўлжалланган хоналар;

ахборот хавфсизлиги сиёсати – ахборот хавфсизлигини бошқариш тизими, объектлари ва иштирокчиларининг фаолият турларини белгилайдиган ва чеклайдиган қоидалар тўплами;

ахборот хавфсизлигини бошқариш тизими (АХБТ) – ахборот хавфсизлигини ишлаб

чиқиш, жорий қилиш, унинг ишлаши, мониторинги, таҳлили, унга хизмат кўрсатиш ва уни такомиллаштириш учун мўлжалланган бизнес рискларни баҳолаш усулларида фойдаланишга асосланган умумий бошқариш тизимининг қисми;

бузгунчи – ахборот тизими ва унинг ресурсларидан рухсат этилмаган тарзда фойдалана олишдан манфаатдор бўлган ва уларни рухсатсиз олиш ёки ўзгартириш учун олдиндан ўйлаб ҳаракат қилган шахс ёки ташкилот;

дастурий таъминот – маълумотларни қайта ишлаш тизими ва дастурий ҳужжатларни ишлатиш зарур бўлган дастурлар тўплами;

фойдалана олишлик – ахборот ва унинг ташувчисининг ҳолати, унда фойдаланувчилар томонидан улар учун мўлжалланган ахборотнинг ҳеч қандай қаршиликсиз ва ўз вақтида олиниши таъминланади;

фойдалана олиниши чекланган ахборот – давлат сирлари ва конфиденсиал ахборотдан иборат маълумотларга эга бўлган ҳужжатлаштирилган ахборот, улардан фойдалана олиш қонун ҳужжатларига мувофиқ чегараланади;

конфиденсиаллик – ахборот ва унинг ташувчисининг ҳолати, бунда у билан рухсат этилмаган тарзда танишишнинг ёки рухсат этилмаган тарзда ҳужжатлаштириш (нусха кўчириш)нинг олдини олиш таъминланади;

конфиденсиал ахборот – Ўзбекистон Республикаси қонун ҳужжатларига мувофиқ фойдаланиш чекланган, давлат сирларига мансуб ахборот мавжуд бўлмаган ҳужжатлаштирилган ахборот;

локал ҳисоблаш тармоғи – битта бино ёки битта корхона билан чекланган битта локал зонада қатор ҳисоблаш техникаси қурилмаларини боғлайдиган ахборот-ҳисоблаш тармоғи;

маълумотлар базаси – обектив шаклда ифодаланган ва бу маълумотлар электрон ҳисоблаш машиналари ёрдамида топиладиган ва қайта ишланадиган тарзда тизимлаштирилган маълумотлар (моддалар, ҳисоб-китоблар) жами;

риск – муайян таҳдидни амалга оширишда маълумотларни қайта ишлаш тизимининг муайян заифлигидан фойдаланиш имконияти;

рискларни баҳолаш – риск моҳиятини аниқлаш мақсадида бажариладиган, ҳисобланган риск ва риск мезонларини таққослаш жараёни;

риск таҳлили – маълумотларни қайта ишлаш тизими ресурсларини, ушбу ресурсларга таҳдидларни ва ушбу таҳдидларга тизим заифлигини идентификация қилиш процедураларининг мунтазам бажарилиши;

рухсатсиз фойдалана олиш – тизимда белгиланган фойдалана олишни чеклаш қоидаларини бузган ҳолда субектнинг объектдан ёки ахборотдан фойдалана олиши;

сервер – компьютерга, бошқа бир компьютерга хизмат кўрсатиш имконини берадиган аппарат ва дастурий таъминот йиғиндиси;

яхлитлик – ахборот ва унинг ташувчисининг ҳолати бўлиб, бунда умуман ва унинг алоҳида таркибий қисмларининг бўлинмаслиги ва рухсат этилмаган тарзда ёки қасддан йўқ қилиниши, бузилиши, чиқиб кетиши, ўғирланиши, қалбакилаштирилишининг олдини олиш таъминланади;

заифлик – маълумотларни қайта ишлаш тизимидаги камчилик, ундан фойдаланиш унинг яхлитлигини бузиши ва нотўғри ишлашига олиб келиши мумкин.

Белгилар ва қисқартмалар

Ушбу сиёсатда қуйидаги белгилар ва қисқартмалардан фойдаланилган:

ХДФУ – хизмат доирасида фойдаланиш учун;

АКТ – ахборот-коммуникация технологиялари;

ИМУТ – идоралараро маълумот узатиш тармоғи;

АХБТ – ахборот хавфсизлигини бошқариш тизими;

МБ – маълумотлар базаси;

МББТ – маълумотлар базасини бошқариш тизими;

ШДМ – Шахсга доир маълумотлар;

ШДМБ – Шахсга доир маълумотлар базаси;
ЭРИ – электрон рақамли имзо;
VLAN (*Virtual Local Area Network*) – тармоқни виртуал равишда бо'лиш имкониятини берувчи технология;
VPN (*Virtual Private Network*) – виртуал хусусий тармоқ
IP, ISMP, TSP, UDP (*Internet Protocol*) – Интернет протоколлари ҳисобланади;
АКТ – Ахборот-коммуникация технологиялари;
HDD, USB, SD, DVD – маълумот сақловчи қурилмалар;

Фойдаланиш соҳаси

Институтнинг ахборот хавфсизлиги сиёсати ахборот хавфсизлиги соҳасидаги мақсад ва вазифаларни, қоидаларни, кўрсатмаларни, шунингдек ташкилий, технологик ҳамда Институт томонидан ўз фаолиятида қўлланиладиган бошқа асосий тамойилларни белгилайди.

