АХБОРОТНИ ҲИМОЯЛАШДА ЁПИҚ ВИРТУАЛ ҚОБИҒИНИ ЛОЙИХАЛАШНИ МАТЕМАТИК МОДЕЛИ

Турдиматов Мамиржон Мирзаевич
Муҳаммад ал-Хоразмий номидаги Тошкент ахборот технологиялари университети Фарғона филиали "Ахборот хавфсизлиги" кафедраси доценти
Мирзаев Жамшид Боймуродович
Муҳаммад ал-Хоразмий номидаги Тошкент ахборот технологиялари университети Фарғона филиали "Ахборот хавфсизлиги" кафедраси ассистенти

https://doi.org/10.5281/zenodo.7178488

Аннотация. *Ушбу мақолада автоматлаштирилган ахборот хавфсизлиги тизимининг таркиби ва қурилиш тамойиллари таҳлил қилиниб, уни четлаб ўтишнинг мумкин бўлган эхтимоллик холатлари математик усуллар билан асосланди, натижада ахборотни ҳимоя қилишнинг ёпиқ виртуал қобиғи яратилди. Математик ёндашув асосида тизимнинг ишламай қолиш(носозлик) вақти тасодифий ўзгарувчи сифатида кўриб чиқилди.*

Калит сўзлар: *ахборот, хавфсизлик, тизим, эхтимоллик, виртуал, носозлик, тасодифий, химоя, лойихалаш, модель.*

МАТЕМАТИЧЕСКАЯ МОДЕЛЬ ПРОЕКТИРОВАНИЯ ЗАМКНУТОЙ ВИРТУАЛЬНОЙ ОБОЛОЧКИ ДЛЯ ЗАЩИТЫ ИНФОРМАЦИИ

Аннотация. *В данной статье были проанализированы структура и принципы построения автоматизированной системы защиты информации, математическими методами обоснованы возможные ситуации ее обхода, в результате создана замкнутая виртуальная оболочка защиты информации. На основе математического подхода время отказов системы рассматривалось как случайная величина.*

Ключевые слова: *информация, безопасность, система, вероятность, виртуальный, отказ, случайный, защита, конструкция, модель.*

MATHEMATICAL MODEL FOR DESIGNING A CLOSED VIRTUAL SHELL FOR INFORMATION PROTECTION

Abstract. *In this article, the structure and principles of building an automated information security system were analyzed, possible situations of bypassing it were substantiated by mathematical methods, as a result, a closed virtual information security shell was created. Based on the mathematical approach, the system failure time was considered as a random variable.*

Keywords: *information, security, system, probability, virtual, failure, random, protection, construction, model.*

КИРИШ

Маълумки ахборот хавфсизлигининг амалий муаммоларини ҳал қилишда унинг заифлигини миқдорий баҳолаш катта аҳамиятга эга. Шунинг учун ахборот хавфсизлиги соҳасидаги бир қатор мутахассислар тасодифий ва қасддан таҳдидлардан ҳимоя қилиш усуллари ва воситаларини такомиллаштириш билан шуғулланиб келмоқдалар. Тасодифий таҳдидлардан ҳимоя қилиш учун автоматлаштирилган тизимлар(АТ) ишлашининг ишончлилигини ошириш воситалари, маълумотларнинг ишончлилиги ва заҳиравий нусхасини ошириш воситалари қўлланилади. Қасддан таҳдидлардан ҳимояланишни лойиҳалашда рўйхат ва тасниф маълум бир АТда ҳимоя қилиниши керак бўлган маълумотларнинг табиати, жойлашуви, аҳамияти ва амал қилиш муддати билан

белгиланади. Ушбу маълумотларнинг табиати ва аҳамиятига кўра, потенциал босқинчининг кутилаётган даражаси ва хатти-ҳаракати танланади. Таҳдид ахборотга рухсатсиз кириш орқали амалга оширилади, деб ишонилади.

