



IJIRSET

International Journal of Innovative Research in
SCIENCE | ENGINEERING | TECHNOLOGY

e-ISSN: 2319-8753 | p-ISSN: 2347-6710



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

Volume 11, Issue 4, April 2022

ISSN INTERNATIONAL
STANDARD
SERIAL
NUMBER
INDIA

Impact Factor: 8.118



9940 572 462



6381 907 438



ijirset@gmail.com



www.ijirset.com

Distribution and Comprehensive Implementation of Information Security Responsibilities in Enterprises and Organizations

Turdimatov M.M.¹, Baratova G.², Ashirmatov O.M³.

Fergana branch of Tashkent University of Information Technologies named after Muhammad al-Khwarizmi.
Uzbekistan.¹²³

ABSTRACT: The article deals with the distribution of responsibilities of heads of enterprises, organizations and government agencies, including those responsible for information security, as well as a comprehensive approach to information security. The standard, which is of particular importance to the organization, and the basic rules for ensuring a protected facility and information security policy that meet its requirements are clearly outlined in its responsibilities.

The proposed measures will prevent the leakage of confidential information from public facilities and unauthorized use of that information.

KEYWORDS: information security, confidentiality, identification, protection concept, assets, liabilities, hardware, security policy, facilities, software, information processing.

КОРХОНА ВА ТАШКИЛОТЛАРДА АХБОРОТ ХАВФСИЗЛИГИНИ ТАЪМИНЛАШ МАЖБУРИЯТЛАРИНИ ТАҚСИМЛАШ ВА КОМПЛЕКС АМАЛГА ОШИРИШ

Турдиматов М.М.¹, Баратова Г.², Аширматов О.М³.

Муҳаммад аль-Хоразмийномидаги Тошкент ахборот технологиялари университети Фарғона филиали¹²³

АННОТАЦИЯ: Мақолада ахборот хавфсизлиги масалаларида корхона, ташкилот ва давлат обьектлари раҳбарлари, жумладан жавобгар шахсларни хавфсизлик сиёсати олдидағи мажбуриятларини тақсимлаш, ҳамда комплекс амалга ошириш йўллари таснифи ишлаб чиқилган. Ташиким учун алоҳида аҳамиятга эга бўлган стандарт ва унинг талабларига жавоб берувчи химоя қилинувчи объект ва ахборот хавфсизлиги сиёсатини таъминлашининг асосий қоидалари унинг вазифалари аниқ кўрсатиб берилган.

Таклиф этилган чора тадбирлар асосида давлат обьектларидан конфеденциал маълумотларни чиқиб кетиши ва у маълумотлардан руҳсатсиз фойдаланиш холатларига йўл қўйилмайди.

Калим сўзлар: ахборот хавфсизлиги, конфеденциал, идентификациялаш, химоя концепцияси, активлар, мажбуриятлар, техник восита, хавфсизлик сиёсати, объектлар, дастурий таъминот, ахборотга ишлов бериси.

Маълумки, хозирги замон талаби, жамиятни тўлиқ ахборотлашуви ва рақамли технологияларга асосланган даврида ахборот хавфсизлиги бўйича мажбуриятларнинг тақсимишини ахборот хавфсизлиги сиёсатига мувофиқ бажаришга мажбурмиз. Давлат ва жамият аҳамиятига эга бўлган маълумотларни муҳофаза қилиш ва хавфсизликнинг муайян жараёнларини бажариш бўйича мажбуриятларни аниқ белгилашимиз керак [1,2].

Хозирги кундан бошлаб хавфсизлик бўйича мажбуриятларни муайян обьектлар ва ахборотга ишлов бериси воситалари учун янада аниқроқ тавсиялар билан тўлдириш ва уларга амал қилишимиз керак. Активларни муҳофаза қилиш ва хавфсизликнинг узлуксиз ишни режалаштириш каби аниқ жараёнларини бажариш бўйича локал мажбуриятларни аниқ белгилашимиз керак.