Ушбу сиёсатнинг талаблари Институтда мавжуд конфиденсиал ахборотни қайта ишлаш, сақлаш ва узатиш учун барча маълумотлар ва манбаларга нисбатан қўлланилади. Давлат сирларини ўз ичига олган маълумотларнинг ҳимояси қонун ҳужжатларига мувофиқ таъминланади.

Ушбу Ахборот хавфсизлиги сиёсати талаблари Институтнинг ходимларига (штатдаги, вақтинча, шартнома асосида ишловчи ходимларга ва бошқаларга), иш жойи ва лавозимидан қатъий назар, шунингдек Институтнинг ахборотлаштириш объектларига қандайдир сабабларга кўра қонуний кириш ҳуқуқига эга бўлган учинчи томон (пудратчилар, аудиторлар, ташриф буюрувчилар, хизмат кўрсатувчи ходимлар ва шу кабилар) ҳамда тингловчилари учун қўлланилади.

Ахборот технологиялари бўлими томонидан ушбу ахборот хавфсизлиги сиёсати қоидаларига риоя қилиниши устидан доимий мониторинг олиб борилади.

Мақсад ва вазифалар

Ахборот хавфсизлиги сиёсатининг асосий мақсадлари қуйидагилардан иборат:

ахборот муносабатлари субъектларини моддий, жисмоний, маънавий ёки бошқа зарар етказилишидан, ахборотлаштириш объектларининг фаолиятига тасодифий ёки атайлаб рухсатсиз аралаштириш ёки улардаги маълумотларга рухсатсиз кириш ва ундан ноқонуний фойдаланишдан ҳимоя қилиш;

ахборот хавфсизлиги соҳасидаги қонун ҳужжатлари, йўриқномалар ва низомларга ва умумий сиёсатга риоя қилинишини таъминлаш;

Институт фаолиятига оид ахборотларнинг конфиденсиаллиги, яхлитлиги ва очиклигини таъминлаш, муҳим ахборот ресурслари, ахборот тизимлари ва бошқа ахборотлаштириш воситаларининг ишлашини таъминлаш;

ахборот хавфсизлиги ҳодисаларининг мумкин бўлган оқибатларини бартараф этиш ва минималлаштириш, таҳдидларни амалга оширишни башорат қилиш, олдини олиш ва тўхтатиш, ахборот тизими ва АХБТда заифликларни аниқлаш ва йўқ қилиш;

кенг қамровли таҳдидларни ҳисобга олган ҳолда, ахборот хавфсизлигини ва ахборот тизимлари, манбалари ва маълумотлар базаларининг узлуксиз ишлашини таъминлаш бўйича ташкилий ва техник тадбирлар мажмуини шакллантириш.

Ахборот хавфсизлиги сиёсатининг асосий вазифалари қуйидагилардан иборат:

ахборот хавфсизлигига ички ва ташқи таҳдидларни, ахборот муносабатларининг манфаатдор томонларига зарар етказадиган сабаблар ва шароитларни ўз вақтида аниқлаш ва прогноз қилиш;

Институтнинг локал ва корпоратив тармоғи, ахборот тизимлари ва ресурсларига рухсатсиз киришнинг олдини олиш ва уринишларни аниқлаш;

ҳимоя объектларини аниқлаш, ахборот ресурслари, тизимларини таснифлаш, шунингдек автоматлаштирилган тизимлар учун хавфсизлик синфини Ўз ДСт 2814:2014 давлат стандарти орқали таснифлаш;

химоя объектлари ва химояланадиган ахборотларнинг конфиденсиаллиги, яхлитлиги ва фойдалана олишлилиги устидан назоратни таъминлаш;

Институтнинг ахборот тизимлари ва АХБТларидаги заифликларни аниқлаш ва бартараф этиш;

Институт инфратузилмасида қўлланиладиган ахборот технологияларига ахборот хавфсизлиги нуқтайи назаридан ягона талабларни ишлаб чиқиш;

ахборот хавфсизлигига таҳдидлардан химоя қилиш ва уларга қарши курашишнинг ташкилий-техник усуллари ва замонавий техник шунингдек дастурий воситаларидан фойдаланган ҳолда ахборот хавфсизлигини таъминлашга комплекс ёндашувни таъминлайдиган Институтнинг АХБТни яратиш ва ривожлантириш;

ахборотлаштириш объектларида ахборот хавфсизлигига таҳдидларни амалга ошириш натижасида етказилган зарарни максимал даражада камайтириш учун шароит яратиш;

ахборот хавфсизлиги бўйича тренинглар ўтказиш, ходимларнинг ахборот хавфсизлиги хавфлари тўғрисида хабардорлигини ошириш;

Институтда ахборот хавфсизлигини таъминлаш бўйича кадрларнинг билим ва кўникмаларини шакллантириш ҳамда ошириш.

