УДК 004.056

К.А.Ташев, Н.Б.Насруллаев, Ш.З.Исломов

АХБОРОТ ХАВФСИЗЛИГИ МОНИТОРИНГИ ТИЗИМЛАРИДА МАЪЛУМОТЛАРНИ ИШЛАШ

Ушбу мақолада инцидентларнинг тизимда муваффақиятли амалга ошира олишини ва ушбу инцидент билан боғлиқ критиклик даражасини аниқлашга имкон берувчи ахборот хавфсизлиги мониторинги тизимининг ахборот-коммуникация тизимлари ҳимояланганлик даражасини баҳолаш, ахборот хавфсизлиги хабарларини генерациялаш, уларни турли хил ахборотни ҳимоялаш воситаларидан йиғиш ва маълумотлар базасида сақлаш ҳамда хабарларини таҳлиллаш босқичлари келтирилган.

Калит сўзлар: мониторинг, ҳимоя, конфиденциаллик, риск, ҳужум, заифлик, протокол, фильтрлаш.

Кириш. Ахборот хавфсизлиги мониторинги тизими-(АХМТ) архитектураси турли хил блоклардан ташкил топган. Ушбу блокларнинг вазифаларидан ташқари, уларнинг ўзаро таъсир қилиш тартибини тушуниш зарур. Йиғилган маълумотларни АХМТда ишлаш жараёни 1-расмда келтирилган ва қуйидаги босқичлардан ташкил топган:

– АКТ ҳимояланганлик даражасини баҳолаш;

– АКТ хабарларини генерациялаш;

– АКТ хабарларини йиғиш ва сақлаш;

– АКТ хабарларини таҳлиллаш.

АКТ хабарларини генерациялаш, йиғиш, сақлаш ва таҳлиллашдан олдин АКТ хавфсизлигининг умумий даражасини баҳолаш зарур. Бу эса кейинчалик ҳужумнинг тизимда муваффақият-ли амалга ошира олишини ва ушбу ҳужум билан боғлиқ критиклик даражасини аниқлашга имкон беради.

АКТ хавфсизлиги даражасини баҳолаш. АКТ ҳимояланганлиги деганда унинг таркибида сақланувчи ёки ишланувчи ахборот активларига йўналтирилган АХ таҳдидларини бартараф этиш ёки уларнинг амалга оширилишини қийинлаштирувчи АКТ хусусияти тушунилади. АКТнинг ҳимояланганлик даражаси маълум вақт онида АКТ ҳимояланганлигининг нисбий характеристикасини ифодалайди.

АКТнинг ҳимояланганлик даражасини баҳолаш бир нечта омилларга боғлиқ: тизимнинг критиклик даражаси, улардаги заифликларнинг мавжудлиги, АХ хабарлари манбаларининг конфигурациялари, қурилмаларни созлаш қоидалари қисми бўйича хавфсизлик сиёсати. АКТнинг ҳимояланганлик даражасини баҳолаш натижалари "тизим мақоми" деб номланган маълумотлар банкининг махсус бўлимида сақланиши зарур.

Асосий қисм

Ушбу маълумотларни олиш учта турли усулда амалга оширилиши мумкин: "қора қути", "оқ қути" ва "кулранг қути". Биринчи вариант "қора қути" - бу АКТ структураси ҳақида маълумотга эга бўлмасдан заифликлар мавжудлигини аниқлаш мақсадида тизимни сканерлаш. Ушбу вариант кенг қўлланилади ва тезда керакли натижаларни бера-ди. Иккинчи вариант, "оқ қути", бу кўп сонли тизимларни ишлаш учун жуда ҳам мос келади ва нияти бузуққа тармоқ топологияси, дастурнинг бошланғич коди ва IP-адреслаш схемалари маълумлигини кўзда тутади [1]. "Кулранг қути" варианти қачонки тизим ҳақидаги барча зарур ахборотлар маълум, аммо ундан бево-сита фойдаланишнинг йўқлиги ҳолатида қўл келади.