Ахборот хавфсизлигини таъминлаш бўйича хосил бўлган муаммоларни ҳал этиш учун жавобгар ходим ўз мажбуриятларини кимгadir юклаши мумкин. Шундай бўлса ҳам, у жавобгар бўлиб қолади ва ҳар бир юкланган топширикнинг тўғри бажарилишини таъминлашга мажбур. Шунинг учун ахборот хавфсизлигини таъминлаш бўйича барча мажбуриятларни аниқ белгилаб қўйишимиз зарур[3,7].

Ташкилот ва корхоналарда ҳар бир ходим жавобгар бўлган соҳаларни аниқ билиши керак, хусусан қуидаги тадбирларни амалга ошириши зарур:

- а) хавфсизликнинг ҳар бир алоҳида тизим билан боғлиқ активлари ва жараёнларини аниқлаш ва аниқ белгилаш керак;
- б) хавфсизликнинг ҳар бир актив ва жараёни учун жавобгарни тайинлаш, шунингдек, ушбу мажбуриятларни хужжатлаштириш керак;
- с) ваколатлар даражасини аниқ белгилаш ва жавобгарлик чегараларини аниқ хужжатлаштириши лозим.

Кўпинчакорхона ва ташкилотларда ташкилот раҳбарлари ўзининг аъзоларидан бирини ахборот хавфсизлиги билан боғлиқ барча масалаларга жавобгар этиб тайинлади. Лекин, активларни қидириш ва бошқариш воситаларини жорий этиш учун жавобгарлик кўпинча алоҳида(аслида) раҳбарлар зиммасида қолади. Ҳар бир активга унинг кундалик муҳофазаси учун жавобгар бўлиб қоладиган эгасини тайинлаш кенг тарқалган тажрибага айланмоқда, бу эса яхши натижага бермайди.

Ахборот турли шаклларда мавжуд бўлиши мумкин, яъни у қоғоз ташувчида жойлаштирилган бўлиши, электрон қўринишида сақланиши, почта орқали ёки телекоммуникацияларнинг электрон воситаларидан фойдаланиб узатилиши, плёнкадан намойиш қилиниши ёки оғзаки ифодаланиши мумкин. Ахборот мавжудлигининг шаклидан, уни тарқатиш ёки сақлаш усулидан қатъий назар у доим адекват муҳофазаланган бўлиши керак.

Ахборот хавфсизлиги-бу ахборотни бизнеснинг узлуксизлигини таъминлаш, бизнес хавфларини минимумга келтириш ва инвестицияларни қайтаришни ҳамда бизнес имкониятларини максимал ошириш масқсадида таҳдидларнинг кенг спектридан муҳофазаси қилиш демакдир.

Ахборот хавфсизлигига дастурий таъминотнинг сиёсатлари, методлари, процедуранлари, ташкилий тузилмалари ва дастурий таъминот функциялари томонидан тақдим этилиши мумкин бўлган ахборот хавфсизлигини бошқариш бўйича тадбирларнинг тегишли комплексини амалга ошириш йўли билан эришилади. Кўрсатилган тадбирлар ташкилотнинг ахборот хавфсизлиги мақсадларига эришишини таъминлаши керак.

Ахборот хавфсизлигининг рискларини баҳолаш учун унга қўйилган талаблар хавфларини мунтазам баҳолаш ёрдамида аниқланади. Ахборот хавфсизлигини бошқариш бўйича тадбирларга кетган сарф-харажатлар ахборот хавфсизлигининг бузилиши натижасида ташкилотга етказилиши мумкин бўлган зарар микдорига пропорционал бўлиши керак[4].

Кўп холатларда баҳолашнинг натижалари ахборот хавфсизлиги билан боғлиқ хавфларни бошқариш соҳасида аниқ чоралар ва устуворликларни белгилашга, шунингдек, ушбу хавфларни минимумга келтириш мақсадида ахборот хавфсизлигини бошқариш бўйича тадбирларни жорий қилишга ёрдам беради. Мавжуд тадбирларнинг самарадорлилигига таъсир кўрсатиши мумкин бўлган ҳар қандай ўзгаришларни ҳисобга олиш учун хавфлар таҳлилини вақти-вақти билан тақрорлаб туриш керак.

Ахборот хавфсизлигининг сиёсати ва мақсади-қонун хужжатлари, бизнес ва раҳбарий хужжатлар талабларига мувофиқ ахборот хавфсизлигини бошқариш ва сақлаб туриш масалаларининг ҳал қилинишини таъминлаш.