АСОСИЙ ҚОИДАЛАР

Институтнинг ахборот хавфсизлиги сиёсати қуйидаги асосий тамойилларга асосланади:

Қонунийлик – Ўзбекистон Республикаси Конституцияси ва қонунчилигига, фойдаланувчиларнинг қонуний ҳуқуқларига, амалдаги қонунлар ва норматив ҳужжатлар талабларига қатъий мувофиқ равишда ахборот хавфсизлиги чораларини амалга ошириш;

жалб қилиш ва шахсий жавобгарлик – Институт раҳбарияти ва барча ходимлари ахборот хавфсизлигини таъминлаш жараёнида иштирок этадилар ва улар меҳнат шартномалари ва ходимларнинг лавозим йўриқномаларида, шунингдек ходимлар билан тузилган бошқа турдаги шартномаларда (битимларда) киритилган ахборот хавфсизлиги талабларига риоя этилиши учун шахсан жавобгардирлар;

ходимларнинг хабардорлиги ва билимлари – Институт ходимларини ахборот хавфсизлигини таъминлаш масалалари бўйича даврий равишда ўқитишва сертификатлаш, шунингдек, ахборот хавфсизлигини таъминлаш учун масъул бўлган мутахассисларнинг малакасини ошириш;

ўзаро ҳамкорлик ва ҳаракатларнинг мувофиқлиги – ахборот хавфсизлигини таъминлаш бўйича ҳаракатлар манфаатдор идоралар билан келишилган ҳолда амалга ошириш, шунингдек, мақсадлар, вазифалар, принциплар ва воситалар бўйича ўзаро ҳамкорликда иш олиб бориш;

иктисодий мақсадга мувофиқлик – ахборот хавфсизлиги чоралари, уларни амалга ошириш харажатлари, ахборот хавфсизлигига таҳдидлар эҳтимоли ва уларни амалга оширишда мумкин бўлган йўқотишлар миқдорини ҳисобга олган ҳолда танланади;

ҳисобот бериш ва хатти-ҳаракатларнинг ҳисоби – Институт ходимлари томонидан ахборот хавфсизлиги бўйича қабул қилинган талабларнинг бажарилишини мониторинг қилиш, ходимларнинг ахборот активларига киришини таъминлаш ва бошқариш, ходимларнинг ахборот активлари билан боғлиқ барча ҳаракатларини ҳисобга олиш;

Институт ахборот хавфсизлигини таъминлаш бўйича ўз функцияларини бажаришда:

ахборотни ва бошқа химоя объектларини белгилайди ва таснифлайди;

ахборот хавфсизлиги таҳдидларини обектив ва ҳар томонлама таҳлил қилиш ва прогнозлаш, ахборот хавфсизлигини таъминлаш бўйича талаблар ва чора-тадбирларни ишлаб чиқади;

ахборот хавфсизлиги таҳдидларининг олдини олиш, йўқ қилиш ва зарарсизлантиришга қаратилган чора-тадбирлар мажмуини амалга ошириш учун зарур бўлинмаларнинг ишини ташкил қилади;

ахборотни муҳофаза қилиш воситаларини сертификатлаш ва лицензиялаш йўли билан ахборотни химоя қилиш воситаларини жорий этиш, ишлаб чиқиш, улардан фойдаланиш устидан назоратни амалга оширади ва таъминлайди;

вакти-вакти билан ахборот активларини ҳимоя қилинганлиги ҳолатини баҳолайди, ахборот хавфсизлигини бузилишларини аниқлайди, ҳисобга олади ва тезкор чоралар кўради.

ИНСТИТУТ ТАРМОҒИ ВА УНДАН ФОЙДАЛАНУВЧИЛАРИНИНГ МАЖБУРИЯТЛАРИ

Институт тармоғи Вазирликнинг тармоғига “Ўзбектелеком” АК телекоммуникация операторидан ижарага олинган ВПН каналлари ёрдамида уланади.

Тегишли аутентификатсия маълумотларига эга бўлган ва Институт тармоғига кириш учун рўйхатдан ўтишнинг белгиланган тартибидан ўтган Институт ходимлари ва тингловчилари тармоқ фойдаланувчилари ҳисобланади.

Тармоқ фойдаланувчилари мажбуриятлари қуйидагилар:

тармоқ, шунингдек интернет тармоғидан ўз лавозим мажбуриятларини бажариш мақсадида фойдаланиш;

ҳаракат ёки ҳаракатсизлик орқали тармоқнинг техник ва ахборот ресурсларига зарар етказиш эҳтимолини йўқ қилиш;

тармоқ орқали ахборот тизимлари ва ресурсларига рухсатсиз киришга уринмаслик;

ташқи манбалардан олинган файлларни ишлатишдан ёки очишдан олдин, уларда зарарли дастур мавжудлигини текшириш;

агар ушбу Йўриқнома талабларига риоя қилишни таъминлаш имкони бўлмаса, бу ҳақда дарҳол Ахборот технологиялари бўлими бошлиғини ёки тармоқ администраторини ва/ёки Ахборот технологиялари бўлими ходимларини хабардор қилиш.

Тармоқ фойдаланувчиларига қуйидагилар тақиқланади:

иш станциясида вирусга қарши ҳимояни ўчириб қўйиш, зарарли дастурларни тармоқ орқали юбориш ва тарқатиш;

конфиденсиал (ХДФУ грифли) маълумотларни очик шаклда тармоқ орқали узатиш, шу жумладан корпоратив электрон почта ва “дос.иив.уз” электрон ҳужжат айланиши тизимларидан фойдаланиш. Ушбу маълумотлар конфиденсиаллигини ва яхлитлигини таъминлаш учун маълумотларни криптографик ҳимоя қилиш воситалари ва электрон рақамли имзолар ёрдамида узатилиши керак.