ТАДҚИҚОТ МАТЕРИАЛЛАРИ ВА МЕТОДОЛОГИЯСИ

Тадқиқот натижаларига кўра тизимда бузғунчи моделига мувофиқ, ҳимояланган маълумотларга рухсатсиз киришнинг мумкин бўлган каналларининг турларини ва уларни миқдорини аниқлаш асосий параметрлардан хисобланади. Айнан шу каналлар техник жиҳатдан бошқариладиган ва бошқарилмайдиганларга бўлинади. Масалан, терминал клавиатурасидан тизимга кириш махсус дастур орқали бошқарилиши мумкин, лекин географик жиҳатдан тақсимланган тизимнинг алоқа каналлари ҳар доим ҳам бошқарилмайди. Каналларни таҳлил қилиш асосида ушбу каналларни блокировка қилиш учун тайёр ёки янги ҳимоя воситалари танланади.

Ягона доимий ҳимоя механизмини яратиш учун махсус ажратилган марказлаштирилган бошқарув воситалари ёрдамида ҳимоя воситалари ягона автоматлаштирилган ахборот хавфсизлиги тизимига бирлаштирилиб, унинг таркиби ва қурилиш тамойилларини таҳлил қилиб, уни четлаб ўтишнинг мумкин бўлган усуллари текширилади. Натижада ахборотни ҳимоя қилишнинг ёпиқ виртуал қобиғи қурилади.

Ҳимоя даражаси ахборотнинг оқиб чиқиши каналларининг тўлиқ қопланиши ва ҳимоя воситаларини четлаб ўтишнинг мумкин бўлган усуллари, шунингдек, ҳимоянинг мустаҳкамлиги билан белгиланади. Бузғунчининг хатти-ҳаракатларининг қабул қилинган моделига кўра, ҳимоя қилишнинг мустаҳкамлиги ушбу қобиқни ташкил этувчи воситалар кучининг энг паст қиймати билан ҳимоя воситалари билан белгиланади.

Ҳимоя кучи(тўсиқ) деганда тажовузкор томонидан уни енгиб ўтмаслик эҳтимоли катталиги тушунилади. Агар бузғунчи томонидан уни енгиб ўтиш учун кутилган вақт ҳимояланган объектнинг ишлаш муддатидан ёки ушбу тўсиқни четлаб ўтиш йўллари бўлмаса, киришни аниқлаш ва блокировка қилиш вақтидан узоқроқ бўлса, ҳимоя тўсиғининг мустаҳкамлиги етарли деб хисобланади.

Ҳимоя қобиғи бир хил принцип бўйича қурилган (назорат қилиш ёки олдини олиш) каналларига жойлаштирилган ҳимоя воситаларидан иборат бўлиши керак. Бошқариладиган каналларда бузғунчи қўлга тушиш хавфини туғдиради ва назоратсиз каналларда у вақт ва пул билан чекланмаган қулай шароитларда ишлаши мумкин. Иккинчи ҳолатда ҳимоя кучи анча юқори бўлиши керак. Шунинг учун, автоматлаштирилган тизимда алоҳида виртуал ҳимоя қобиқларига эга бўлиш тавсия этилади. Бундан ташқари, биргаликда ўзларининг ҳимоя қобиғини яратиши мумкин бўлган ташкилий чора-тадбирлардан фойдаланишни ҳисобга олиш керак.

ТАДҚИҚОТ НАТИЖАЛАРИ

Олинган натижаларга асосан таҳдидлар рўйхатини аниқлаш ва бузғунчи моделини яратиш ҳимоя тизимини лойиҳалашда мажбурий қадам хисобланади. Ҳар бир тизим учун хавфсизликка эҳтимолий таҳдидлар рўйхати, шунингдек, эҳтимолий босқинчининг хусусиятлари индивидуалдир. Шунинг учун рўйхат ва модел норасмий бўлиши керак. Ахборот хавфсизлиги тахмин қилинаётган таҳдидлар ва тажовузкорнинг сифатлари ҳақиқий вазиятга мос келган тақдирдагина таъминланади. Тизимда заифлик мавжуд бўлса, потенциал хавфсизлик таҳдиди ҳужум шаклида амалга оширилиши мумкин.

Ҳужумлар одатда мақсадлар, мотивлар, фойдаланилган механизм, тизим архитектурасидаги ўрни ва тажовузкорнинг жойлашувига қараб таснифланади. Муваффақиятли ҳужумларнинг олдини олиш учун тизимнинг заиф томонларини қидириш

ва таҳлил қилиш керак. Заифликлар пайдо бўлиш манбасига, хавф даражасига, тарқалиш даражасига, АТ ҳимояси қуйи тизимлари билан боғлиқлигига қараб фарқланади. Заифликни таҳлил қилиш - ахборотлаштириш объектини сертификатлашнинг мажбурий тартиби. Янги заифликлар пайдо бўлиши эҳтимоли туфайли уларни аллақачон сертификатланган объектда даврий таҳлил қилиш талаб қилинади.