Тизим критиклиги ҳужум натижасида унинг обрўсизлантирилиши ҳолатидаги зарар орқали аниқланади. Бу усул жуда субъектив, чунки зарарни баҳолаш ҳужумлар таснифи ва стандарт таксо-номия усулидан фойдаланиб амалга оширилиши лозим.

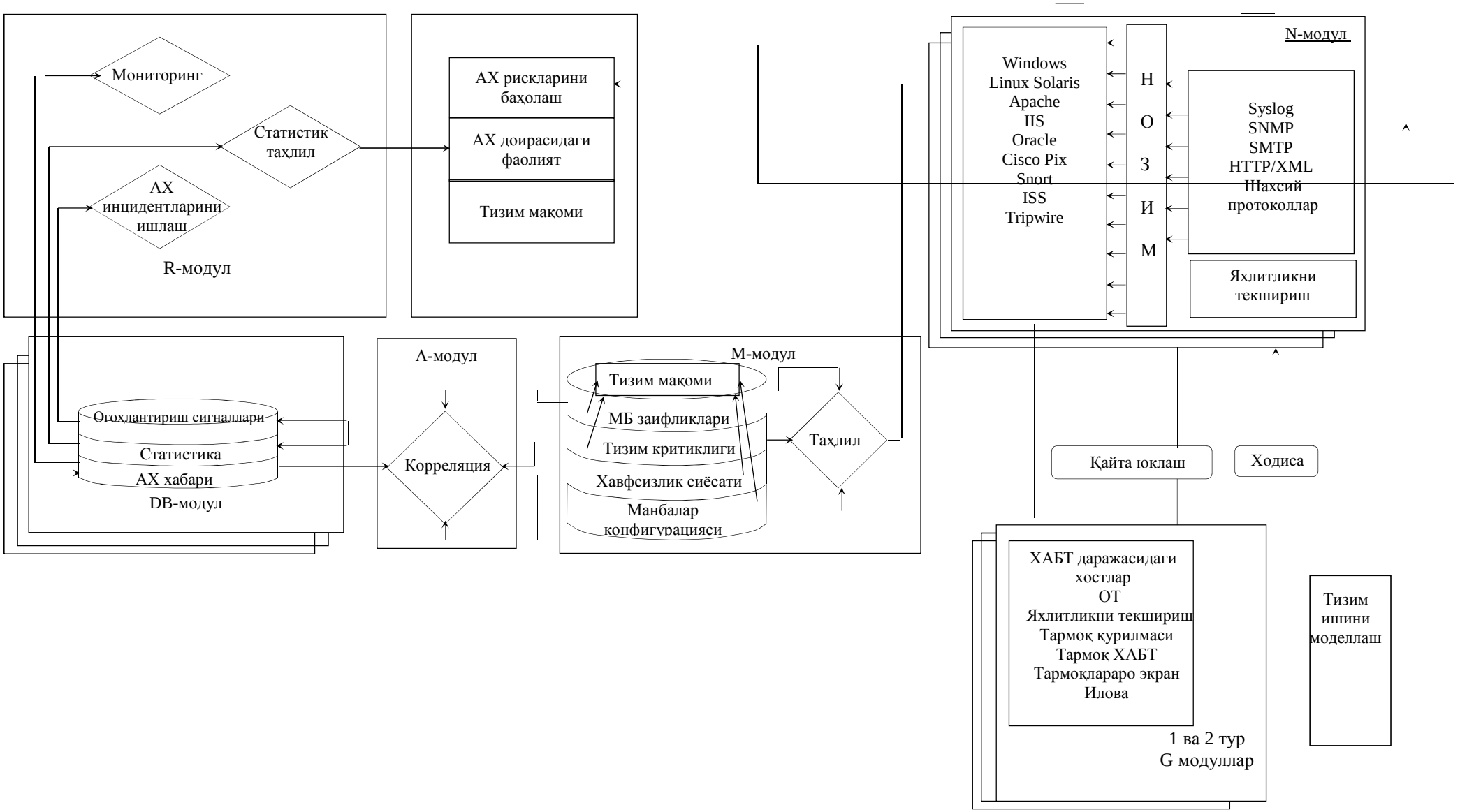
Ҳужумлар таснифини ҳужумлар рўйхати ёки ҳужумлар матрицаси ёрдамида амалга ошириш мумкин. Бу усулларнинг ҳар бири матрица ёки рўйхат элементини аниқлашни кўзда тутади. Бу айрим ҳужумлар учун мақбул таксономиянинг олти хусусиятини (кесишмаслик, тўлиқлик, аниқ-лик, натижаларни такрорланиши, мақбуллик, фойдалилик) қаноатлантирувчи тавфсифнинг мавжуд эмаслигига олиб келиши мумкин[2], бу эса ўз навбатида ҳужумнинг нотўғри таснифланишига олиб келиши мумкин. Бу ҳолда, махсус тавсифни ёки баъзи бир умумий ҳужум гуруҳини, масалан, "таснифланмаган ҳоллар" ҳужумлари гуруҳини ишлатиш мумкин[3].