Ҳар бир раҳбар сиёсатнинг аниқ йўналишини бизнес мақсадларига мувофиқ белгилаши, ахборот хавфсизлигини сақлаб туриши, бутун ташкилот бўйича ахборот хавфсизлиги сиёсатини ишлаб чиқиши ва амалга ошириш йўли билан унга таалукли мажбуриятларга риоя қилиши керак.

Хавфсизлик сиёсати, уни ташкил этишнинг, ҳамда ташкилот учун алоҳида аҳамиятга эга стандарт ва талабларга жавоб берининг кисқача мазмунини кўрсатиб ўтамиш:

- хавфсизлик сиёсатининг маҳаллий ва халқаро меъёрларга зид эмасми?
- хавфсизлик масалалари бўйича ходимларни ўқитиш ва малакасини ошириш бўйича талабларга амал киласизми?
- вирус ва бошқа зааркунанда дастурларни аниқлаш ва йўқотиш бўйича чора тадбирлар ишлаб чиқилганми?
- ахборот хавфсизлигини ва ташкилот фаолиятини узлуксиз ишлашини таъминлаш бўйича талабларишлаб чиқилганми?
- хавфсизлик сиёсатини бузганлик бўйича жавобгарлик сиёсати юргизилганми?
- раҳбарларнинг лавозим мажбуриятномаларига қўшимчалар — ахборот хавфсизлигини таъминлаш бўйича жавобгарлик ҳамда юзага келган қоидабузарликни ўз вақтида маълум қилиш бўйича жавобгарлик

ишлиари йўлга қўйилганми?

• масъул шахслар томонидан ахборот хавфсизлиги бўйича жавобгарликнинг тақсимланиши хужжатлаштирилганми?

Ахборот хавфсизлигининг сиёсатини ишлаб чиқишида, аввало химоя килинувчи обьект ва унинг вазифалари аниқланиши керак. Сўнгра душманнинг бу обьектга қизиқиши даражаси, хужумнинг эҳтимолли турлари ва кўриладиган зарап баҳоланади. Нихоят, мавжуд карши таъсир воситалари етарли химояни таъминламайдиган обьектнинг зайнф жойлари аниқланади.

Самарали химоя учун хар бир обьект мумкин бўлган таҳдидлар ва хужум турлари, маҳсус инструментлар, куроллар ва портловчи моддалар- нинг ишлатилиши эҳтимоллиги нуқтаи назаридан баҳоланиши зарур. Таъкидлаш лозимки, нияти бузук одам учун энг қимматли обьект унинг эътиборини тортади ва эҳтимолли нишон бўлиб хизмат қиласи ва унга қарши асосий кучлар ишлатилади. Бунда, хавфсизлик сиёсатининг ишлаб чиқилишида очими берилган обьектнинг реал химоясини таъминловчи ма-салалар хисобга олиниши лозим.

Хар доим қарши таъсир воситалари химоянинг тўлиқ ва эшелонланган концепциясиға мос келиши шарт. Бу дегани, қарши таъсир воситаларини марказида химояланувчи обьект бўлган концентрик доираларда жойлаштириш лозим. Бу холда душманнинг исталган обьектга химоянинг эшелонланган тизимини кесиб ўтади. Мудофаанинг хар бир чегараси шундай ташкил қилинади, кўриқлаш ходимининг жавоб чораларини кўришига етарлича вақт мобайнида хужумчини ушлаб туриш имкони бўлсин.

Сўнгги босқичда қарши таъсир воситалари қабул қилинган химоя концепциясиға биноан бирлаштирилади. Бутун тизим хаёти циклининг бошлангич ва кутилувчи умумий нархини дастлабки баҳолаш амалга

оширилади. Агар бир бинонинг ичидаги турли химоялаш талабларига эга бўлган обьектлар жойлашган бўлса, бино отсекларга бўлинади. Шу тариқа умумий назоратланувчи макон ичидаги ички периметрлар ажратилади ва рухсатсиз фойдаланишдан ички химоя воситалари яратилади. Периметр, одатда, физик тўсиқлар орқали аниқланиб, бу тусиқлардан ўтиш электрон усул ёки кўриқлаш ходимлари томонидан бажарилувчи маҳсус муолажалар ёрдамида назоратланади.