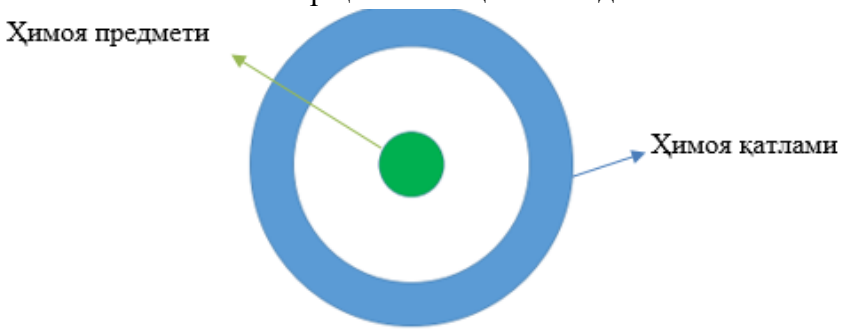
Назорат қилиш ва блокировка қилиш воситалари рухсатсиз киришнинг мумкин бўлган каналларида, техник ёки ташкилий жиҳатдан мумкин бўлган жойларда ўрнатилади ва бундай имкониятлар мавжуд бўлмаганда огоҳлантириш воситалари (профилактика воситалари) қўлланилади.

Ҳимоя ускунасининг кучини ҳисоблашда вақт омили ҳисобга олинади, бу унинг кучининг миқдорий баҳосини олиш имконини беради - потенциал бузувчи томонидан уни енгиб ўтмаслик эҳтимолининг кутилган қиймати.

Энг оддий ҳолатда ҳимоя объекти ёпиқ бир хил ҳимоя қобиғига жойлаштирилади (1-расм).

1-Расм.

Бир қатламли ҳимоя модели.



Ҳимоянинг мустаҳкамлиги тўсиқнинг хусусиятларига боғлиқ. Яратилган тўсиқнинг кучи, агар потенциал тажовузкор томонидан уни енгиб ўтиш учун кутилаётган харажатларнинг қиймати ҳимояланган маълумотларнинг нархидан ошса, етарли деб ҳисобланади.

Агар биз бузғунчи томонидан тўсиқни енгиб ўтмаслик эҳтимолини **P0**, бузғунчи томонидан тўсиқни енгиб ўтиш эҳтимолини **P1** орқали белгиласак, эҳтимоллик назариясига кўра[1]

P0 + P1= 1.

Ҳақиқий ҳолатда, тўсиқни айланиб ўтиш йўллари бўлиши мумкин. Босқинчи томонидан тўсиқни четлаб ўтиш эҳтимолини **P2** деб белгилаймиз. Бузғинчи ёлғиз ҳаракат қилиб, йўллардан бирини танлайди, яъни тўсиқни енгиб ўтиш ёки вақтинчалик ечим излаш. Демак, ҳодисаларнинг мос келмаслигини ҳисобга олган ҳолда, тўсиқнинг кучини расман қуйидагича ифодалашимиз мумкин

P0 = min{(1 –P1) , (1 – P2)}.

Бузғунчи тўсиқни енгиб ўтиш эҳтимоли юқори бўлган йўлни аниқлаш ва танланган энг хавфли вазиятни кўриб чиқиш лозим. Бундай ҳолда, тўсиқнинг мустаҳкамлиги ушбу эҳтимолликнинг энг юқори қийматига эга бўлган йўл бўйлаб потенциал босқинчи томонидан уни енгиб ўтиш ёки четлаб ўтиш эҳтимоли билан белгиланади деб тахмин қилиш мумкин. Яъни, битта қоидабузарнинг ҳаракатларида ҳимоянинг мустаҳкамлиги унинг энг заиф бўғини билан белгиланади.

Тўсиқнинг атрофида бир неча йўл бўлиши мумкин. Шунинг учун қуйидаги эхтимолий хулосаларни ифодалаймиз

P0 = min{(1 – P1), (1 –P01), (1 – P02), (1 – P03), ... (1 – P0k)},

бу ерда **k** - айланма йўллар сони.