Заифликлар маълумотлари базасида АХ бузилиши ҳоллари ва ҳужумни амалга ошириш учун хужумчи томонидан фойдаланиши ёки тизим хавфсизлигига таъсир ўтқазиши мумкин бўлган хавфли хатти-ҳаракатлар хусусидаги маълумотлар сақланади.

Маълумотлар базаси қуйидаги заифлик турларини ўз ичига олиши лозим:

техник заифликлар – муайян дастурий ёки аппарат таъминоти учун техник жиҳатдан ўзига хос, масалан: буферларнинг тўлиб-тошишига олиб келувчи дастур кодининг заифлиги, қаторнинг нотўғри ишланиши, «мусобақалар» ва ҳ. Маълумотлар базасининг ушбу қисми яратиш, тўлдириш ва мададлаш учун энг осон. Маълумотларнинг очиқ манбалардан кенг фойдаланувчанлиги сабабли жараёнларнинг аксарияти скриптлар ёрдамида яратилиши мумкин:

- очиқ жўнатмалар рўйхатлари, ишлаб чиқарувчилар тавсиялари ва АХ бўйича веб-сайтлар. Бироқ олинган маълумотларни (айниқса, ахборотнинг бир нечта манбаларидан фойдаланилса) валидлаш ва корреляциялаш мажбурий тартибда эксперт гуруҳ-лари томонидан амалга оширилиши лозим



1–расм. АХ мониторинги тизимида маълумотларни ишлаш

функционал заифликлар - аппарат ва дастурий таъминот созланмалари, иш вақтидаги фойдаланувчи ҳаракатига ва ҳ. боғлиқ.Ушбу заифликлар