Умумий чегарага ёки периметрга эга бўлган бинолар гурухини химоялашда нафақат алохида обьект ёки бино, балки унинг жойланishi жойи хам хисобга олиниши зарур. Кўп сонли бинолари бўлган ер участкалари хавфсизликни таъминлаш бўйича умумий ёки қисман мос келадиган талабларга эга бўлади, баъзи участкалар эса периметр бўйича тўсиқка ва ягона йўлакка эга. Умумий периметр ташкил этиб, хар бир бинодаги химоя воситаларини камайтириш ва уларни фақат хужум қилиниши эҳтимоли кўпроқбўлган мухим обьектларга ўрнатиш мумкин. Худди шу тариқа участкадаги хар бир иморат ёки обьект хужумчини ушлаб қолиш имконияти нуқтаи назаридан баҳоланади.

Юқоридаги келтирилган талаблар таҳдиди кўрсатади, уларнинг барчаси ахборотни ишлаш ва узатиш курилмаларидан хукуқсиз фойдаланиш, ахборот элтувчиларини ўғирлаш ва саботаж имкониятини йўл қўймасликка олиб келади.

Корхоналарда бинолар, иморатлар ва ахборот воситаларининг хавфсизлик тизимини назорат пунктларини бир зонадан иккинчи зонага ўтиш йўлида жойлаштирган холда концентрик ҳалқа кўринишида ташкил этиш максадига мувофиқхисобланади.

Компьютер тармоғи(КТ) хавфсизлигининг ташки зонаси таъминланиши: - физик тўсишлар периметр бўйлаб ўтиш жойлари худудга кириш назоратининг ноавтоматик тизими зонаси. КТ хавфсизлигининг ўртадаги зонаси. Таъминланиши: - эшиклари электрон химояланган назорат пунктлари видеокузатиш бўш зоналарни чиқариб ташлашзонаси. КТ хавфсизлигининг ички зонаси. Таъминлаш: - шахсий компьютерга фойдаланиш фақат назорат тизими орқали идентификациялашнинг биометрик тизими. Ахборот хизмати бинолари ва хоналарига киришнинг назорати масаласига келсақ, асосий чора-нафақат бино ва хоналарни, балки воситалар комплексини, уларнинг функционал вазифалари бўйича ажратиш ва изоляциялаш. Бино ва хоналарга киришни назоратловчи автоматик ва ноавтоматик тизимлар ишлатилади. Назорат тизими кундузи ва кечаси кузатиш воситалари билан тўлдирилиши мумкин.

Хавфсизликнинг физик воситаларини танлаш химояланувчи обьект- нинг мухимлигини, воситаларга кетадиган харажатни ва назорат тизими ишончлилиги даражасини, ижтимоий жихатларни ва инсон нафси бузуқлигини олдиндан ўрганишга асосланади. Бармоқ, кафтлар, кўз тўр пардаси, қон томирлари излари ёки нуткни аниқлаш каби биометрик ин- дентификациялаш ишлатилиши мумкин. Шартнома асосида техник восита- ларга хизмат кўрсатувчи ходимларни обьектга киритишнинг маҳсус режими кўзда тутилган. Бу шахслар идентификацияланганларидан сўнг обьектга ку- затувчи хамроҳлигида киритилади. Ундан ташқари уларга аниқ келиш ре-жими, маконий чегараланиш, келиб-кетиш вақти, бажарадиган иш характеристи ўрнатилади.

Нихоят, бино периметри буйича бостириб киришни аникловчи турли датчиклар ёрдамида комплекс кузатиш ўрнатилади. Бу датчиклар объектни кўриқлашнинг марказий пости билан боғланган ва бўлиши мумкин бўлган бостириб кириш нұкталарини, айниқса ишламайдиган вақтларда, назорат қиласди.

Хар доим вақти-вақти билан эшиклар, ромлар, том, вентиляция туйнуклари ва бошқа чикиш йўлларининг физик химояланиш ишончлилигини текшириб туриш лозим.