Агар бир нечта қоидабузар бўлса ва улар бир вақтнинг ўзида (уюшган гуруҳ) ҳар бир йўлда ҳаракат қилса, ҳаракатларнинг мувофиқлигини ҳисобга олган ҳолда уни қуйидагича ифодалаш мумкин:

P0= (1 – P1) · (1 – P01) · (1 – P02) · (1 – P03) ... (1 – P0k),

ушбу формула назоратсиз тўсиқ учун амал қилади.

Келинг, назорат қилинадиган тўсиқ учун нисбатларни ҳисоблаш хусусиятларини кўриб чиқайлик. Доимий қийматга эга бўлган ҳимоя объектига киришни бошқаришни таъминлаш зарур ва техник жиҳатдан мумкин бўлганда, одатда, тажовузкорнинг ҳимоя объектига ёки объектига киришини аниқлаш ва блокировка қилиш хусусиятларига эга бўлган доимий тўсиқ қўлланилади.

Агар сегментнинг назорат пулсига урилиш эҳтимолини, яъни хавфни аниқлаш ва блокировкаланиш эҳтимолини $P_{бэ}$ деб белгиласак, у ҳолда

$P_{бэ}$= $T_{бв}$/($T_{бў}$+ $T_{ув}$),

бу ерда $T_{ув}$ –хавф сигналини узатиш вақти, $T_{бў}$ – блокировкага ўтиш вакти; $T_{бв}$ – бузилган вақт.

Рухсатсиз киришни аниқлаш ва блокировка қилишнинг автоматлаштирилган тизими кўринишидаги тўсиқнинг кучини янада тўлиқроқ расмий равишда тақдим этиш учун унинг ишлашининг ишончлилигини ва тажовузкор уни четлаб ўтиши мумкин бўлган усулларни ҳисобга олиш керак[2].

Тизимнинг ишдан чиқиши эҳтимоли[1] формула билан аниқланади

$P_{ич}(t) = e^{-t\lambda}$,

бу ерда **λ** - хавфни аниқлаш ва блокировка қилиш тизимини ташкил этувчи техник воситалар гуруҳининг ишдан чиқиш даражаси;

t - хавфни аниқлаш ва блокировка қилиш тизимининг ишлаши учун кўриб чиқилган вақт оралиғи.

Энг хавфли вазиятларни хисобга олиб - биз назорат қилиш тизими ва унинг ишдан чиқиши қўшма ҳодисалар бўлиши мумкинлигига асосланамиз. Шунинг учун, ушбу вазиятни ҳисобга олган ҳолда, бошқариладиган тўсиқнинг мустаҳкамлиги формуласи қуйидагича бўлади

Pн =min{ P (1 – $P_{ич}$), (1 - Po1), (1 - Po2), (1 - Po3), ... (1 - Pok)},

бу ерда **k** айланма йўллар сони.

Хавфли вазиятларни назорат қилиш ва блокировка қилиш учун муайян тизимни қуриш тамойилларини таҳлил қилиш мутахассис томонидан белгиланади.

Вақт ўтиши билан маълумотларнинг қиймати пасайган тақдирда, ҳимоянинг етарлилик шарти маълумотларнинг амал қилиш муддати давомида тажовузкор томонидан тўсиқни енгиб ўтиш учун сарфланган вақтдан ошиб кетиши сифатида қабул қилиниши мумкин. Бундай ҳимоя сифатида ахборотнинг криптографик трансформациясидан фойдаланиш мумкин. Криптографик тўсиқни четлаб ўтишнинг мумкин бўлган усуллари шифрланган хабарнинг асл матнини криптотаҳлил қилиш ёки сақлаш ва узатиш пайтида шифрлаш калитларининг ҳақиқий қийматларига эга бўлиши мумкин.

Назорат қилинмаган ва бошқариладиган тўсиқлар учун охирги ҳимоя кучларини ҳисоблаш алоҳида бўлиши керак, чунки улар учун дастлабки маълумотлар ҳар хил ва шунинг учун турли вазифалар учун турли хил эчимлар бўлиши керак - бир хил даражадаги икки хил ҳимоя қобиғи.