ахборот ресурслари ва тизимларига, шунингдек бошқа активларига кириш (авторизатсия) маълумотларини Институтнинг бошқа ходимларига ёки бегона шахсларга бериш;

тармоққа бошқа фойдаланувчиларга берилган ҳуқуқлардан фойдаланган ҳолда уланиш;

рухсатсиз шахсларнинг тармоққа уланишига рухсат бериш;

тармоқни сканерлайдиган (турли хил снифферлар, порт сканерлари) дастурлардан фойдаланиш;

қўшимча тармоқ протоколларини ўрнатиш, тармоқ администратори ва ахборот хавфсизлиги администраторидан яширинча тармоқ протоколи созламаларини ўзгартириш;

ахборот ресурслари ва тармоқ тизимларига бошқаларнинг кириш ҳуқуқларини мустақил равишда ўзгартириш;

рухсат берилган дастурий таъминотлар таркибига кирмайдиган ҳар қандай дастурий таъминотларни ўрнатиш, тармоқдаги бошқа фойдаланувчининг иш станциясидан фойдаланиш тақиқланади.

Ушбу йўриқнома талаблари мунтазам равишда бузилганда, ходим тармоқдан узилади.

Фойдаланувчи фаолияти натижасида мулкка зарар ёки шикаст етганда, етказилган зарар фойдаланувчи томонидан қопланади.

ПАРОЛЛАРДАН ФОЙДАЛАНИШ

Шахсий паролни сир сақлаш учун фойдаланувчи шахсан жавобгардир. Паролни бошқаларга ошкор қилиш, шунингдек паролни жамоат жойларида сақлаш тақиқланади.

Ходим ўз паролларини қоғозда сақлашга фақат парол эгаси томонидан шахсий муҳр

билан муҳрланган кутида ёки сейфида сақлашга рухсат этилади.

Зарурати туғилганда (командировка, таътил, ўрганишлар, текширишлар, ва бошқалар), фойдаланувчининг пароли талаб қиладиган бўлса, унинг паролини компрометатсия қилишга рухсат берилади.

Паролни бериш фактини фойдаланувчи томонидан Ахборот хавфсизлиги администраторига етказиш керак. Ишлаб чиқариш ёки текшириш ишларининг охирида фойдаланувчилар мустақил равишда компрометатсия қилинган паролларни дарҳол мажбурий равишда ўзгартиришлари шарт.

Фавқулудда вазиятлар, шунингдек фойдаланувчи қайд ёзуви ва паролларни ўзгартиришга технологик эҳтиёжи туғилган тақдирда Ахборот хавфсизлиги администраторига паролларни ўзгартиришга рухсат берилади. Бундай ҳолларда пароллари ўзгартирилган фойдаланувчилар ўзларининг пароллари ўзгартирилганлигини билгандан сўнг дарҳол янги парол яратишга мажбурдирлар.

Агар фойдаланувчи узоқ вақт хизмат сафари, касаллик ва бошқа сабабларга кўра ишда бўлмаган тақдирда унинг аккаунти ахборот тизими орқали блокланади, зарур ҳолларда ушбу фойдаланувчи ресурсларига нисбатан бошқа фойдаланувчиларнинг кириш ҳуқуқлари Ахборот хавфсизлиги администраторига хабар берган ҳолда ўзгартирилади.

Парол эгалари юқорида санаб ўтилган талаблардан хабардор бўлишлари ва ушбу талабларга жавоб бермайдиган пароллардан фойдаланиш, шунингдек парол маълумотларини компрометатсия қилиш масъулияти ҳақида огоҳлантиришлари лозим.

Серверлар, тармоқ ускуналари ва ахборотни муҳофаза қилиш воситаларига қўйилган пароллар хавфсиз жойда, ёнғинга қарши сейфда сақланиши керак. Ушбу паролларга кириш фақат Ахборот хавфсизлиги администратори ва Ахборот технологиялари бўлими бошлиғи томонидан амалга оширилади.

Институт ходимлари ишчи станциялари ва тармоққа киришдаги пароллар 3 ойда бир маротаба ўзгартиришлари керак.

Бегона шахсларнинг серверга, тармоқ ускуналарига ва ахборотни муҳофаза қилиш воситаларига киришини чеклаш, уларга кириш пароллари, шунингдек уларга масофадан киришни таъминлайдиган иш станциялари, уларнинг ишлаши учун масъул ходимлар томонидан шакллантирилади ва фойдаланилади.

Белгиланган пароллар режага асосан ўзгартириш Ахборот хавфсизлиги администратори томонидан ҳар 30 кунда бир марта амалга оширилиши керак.

Ахборот хавфсизлиги администратори томонидан вақти-вақти билан паролларни ўзгартириш талабининг бажарилиши Ахборот технологиялари бўлими бошлиғи томонидан назорат қилинади.

Институт ходимларининг ахборот тизимларига кириши парол асосида амалга оширилади, унинг режадаги ўзгариши Институт ходимлари томонидан 60 кун ичида камида бир марта амалга оширилади. Бу талабни бажариш ҳар бир ходимга юклатилади. Улар томонидан ушбу тартиб амалга оширилиши юзасидан назорат қилиш ишлари назорат тизимини тартибга солиш ва ахборот тизимларига киришни назорат қилиш билан таъминланиши мумкин.