АКТ ишлаётган муҳитга ҳам етарлича боғлиқ. Мисол учун, NF mount функцияси нияти бузуққа файл тизимини ўрнатиш ва ҳимояланган хостга кириш имконини беради. Ушбу заифликларнинг аксарияти тизимда мавжуд, аммо тегишли хизмат ўчирилганлиги сабабли улар фаол эмас. Энг қийин қисм – ушбу заифликларни формаллашган аниқлаш ва маълумотлар базасига қўшиш. Бунинг учун ҳар бир предмет соҳасига оид (операцион тизим, илова, ҳисоблаш тармоғи ва ҳ.) бир неча мутахассис ва экспертлар гуруҳининг мавжудлиги зарур. Архитектура заифликлари (топология заифликлари) – ҳисоблаш тармоғи дизайнининг ҳужумларга ва уларнинг оқибатларига таъсири билан боғлиқ. Бу заифликлар сниффинг ёки спуффинг каби ҳужумларга олиб келиши мумкин. АХМТ топологиясини моделлаш бўйича ҳеч бўлмаганда минимал имкониятларга эга бўлмай туриб, уларни маълумотлар базасига жойлаштириш мумкин эмас. Ҳимояланаётган АКТ инвентаризацияси бўйича кейинги қадам АХ хабарларининг критиклигини, жавоб реакциясини ва ҳисобот бериш зарурлигини аниқловчи АХ сиёсати қоидаларини созлашдан иборат. Хавфсизлик сиёсатининг иккита муҳим жиҳати - АХ ҳодисаларининг қонунийлигининг метрикаси ва ҳимоя объектларини тестлаш/мониторинглаш қоидалари. Ушбу икки жиҳат генерацияланган хабарларни (маъмурнинг тизимга муваффақиятли кириши, портларни сканерлаш ва ҳ.) АХМТда созланган қоидаларга мос ёки мос келмайдиганларига ажратувчи АХ мониторинги тизими мантиғини ҳосил қилади. Техник хавфсизлик сиёсатига мос эмас каби белгиланган хабарларга ҳужумнинг бир қисми каби қаралади. Хавфсизлик сиёсати қоидаларининг созланмалари маълумотлар банкида сақланади. Маълумотлар банкининг "тизим мақоми" бўлими ўзида АКТ ҳимояланганлиги даражасининг интеграллашган баҳосини сақлайди. Маълумотлар базасида сақланадиган барча маълумотлар ҳимоя объектидаги муайян заифликларнинг мавжудлигини, ҳимоя объектининг критиклик даражасини, хавфсизлик сиёсатининг созланишини ва манба конфигурацияси параметрларини инобатга олган ҳолда таҳлилланади. Таҳлиллагич ўз фаолияти натижасида “нофаол” заифликларнинг ишга тушишига олиб келувчи ҳужум шаклидаги заифликларни амалга ошишидан кўриладиган нисбий зарарни, ҳар бир ҳимоя объекти дучор бўлган заифликлар рўйхатини тақдим этади. Назоратланаётган тизимда янги заифлик топилганида ёки ўзгаришлар содир бўлганида бундай баҳолаш ишончли бўлиши учун ҳар сафар қайта генерацияланиши лозим. АХ хабарларини генерациялаш. Идеал ҳолда, G-модуллари АХ хабарларини имкон қадар кўп генерациялашга созланган бўлиши лозим. Вақтнинг реал режимида бу ахборот RMON (Remote Network Monitoring) ишлайдиган принцип бўйича ҳаракат қилиб, N-модулга юборилиши ёки N-модулларда кейинги йиғиш учун локал сақлаб қўйилиши мумкин[4]. Шу билан бирга, АХ хабарларини агрегатлаш ва корреляциялаш жараёнида кераксиз ва такрорланувчи ахборот ўчирилади. Бироқ АХ хабарлари қанча кўп генерацияланса, G-модулдан шунча кўп унумдорлик талаб қилинади. Шундай қилиб, энг яхши амалиёт унумдорлик бўйича чекловлардан қочишга имкон берувчи АХ хабарларини дастлабки фильтрлаш ҳисобланади. G - модулда фильтрлаш икки усулда амалга оширилиши мумкин: структурали спецификация – бу ҳолда ҳимояланган тизимда қатнашмайдиган компонентларга(аппаратура, операцион тизим, илова ва ҳ) тегишли бир қанча АХ хабарлари генерацияланмайди. Қоидага кўра бу тур фильтрлар суқилиб киришларни аниқлаш ва бартараф этиш тизимлари ва тармоқлараро экранларга ўрнатилади; хавфсизлик сиёсатининг дастлабки фильтрлари - бу фильтрлар, АХ хабарларини генерациялашни блокировка қилиш учун ўрнатилади, чунки улар қонуний ҳисобланади, яъни техник хавфсизлик сиёсатини қаноатлантиради. Масалан, «su» командасига сутка давомида маълум бир вақтда бажарилиши ёки аниқ ир IP-адрес орқали портларни сканерлаш учун рухсат берилган ва ҳ.