Агар ҳимоянинг энг заиф бўғинининг мустаҳкамлиги умуман ҳимоя қобиғининг талабларига жавоб берса, ушбу қобиқнинг қолган бўғинларида кучнинг ортиқчалиги ҳақида савол туғилади. Бундан келиб чиқадики, кўп бўғинли ҳимоя қобиғида тенг қувватли тўсиқлардан фойдаланиш иқтисодий жиҳатдан мақсадга мувофиқдир.

Ҳимоя воситаси талабларга жавоб бермаса, бу звенодаги тўсиқ кучлироғи билан алмаштирилиши керак ёки бу тўсиқ яна битта, баъзан эса икки ёки ундан ортиқ тўсиқлар билан такрорланади. Қўшимча тўсиқлар биринчиси каби бир хил ёки ундан кўп бўлган алоқа каналларини қамраб олиши керак.

Ресурсларни аниқлаш ва баҳолашнинг иккинчи босқичида-"Активларни идентификациялаш ва баҳолаш"да активлар аниқланади. Ахборот активларининг таннархини ҳисоблаш сизга таклиф қилинаётган назорат ва ҳимоя воситаларига эҳтиёжни етарлилигини аниқлаш имконини беради.

Таҳдид ва заифликларни баҳолашнинг учинчи босқичида - "Хавф ва заифликларни баҳолаш" - ташкилотнинг ахборот активларининг таҳдидлари ва заифликлари аниқланади ва баҳоланади[2]. CRAMM усулининг тижорат версиясида бундай баҳолаш ва идентификациялаш учун қуйидаги мезонлар тўпламидан фойдаланилади (ахборот хавфсизлиги таҳдидларини амалга ошириш оқибатлари):

1 -мезон - ташкилот обрўсига путур етказиш;

2 - ресурсларни тиклаш билан боғлиқ молиявий йўқотишлар;

3 - компаниянинг тартибсизлиги;

4-ахборотни ошкор қилиш ва рақобатчиларга етказишдан молиявий йўқотишлар, шунингдек бошқа мезонлар.

Хатарларни таҳлил қилишнинг тўртинчи босқичи - "Хатарларни таҳлил қилиш" сизга хавфларнинг миқдорий баҳосини олиш имконини беради. Бу тахминларни қуйидаги ифодалар ёрдамида ҳисоблаш мумкин:

$P = P_{зар} * C_{зар}$;

$P = P_{тах} * P_{заиф} * C_{зар}$, бу ерда:

P-таҳдидни амалга ошириш натижасида хавф миқдори;

$P_{зар}$-таҳдидни амалга ошириш натижасида зарар етказиш эҳтимоли;

$P_{тах}$-таҳдидни амалга ошириш эҳтимоли;

$P_{заиф}$-заифликларни амалга ошириш эҳтимоли;

$C_{зар}$-таҳдидни амалга ошириш натижасида зарар миқдори.

Агар ахборот объекти бир нечта (N) таҳдидларга дуч келса (мумкин бўлган зарарни баҳолаш мезонлари), унда ахборот объектига тажовузкорлар этказган зарарнинг умумий хавфи (умумий қиймати) қуйидагича ифодаланиши мумкин:

$$R_{Um} = \sum_{i=1}^{N} P_i * C_i ;$$

бу ерда **C_i i**-чи таҳдид учун етказилган зарар қиймати;

P_i-бу мутахассислар томонидан танланган **i**-таҳдиднинг шикастланиш эҳтимоли.

Хавфларни бошқаришнинг бешинчи босқичида- "Хавфларни бошқариш" - таваккалчиликни камайтириш ёки олдини олиш чоралари ва воситалари таклиф қилинади. Натижаларни тўғрилаш ёки бошқа баҳолаш усулларидан фойдаланиш мумкин. Натижада юзага келадиган таҳдидлар, заифликлар ва хавфлар даражаси таҳлил қилинади ва мижоз билан келишилади. Шундагина усулнинг охирги босқичига ўтиш мумкин.

МУҲОКАМА

Охирги босқичда, CRAMM аниқланган хавфлар ва уларнинг даражаларига мос келадиган қарши чоралар учун бир нечта вариантни ишлаб чиқилади. Қарши чоралар қуйидаги тоифаларга кўра гуруҳлар ва кичик гуруҳларга бўлинади[3,4]:

- тармоқ даражасида хавфсизликни таъминлаш;
- физик хавфсизликни таъминлаш;
- қўллаб -қувватловчи инфратузилма хавфсизлигини таъминлаш;
- тизим маъмури даражасида хавфсизлик чоралари.