Агар парол компрометатсияга учраган деб гумон қилинган бўлса, Институт ходими дарҳол Ахборот хавфсизлиги администраторига хабар бериши ва режадан ташқари паролни ўзгартириши шарт.

Ходимнинг қайд ёзувларини ўчириш орқали киришни блокировка қилиш унинг ваколатлари тугатилган тақдирда (ишдан бўшатиш, бошқа ишга ўтиш ва ҳ.к.) амалга оширилади ва ушбу ходимнинг тизимдаги сўнгги сессияси тугагандан сўнг дарҳол амалга оширилиши керак.

Барча фойдаланувчилар учун паролларнинг режадан ташқари тўлиқ ўзгарилиши Ахборот хавфсизлиги администратори ва парол ҳимоясини бошқариш ваколатига эга бўлган бошқа ходимлар томонидан амалга оширилиши керак.

Ишчи станция созламалари, агар фойдаланувчи 5 дақиқа ишчи ҳолатида бўлмаса блок ҳолатига, 30 дақиқа ухлаш режимига ва 120 дақиқада гибернатсия ҳолатига ўтиши автоматлаштирилган тарзда бўлиши керак.

Институт ходимлари ва тингловчилари қуйидагиларга мажбур:

турли ахборотлаштириш объектларига киришда ҳар бир қайд ёзувлари учун турли паролларни қўллаш;

Ахборот хавфсизлиги администраторига киришни блокировка қилиш учун уларнинг пароли бузилганлиги тўғрисида хабар бериш;

парол хавфсизлигини таъминлаш;

бегона шахсларга ва ходимларга шахсий паролни ошкор қилмаслик.

Институт ходимлари ўз паролларини ҳимоя қилиш бўйича етарли чораларни қўллашлари шарт, шу жумладан:

шахсий паролни ёдда сақлаш ва бошқа ходимларни билмаслигини таъминлаш;

шахсий паролни фақатгина таркибий бўлинма раҳбаридан ташқари ҳар қандай вазиятда ҳеч кимга бермаслик;

паролдан фойдаланганда (масалан, уни киритиш), унинг бузилиш эҳтимолини истисно қилиш учун зарур чораларни кўриш (масалан, киритилган паролни визуал кўриш имкониятини истисно қилиш).

Ходим томонидан ишлатилган пароллардан Институт ахборот тизимидан ташқаридаги тизимлар (масалан, Интернет-сайтларда, Интернет-дўконларда, электрон тўлов тизимлари ва бошқа тизимлар)да фойдаланиш тақиқланади.

Ахборот хавфсизлиги администраторига ходимларнинг паролларини аниқ матнда ёки ҳеш қийматлари шаклида сақлаш, шунингдек паролларни умумий ресурсларга жойлаштириш ёки электрон почта орқали юбориш тақиқланади (паролларни фақат корпоратив электрон почта орқали ходимнинг ўзига юборишдан ташқари).

Институт ходимлари ва тингловчилари томонидан пароллар бузилган тақдирда, ушбу йўриқномани бузганлик ҳолатлари бўйича Ахборот технологиялари бўлими бошлиғига зудлик билан хабар бериш.

ПАРОЛНИ ЯРАТИШ ТАЛАБЛАРИ

Институтнинг ахборотлаштириш объектларига ҳамда ишчи станцияларига кириш учун паролларни шакллантиришда қуйидаги талабларга жавоб бериш керак:

парол камида 8 та белгилардан иборат бўлиши;

парол белгиларида катта ва кичик ҳарфлар, рақамлар ва махсус белгилардан иборат бўлиши;

паролда осон ҳисобланадиган белгилар комбинатсиялари (исмлар, фамилиялар, туғилган кунлар ва бошқалар), шунингдек, умумий қабул қилинган қисқартмалардан иборат бўлмаслиги;

паролни ўзгартирганда, янги қиймат камида 3 ҳолатда аввалгисидан фарқ қилиши лозим.

Администраторларнинг пароли кичик ва катта ҳарфлар, рақамлар ва махсус белгилар ёрдамида камида 12 та белги бўлиши керак.

АНТИВИРУСДАН ФОЙДАЛАНИШ

Ишчи станциялари ва серверларини ўрнатилган антивирус дастурисиз ишлатиш тақиқланади. Антивирус дастурини янгилаб туриш керак.

Агар зарарли дастур мавжудлигига шубҳа туғилса (дастурларнинг нотўғри ишлаши, график ва овозли эффектларининг пайдо бўлиши, маълумотларнинг бузилиши, йўқолган файллар, тизим хатоси ҳақидаги хабарларнинг тез-тез пайдо бўлиши), фойдаланувчининг ўзи ёки Ахборот хавфсизлиги администратори билан биргаликда ўз иш станциясида антивирус назоратини амалга ошириши керак.

Компютер вирусларини юктирган файлларни антивирус текшируви пайтида аниқланган бўлса, фойдаланувчилар:

ишни тўхтатиб қўйиш;

вирусни юктирган файллар аниқланганлиги тўғрисида Ахборот хавфсизлиги администратори, шунингдек ушбу файллардан ўз ишларида фойдаланадиган фойдаланувчиларни дарҳол хабардор қилиш керак;

ундан кейинги фойдаланиш таҳлилини ўтказиш;

зарарланган файлларни зарарсизлантириш ёки йўқ қилиш;

агар антивирус дастури зарарсизлантира олмаган янги вирус аниқланса, вирус билан зарарланган файлни Ахборот хавфсизлиги администраторга тақдим этиш.