Хар бир хонага ичидаги нарсанинг муҳимлилигига боғлиқ фойдаланиш тизимиға эга бўлган зона сифатида қаралади. Кириш-чиқиши хуқуқи тизими шахс ёки объект муҳимлигига боғлиқ холда селекцияли ва даражалари бўйича тоифалangan бўлиши шарт. Кириш-чиқиши хуқуқи тизими марказлашган бўлиши мумкин (руҳсатларни бошқариш, жадвал ва календарь режаларининг режалаштирилиши, кириш-чиқиши хуқуқининг ёзма намуна-лари ва х.о.).

Назорат тизимини вақти-вақти билан текшириб туриш ва уни доимо ишга лаёқатли холда сақлаш лозим. Буни ихтисослашган бўлинмалар ва назорат органлари таъминлайди.

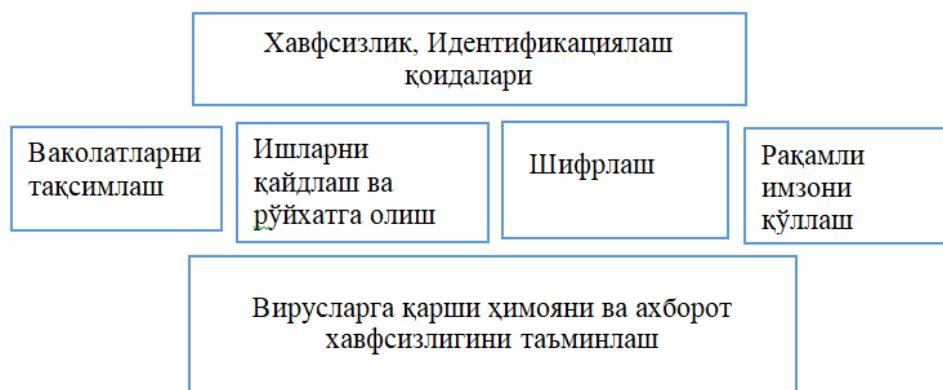
Шахсий компьютер ва физиковий химоя воситалари каби ўлчамлари кичик асбоб-ускуналарни кўзда тутиш мумкин. Юкорида келтирилганларга хуроса қилиб, компьютер тармоқларини химоялашда ахборот хавфсизлиги сиёсати қандай аниқланиши хусусида сўз юритамиз. Одатда кўп сонли фойдаланувчиларга эга бўлган корпоратив компьютер тармоқлари учун маҳсус "Хавфсизлик сиёсати" деб аталувчи, тармоқда ишлашни маълум тартиб ва коидаларга бўйсингидирувчи (регламентловчи) хужжат тузилади.

Сиёсат одатда икки қисмдан иборат бўлади: умумий принциплар ва ишлашнинг муайян қоидалари. Умумий принциплар Internetхавфсизликка ёндашиши аниқласа, қоидалар нима рухсат этилишини ва нима рухсат этилмаслигини белгилайди. Қоидалар муайян муолажалар ва турли қўлланмалар билан тўлдирилиши мумкин.

Одатда хавфсизлик сиёсати тармок асосий сервисларидан(электрон почта, WWWва х.о.) фойдаланишни регламентлайди хамда тармоқдан фойдаланувчиларни улар қандай фойдаланиш хуқуқига эга эканликлари билан таништиради. Бу эса ўз навбатида фойдаланувчиларни аутентификациялаш мулажасини аниқлади[6].

Бу хужжатга жиддий ёндашиш лозим. Химоянинг бошқа барча стра-тегияси хавфсизлик сиёсатининг қатъий бажарилиши таъминига асосланган. Хавфсизлик сиёсати фойдаланувчилар томонидан кўпгина маломат ортти-рилишига сабаб бўлади, чунки унда фойдаланувчига маън этилган нарсалар очик-оидин ёзилган. Аммо хавфсизлик сиёсати расмий хужжат, у бир то-мондан Internetтақдим этувчи сервисларда ишлаш зарурияти, иккинчи то-мондан мос мутахассис-профессионаллар тарафидан ифодаланган хавфсизлик талаблари асосида тузилади.