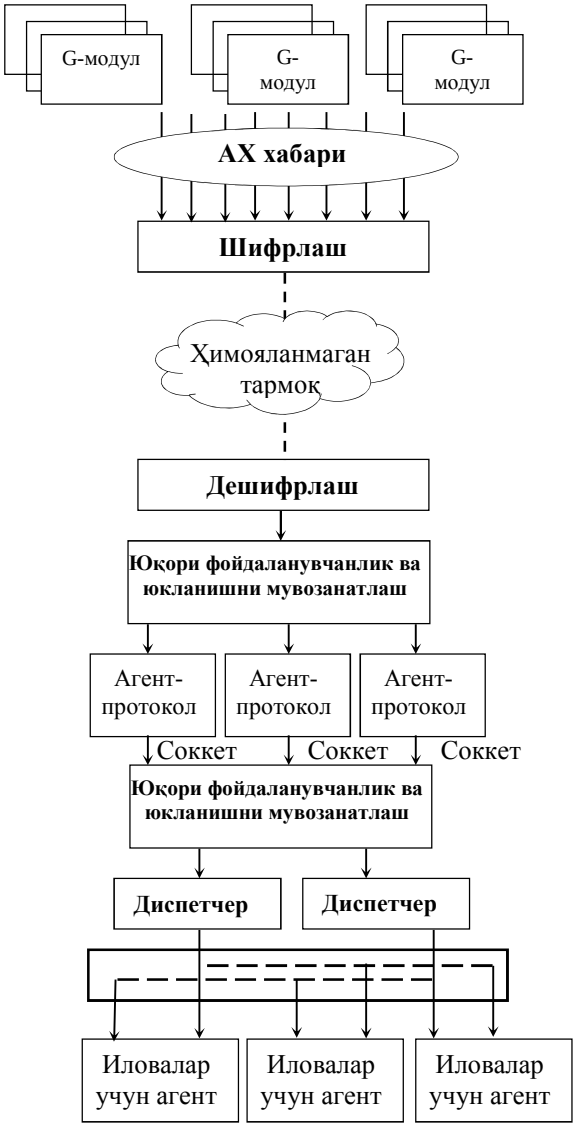
Дастлабки фильтрлар G-модулларнинг бўш ресурсларини сезиларли даражада оширади, аммо иккита асосий камчилиги бор. Биринчиси - тақсимланган фильтрларни бошқариш мураккаблиги. Ҳар бир фильтр айнан зарур бўлган созланмаларни ўзида сақлашини кафолатлаши учун, ўзгаришларни амалга оширишда аниқ муолажалар зарур. Бундан ташқари, аксарият дастлабки фильтрлар бошқарув мураккаблигини жуда ҳам оширадиган конфигурациянинг турли файлларидан фойдаланиши мумкин бўлган иловалар сатҳига ўрнатилади. Иккинчиси - фильтр қўлланиладиган тизим хусусидаги билим миқдорининг камайтирилиши. Статистикалар ишончсиз бўлиб боравергач, АХ инцидентини таҳлиллаш ва муҳокамасини ўтказиш қийинлашаверади.

АХ хабарларини йиғиш ва сақлаш. G-модуллар томонидан амалга ошириладиган асосий ҳаракатлар – “хом”(ишланмаган) маълумотларни турли протоколлар бўйича қабул қилиш ва уларни маълумот манбаси турини идентификациялаш, маълумотларни форматлаш ва умуий кўринишга олиб келиш билан шуғулланадиган N-модулга юбориш. Хабар форматлаштирилганидан сўнг, у ходисалар маълумотлар базасида (DB модулда) сақланади. Модулларнинг унумдорлиги ва фой-даланувчанлиги масалалари ҳисоблаш тармоғидаги тақсимланган G-модуллар, N-модуллар ва DB-модуллар жойлашишини регламентловчи АХМТ архитектураси дизайни ва масштаблилиги билан аниқланади.