Фойдаланувчига ишчи станциясидан Ахборот хавфсизлиги администратори розилигисиз қуйидагилар тақиқланади:

антивирус ҳимоя воситалари созламалари ва конфигурациясини ўзгартириш;

вирусга қарши ҳимоя воситаларини олиб ташлаш ёки тизимга қўшиш;

иш станциясида ўрнатилган антивирус ҳимояси воситаларида текширмасдан туриб сақлаш воситаларидан фойдаланиш;

электрон почта орқали келган номаълум дастурларни ишга тушириш.

Фойдаланувчилар қуйидагиларга мажбур:

Номаълум, шубҳали ёки ишончсиз манбалардан олинган электрон почта хабарларига қўшимчаларни очмаслик. Бундай бириктирилган файллар тезда ўчирилиши керак;

номаълум ёки шубҳали манбалардан маълумотларни юкламаслик;

агар асосий фаолиятнинг бир қисми сифатида талаб қилинмаса, ўқиш/ёзиш рухсати билан мантиқий дискларга умумий киришни таъминлашдан сақланиш;

номаълум ёки шубҳали манбалардан олинган ахборот ташувчисидан фойдаланишдан олдин, уни вируслардан текшириш;

ҳар куни, ишчи станциясини дастлабки юклашда, резидент антивирус монитор мавжудлигига ишонч ҳосил қилиш ва агар мавжуд бўлмаса, Ахборот хавфсизлиги администраторини хабардор қилиш;

Ахборот хавфсизлиги администраторидан тизимда вирус мавжудлиги тўғрисида, шунингдек, вирусга шубҳа туғилганда хабарнома олингандан сўнг, ишчи станциясини режадан ташқари антивирус текширувини мустақил равишда амалга ошириш.

ТАШУВЧИ, САҚЛОВЧИ ВА МОБИЛ ҚУРИЛМАЛАР ФОЙДАЛАНИШ

Институт ходимларга тегишли бўлган ташувчи, сақловчи ва мобил қурилмалар фойдаланиш қуйидаги ҳолларда тақиқланади:

конфиденциал музокаралар ва конфиденциал характердаги тадбирлар ўтказиладиган хоналарда;

локал тармоқ ва ахборот тизимларига уланиш учун;

масофадан фойдаланувчиларнинг мобил қурилмаларини умумий фойдаланишдаги телекоммуникация тармоғи ва интернет орқали ахборот тизимига ва тармоққа улаш;

конфиденциал ёки бошқа ҳимояланган маълумотларни, шу жумладан паролларни ва бошқаларни ташувчилар сифатида фойдаланиш.

Институт ҳудудида бир марталик рухсатномаси бўлган учинчи шахслар томонидан мобил қурилмалардан фойдаланишни тақиқлаш чоралари кўрилиши мумкин.

Ахборот-коммуникация тизимида фақат Институтнинг мулки бўлган ва рўйхатдан ўтган мобил қурилмалар, маълумотларни сақловчи ва ташувчи ташқи қурилмалардан фойдаланишга рухсат берилади.

Мобил қурилмалар, маълумот сақловчи ва ташувчи қурилмаларни ҳисобга олиш журнали Институт Ташкилий бўлим Қўриқлаш отряди ходимлари томонидан юритилади (ИИВнинг 194 буйруғи асосида).

Ҳисобга олинган мобил қурилмаларни (ноутбуклар), маълумотларни сақловчи ва ташувчи ташқи қурилмаларни (USB флаш-хотиралар), ҳафтасига камида бир марта, вирусга қарши воситалар томонидан зарарли дастур бор йўқлигини аниқлаш мақсадида текшириб туриши керак.

Институтнинг ҳар қандай конфиденсиал маълумотларини сақлаш учун мобил қурилмаларидан фойдаланиш тақиқланади.

Мобил қурилмаларидан фақат Институт ахборот тизимларига улашиш учун фақат бошқариладиган ҳудуд доирасида фойдаланиш мумкин. Бундай ҳолда, уларга қўйиладиган талаблар иш станциялари билан бир хил.

Мобил қурилмалар ва маълумотларни сақловчи ва ташувчи ташқи қурилмалардан фойдаланиш пайтида, Институт ходимлари қуйидаги талабларни бажаришлари керак:

улардан белгиланган мақсадларда ва фақат хизмат вазифаларини бажаришда фойдаланиш;

Ахборот хавфсизлиги администраторига ушбу Йўриқноманинг талаблари бузилганлиги тўғрисида хабар бериш;

Ахборот хавфсизлиги администраторига мобил қурилмалар, маълумотларни сақловчи ва ташувчи ташқи қурилмаларнинг йўқолиши (ўғирланиши) тўғрисида хабар бериш;

мобил қурилмалар, маълумотларни сақловчи ва ташувчи ташқи қурилмаларни жисмоний хавфсизлигини ҳар қандай оқилона усулда таъминлаш;

мобил қурилмалар ва маълумотларни сақловчи ва ташувчи ташқи қурилмаларни бошқа шахсларга бермаслик.

Ҳисобга олинган мобил қурилмалар, маълумотларни сақловчи ва ташувчи ташқи қурилмалар Институт ходимлари томонидан қаровсиз қолдирилиши тақиқланади.