Автоматлаштирилган комплекс химояланган хисобланади, қачонки барча амаллар обьектлар, ресурслар ва муолажаларни бевосита химоясини таъминловчи қатъий аниқланган қоидалар бўйича бажарилса[5,6].



Aхборот хавфсизлиги сиёсатини таъминлашнинг асосий қоидалари.

Химояга қўйиладиган талабларнинг асосини таҳдидлар рўйхати ташкил этади. Бундай талаблар ўз навбатида химоянинг зарурий вазифалари ва химоя воситаларини аниқлади.

Демак, компьютер тармоғида ахборотни самарали химоясини таъминлаш учун химоя тизимини лойихалаш ва амалга ошириш уч босқичда амалга оширилиши керак.

- хавф-хатарни таҳлиллаш;
- хавфсизлик сиёсатини амалга ошириш;

- хавфсизлик сиёсатини мададлаш.

Биринчи босқичда компьютер тармоғининг заиф элементлари таҳлил-ланади, таҳдидлар аниқланади ва баҳоланади, ҳимоянинг оптималь воситалари танланади. Хавф-хатарни таҳлиллаш хавфсизлик сиёсатини қабул қилиш билан тугалланади.

Иккинчи босқич - хавфсизлик сиёсатини амалга ошириш молиявий харажатларни ҳисоблаш ва масалаларни ечиш учун мос воситаларни танлаш билан бошланади. Бунда танланган воситалар ишлашининг ихтилоғли эмаслиги, воситаларни етказиб берувчиларнинг обрўси, ҳимоя механизмлари ва бериладиган кафолатлар хусусидаги тўла ахборот олиш имконияти каби омиллар хисобга олиниши зарур. Ундан ташқари, ахборот хавфсизлиги бўйича асосий қоидалар акс эттирилган принциплар хисобга олиниши керак.

Учинчи босқич - хавфсизлик сиёсатини мададлаш босқичи энг муҳим ҳисобланади. Бу босқичда ўтказиладиган тадбирлар нияти бузук одамларнинг тармоққа бостириб киришини доимо назорат қилиб туришни, ахборот объектини ҳимоялаш тизимидағи "раҳна"ларни аниқлашни, конфиденциал маълумотлардан рухсатсиз фойдаланиш холатларини хисобга олишни талаб этади. Тармоқ хавфсизлиги сиёсатини мададлашда асосий жавобгарлик тизим маъмури бўйнида бўлади. У хавфсизликнинг муайян тизими бузилишининг барча холларига оператив муносабат билдириши, уларни таҳлиллаши ва молиявий воситаларнинг максимал тежалишини хисобга олган холда ҳимоянинг зарурий аппарат ва дастурий воситаларидан фойдаланиши шарт.

АДАБИЁТЛАР

1. O'zbekiston Davlat standarti. O'zDSt 1105:2006.
2. O'zbekiston Davlat standarti.O'z DSt 1105:2009, GOST R 28147-89.
3. Турдиматов М.М., Баратова Г. Тоифаланган ташкилотларда таҳдидларни аниқлаш ва баҳолаш. Ахборот-коммуникация технологиялари ва телекоммуникацияларнинг замонавий муаммолари ва ечимлари. Онлайн республика илмий-техник анжумани. Фаргона, ТАТУ ФФ 16-17 апрель 2021й.
4. Galatenko V.A.Axborot xavfsizligi standartlari. Internet axborot texnologiyalari universiteti. 2016 yil.
5. Instrumental boshqarish va axborotni muhofaza qilish: o'quv qo'llanma. Voronej davlat muhandislik texnologiyalari universiteti. 2013 yil.
6. Mazanik S.Kompyuter xavfsizligi: avariylar, viruslar va nosozliklardan himoya qilish. - 2014 yil.
7. Турдиматов М.М., ТиллабоевМ. Кўриқланадиганзоналардаҳавф-атарларни баҳолашвабартарафэтишусуллари. Международный журнал “Образование и наука в XXI-веке” Ноябрь, Часть 1, 138-142 стр. 2021 г.



SJIF Scientific Journal Impact Factor

Impact Factor: 8.118



INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH

IN SCIENCE | ENGINEERING | TECHNOLOGY

9940 572 462 6381 907 438 ijirset@gmail.com

www.ijirset.com



Scan to save the contact details