Ишончлилик назарияси - эҳтимоллик назариясининг қўлланиладиган соҳаси бўлиб, унда тизимнинг ишламай қолиш вақти тасодифий ўзгарувчи сифатида кўриб чиқилади.

Энг муҳим кўрсаткичлардан бири бу носозликларсиз ишлаш эҳтимоли бўлиб, бу нотўғри ишлашнинг маълум бир вақт ичида содир бўлмаслиги эҳтимоли сифатида МТТФ, носозлик вақти деб аталади:

P(t) = P{МТТФ > t}.

Ҳар қандай эҳтимоллик сингари, ишламай қолиш эҳтимоли 1 дан 0 гача қийматларни олади ва у вақтнинг бошланғич моментида бирга, вақт чексизликка мойил бўлганда эса нолга тенг.

Муваффақиятсизлик эҳтимоли - бу маълум бир **t** вақт ичида, яъни носозлик юзага келиши эҳтимоли муваффақиятсизлик эҳтимоли биттага ишламай қолиши эҳтимолини тўлдиради(муваффақиятсизлик содир бўлади ёки бўлмайди, яъни бизда тўлиқ ҳодисалар гуруҳи мавжуд):

F (t) = 1 - P (t).

Ишончлилик назариясининг муҳим тахмини - бу бузилиш тезлиги вақт бўйича доимий деб қабул қилинганда, муваффақиятсизликка қадар вақтнинг экспоненсиал тақсимотидан фойдаланишдир.

Ишламай қолиш вақти МТТФ вақт ўтиши билан ишламай қолиш эҳтимоли учун нолдан чексизгача бўлган аниқ интеграл сифатида ҳисобланади.

Мавжудлик коэффициенти-объектдан белгиланган мақсадда фойдаланиш таъминланмаган режалаштирилган даврлар бундан мустасно, объектнинг ихтиёрий вақтда иш ҳолатида бўлиш эҳтимоли. Мавжудлик коэффициенти ишламай қолиш вақтига вақт йиғиндисига (МТТФ) ва муваффақиятсизликдан кейин тикланишнинг ўртача вақтига (МТТР) нисбати сифатида ҳисобланади:

A = МТТФ / (МТТФ + МТТР).

Ишончлилик ва хавфсизлик ўртасидаги боғлиқликни тушуниш учун IES 61508 да муҳокама қилинган носозликлар таснифига мурожаат қилайлик[5].

ХУЛОСА

Муваффақиятсизликлар хавфли ёки хавфсиз бўлиши мумкин, лекин ташхис қўйиш ва ишончлилик доирасида барча турдаги носозликлар ҳисобга олиниши шарт. Хавфсизлик нуқтаи назаридан- бизни фақат хавфли носозликлар қизиқтиради ва бундай носозликлар диагностика қилиниши муҳим ва агар улар аниқланса, тизим хавфсиз ҳолатга ўтиши мумкин[5].

Шундай қилиб, хавфсизлик тизимларида нафақат хавфсизлик кўрсаткичларини, балки ишончлилик кўрсаткичларини ҳам таҳлил қилиш ва мавжуд маълумотларнинг барча тўпламини ҳисобга олган ҳолда тузилмаларни танлаш керак.

REFERENCES

1. Коршунов Ю.М. Математические основы кибернетики. М., “Энергоатомиздат”, 1987 г. 496 с.
2. Turdimatov M.M., Baratova G., Ashirmatov O.M. Distribution and Comprehensive Implementation of Information Security Responsibilities in Enterprises and Organizations. International Journal of Innovative Research in Science, Engineering and Technology. Volume 11, Issue 4, April 2022.
3. Шангин В.Ф., «Комплексная защита информации в корпоративных системах», Учебное пособие. М.: ИД. «ФОРУМ» - ИНФРА М. 2019, 591с.
4. Бирюков, А.А. Информационная безопасность: защита и нападение / А.А. Бирюков. - М.: ДМК Пресс, 2013. - 474 с.
5. ISO/IEC 27002:2013, Information technology — Security Techniques — Code of practice for information security controls.