Институтдан ташқарида (хизмат сафарлари, учрашувлар, музокаралар ва бошқалар) ишлатилганда мобил қурилмаларнинг ахборот ва жисмоний хавфсизлигини таъминлаш учун қуйидаги чоралар қўлланилиши керак:

мобил қурилмага киришда фойдаланувчи биометрик маълумотлари асосида кириш паролни ўрнатиш ёки аутентификатсия воситаларидан фойдаланиш;

мобил қурилманинг маълум дастурларига кириш учун паролни ўрнатиш;

мобил қурилмада вирусга қарши ҳимоя ва шахсий тармоқлараро экранидан фойдаланиш.

Институт ахборот инфратузилмасида фақат Институтнинг мулки бўлган ва назоратга олинадиган, рўйхатдан ўтган ахборот ташувчи воситаларидан фойдаланишга рухсат берилади.

Ахборот ташувчи воситаларни бошқариладиган ҳудуддан ташқарига олиб чиқиш Ахборот технологиялари бўлими бошлиғининг рухсати билан амалга оширилади.

Ахборот ташувчи қурилмаларини олиб чиқиш учун рухсатномада қуйидагилар кўрсатилиши керак:

тўлиқ Ф.И.О ва қурилмадан фойдаланадиган ходимнинг лавозими;

қурилманинг модели ва қайд рақами;

олиб чиқиш сабаби (хизмат сафарлар, учрашувлар, музокаралар ва бошқалар);

рухсатноманинг амал қилиш муддати.

Институт ходимларига мобил қурилмалардан фойдаланиш фақат ўз хизмат вазифаларини бажариш учун рухсат этилади.

Мобил қурилмалар Институт ходимлари ва тингловчиларига таркибий бўлинмалар раҳбарларининг ташаббуси билан қуйидаги ҳолларда берилади:

ходимнинг ёки тингловчининг ўз хизмат вазифаларини бажариш зарурати;

Институт ходими учун ишлаб чиқариш эҳтиёжининг пайдо бўлиши.

дарс жараёнларида инновацион методлардан фойдаланиши учун.

Мобил қурилмаларнинг жисмоний хавфсизлигини таъминлаш мобил қурилма фойдаланувчисига юклатилади.

Конфиденсиал маълумотларни сақлаш учун ишлатиладиган маълумотларни ташувчи, сақловчи ва мобил қурилмаларни бошқариладиган зонадан ташқарига олиб чиқишга йўл қўйилмайди.

Хизмат зарурати туфайли Институт ҳудудига мобил қурилмалар, маълумот сақловчи ва ташувчи қурилмаларни (маълумот тўплагичлар, ноутбук ва ҳ.к.) олиб кириш ёки ҳудуддан олиб чиқиш учун рухсат бериш Институт раҳбарига билдирги расмийлаштирган ҳолда амалга оширилади.

Институт ходимлари ахборот ташувчи, сақловчи ва мобил қурилмалардан фойдаланишда қуйидаги талабларга риоя қилишлари шарт:

воситалардан фақат ўзларининг иш фаолиятига оид вазифаларини бажариш учун фойдаланиши;

ахборот хавфсизлиги администраторига ушбу Йўриқнома талабларининг бузилишининг ҳар қандай фактлари тўғрисида хабар бериш;

маълумотларни ташувчи, сақловчи ва мобил қурилмаларни йўқотиш (ўғирлаш) ёки ишламай қолиш фактлари тўғрисида Ахборот хавфсизлиги администраторига хабар бериш;

ахборот ташувчи, сақловчи ва мобил қурилмаларни жисмоний хавфсизлигини барча оқилона усуллар билан таъминлаш;

ахборот ташувчи, сақловчи ва мобил қурилмаларни бошқа шахсларга бермаслик.

Ахборот ташувчи, сақловчи ва мобил қурилмаларни воситалардан фойдаланишда Институт ходимларига уларни хавфсизлигини таъминлаш чоралари кўрилмаган бўлса, уларни қаровсиз қолдириш тақиқланади.

Агар ишчи станцияни ёки серверни учинчи шахслар таъмирлашни талаб қилса, таъмирлашни бошлашдан олдин маълумотларни ташувчи, сақловчи ва мобил қурилмалар (HDD) маълумотлардан тозаланиши керак. Ушбу таъмирлаш ишлари Ахборот хавфсизлиги администратори томонидан назорат қилиниши керак.

ИНТЕРНЕТДАН ФОЙДАЛАНИШ

Қуйидаги ҳолларда интернетдан фойдаланиш тақиқланади:

интернетдан шахсий мақсадларда фойдаланиш;

ходимларга интернетга рухсатсиз уланиш имкониятини берадиган махсус жиҳоз ва дастурлардан фойдаланиш;

Институт локал тармоғи элементларининг нормал ишлашини бузишга қаратилган ҳар қандай ҳаракатларни бажариш;

конфиденциал маълумотларни шифрланмаган ҳолда узатиш;

фойдаланувчи маълумотлари ва паролларини узатиш;

ташқи прокси-серверлардан фойдаланиш;

шахсий ва конфиденциал маълумотларни юбориш учун шахсий электрон почта, ижтимоий тармоқлар ва тезкор хабар алмашиш тизимларидан фойдаланиш;

ноқонуний операцияларни амалга ошириш ва интернетда қонунга зид бўлган бошқа ҳаракатларни амалга ошириш.

Қуйидаги маълумотларни ўз ичига олган материалларни нашр этиш, юклаб олиш ва тарқатиш тақиқланади:

конфиденциал маълумотлар, шунингдек Институт ва тижорат сирини ташкил этувчи маълумотлар, агар у хизмат вазифаларига кирмаса ва узатиш усули хавфсиз бўлса, Тизим администратори, Ахборот технологиялари бўлими бошлиғи билан олдиндан келишиб олинмаган бўлса;

эгасининг рухсатсиз, тўлиқ ёки қисман муаллифлик ҳуқуқи ёки бошқа ҳуқуқлар билан ҳимояланган маълумотлар;

рухсатсиз кириш учун ҳар қандай аппарат ва дастурий таъминотни бузиш, йўқ қилиш ёки чеклаш учун мўлжалланган зарарли дастур, шунингдек тижорат дастурлари ва уларни ишлаб чиқариш учун дастурий таъминот учун серия рақамлари, пароль ва пуллик интернетга рухсатсиз кириш ҳуқуқини берадиган бошқа воситалар;

тахдид солувчи, тухмат, номаъқул маълумот, шунингдек бошқаларнинг шаъни ва қадр-қимматини камситувчи маълумотлар, этник нафратни кўзғатувчи, зўравонликни кўзғатувчи, ноқонуний хатти-ҳаракатларни содир этишга чақирувчи материаллар ва бошқалар;

ИП-манзилингизни ва бошқа хизмат маълумотларини қалбакилаштириш.

Интернетдан юклаб олинган барча файллар зарарли дастурларнинг мавжудлиги бўйича мажбурий равишда текширилиши шарт.

Қуйидагилар тақиқланади:

тармоқ юкини оширадиган ва бошқа фойдаланувчиларнинг нормал ишлашига халақит берадиган видео ва аудио оқимларнинг узатиладиган манбалардан фойдаланиш;

порнографик манбаларини, миллатчилик ташкилотлари манбаларини, зўравонлик ва терроризмни тарғиб қилувчи манбаларга кириш ва улардан фойдаланишга қаратилган ҳар қандай ҳаракат;

интернетда ноқонуний операцияларни амалга ошириш ва қонун ҳужжатларига, шунингдек ушбу қўлланмага зид бўлган бошқа ҳаракатларни бажариш.

Ахборот хавфсизлиги администратори ходимларнинг Ахборот хавфсизлиги сиёсатида зид бўлган баъзи бир интернет-ресурсларидан фойдаланишни сўров ва трафикни филтрлаш орқали чеклаш ҳуқуқига эга.

Корпоратив электрон почтадан фойдаланиш

Корпоратив электрон почта билан ишлашда фойдаланувчи электрон почта юборилган хабарни қабул қилувчига қафолатли етказиш ҳамда узатилаётган маълумотларнинг конфиденсиаллигини таъминлайдиган маълумотни узатиш воситаси ҳисобланмайди. Конфиденсиал маълумотларни узатиш фақат хавфсиз уланишлар орқали амалга оширилади.

Корпоратив электрон почта фойдаланувчиларига қуйидагилар тақиқланади:

корпоратив электрон почтадан шахсий ёзишмалар ёки шасхий тижорат мақсадларида фойдаланиш;

конфиденсиал маълумотларни шифрланмаган ҳолда юбориш;

сиёсий, диний, инсонийликка қарши характердаги, шунингдек, одобсиз, тухмат, ҳақоратли, таҳдид солувчи ёки ноқонуний материалларни корпоратив электрон почта ёки бошқа электрон воситалар орқали юбориш, сақлаш ва фойдаланиш. Шунга ўхшаш характерга эга маълумотлар пайдо бўлганда, фойдаланувчи дарҳол ўзининг бевосита раҳбарини хабардор қилиш;

реклама (соҳага оид бўлмаган) ва кўнгилочар характердаги материалларни тарқатиш;

иш фаолиятига алоқаси бўлмаган хатларнинг оммавий тарқатилишини амалга ошириш;

зарарли дастурларни ёки вирусларни юқтирган файлларни юбориш;

расмий ёзишмалар учун бепул интернет почта хизматларидан (маил.ру, яндех.ру ва бошқалар) фойдаланиш;

учинчи шахсга ва бошқа ходимларга ўз почта қутиларига кириш учун паролини бериш;

электрон почта орқали паролларни Институтнинг исталган ахборот тизимлари ва манбаларига юбориш.

Узатилган электрон почта хабари ва бошқа электрон ҳужжатларнинг мазмуни аниқ, қисқа ва тушунарли бўлиши керак.

Қуйидагилар қаттиқ тақиқланган:

ёзишмалар ва расмий маълумот алмашиш учун .UZ домен зонасидан ташқарида рухсатсиз ташқи почта хизматларидан фойдаланиш;

конфиденсиал маълумотни ҳимояланмаган шаклда электрон почта орқали юбориш.

ЖАВОБГАРЛИК

Институт барча ходимлари ва тингловчилари Ахборот хавфсизлиги сиёсатида белгиланган талаб ва мажбуриятларнинг бажарилиши учун жавобгардир.

Ушбу йўриқномада белгиланган талабларни бузиш ташкилот ички меҳнат қоидаларига шунингдек, Ўзбекистон Республикасининг меҳнат қонунчилигига мувофиқ интизомий жавобгарликка тортилиши мумкин.