Ҳар хил гетероген маълумотлар манбаларидан мониторинг маълумотларини тўплаш икки турдаги дастур компонентлари мавжудлигини талаб қилади: протокол агентлари ва иловалар учун агентлар. Биринчи тур G-модуллардан маълумотларни йиғади, иккинчи тур олинган хабарларни стандарт форматда базада сақлаб, уларни фарқлайди ва структуралайди. Агент-протокол диспетчер орқали илова учун агент билан бирга иш олиб боради. Бундай ёндашув АХ мониторинги маълумот манбаларининг, юкланишни мувозанатлаш механизмларидан фойдаланиб, АХМТ

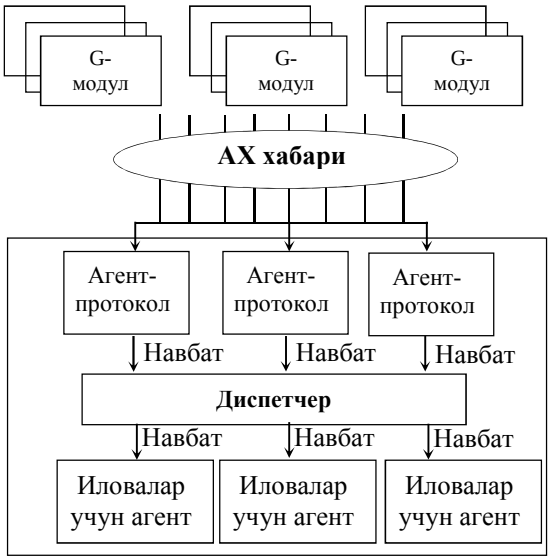
умумий архитектурасининг ҳар қандай сатҳида ишончли интеграциялашувига имкон беради.

Агент-протоколлар хабарларни АХ маълумотлар манбасидан маълумотни узатишнинг маълум транспорт протоколлари(масалан, Syslog, SNMP, SMTP, HTML) орқали N-модулга узатиш учун зарур. Агент-протокол - ахборотни ҳимоялаш воситалари ишлайдиган операцион тизимлардаги жараён. Ушбу жараённинг асосий вазифаси G-модулдан келган хабарларни қабул қилиш ва йиғилган маълумотларни диспетчерга узатишдан иборат. Одатда бу қийин бўлмаган жараён ва уларни амалга ошириш ва хизмат кўрсатиш анча енгил. Дастлабки АХ хабарлари оддий матнли файлда сақланиши, сўнгра транспорт протоколидан фойдаланиб N-модулга юборилиши мумкин, бироқ маълумотларнинг каналлар (named pipec), соккетлар (sockets) ёки тақсимланувчи хотира (shared memory) технологияларидан фойдаланган ҳолда диспетчерга бевосита узатилиши тезкор ҳаракатланишни таъминлайди.



Маълумотларни йиғишнинг тақсимланган архитектураси

“а”



Маълумотларни йиғишнинг локал архитектураси

“б”

2 –расм. АХ хабарларини йиғиш жараёни

Агент-протоколларнинг юқори фойдаланувчанлигига қуйидаги усуллар ёрдамида эришиш мумкин:

– агентлар фермаси – агент-протоколларининг (Syslog, SNMP, SMTP) сервер дастурий таъминотининг бир неча инстанциялари аппарат серверлари массивидан юқорида ўрнатилади. Юкланишни мувозанатлаш ва бузилишга бардошлилик стандарт воситалар билан таъминланади;

– кластер – агент-протоколларнинг сервер дастурий таъминоти кластерли архитектурадан юқорида ўрнатилади.

Юқорида номи келтирилган вариантлардан ҳар бири, юқори фойдаланувчанликни таъминлашнинг қайси усулидан фойдаланишидан қатъий назар, маълумотларни йиғишнинг ишончли масштабланувчи платформасига таянади.

Ахборот хавфсизлиги нуқтаи назаридан, энг муҳим он, агентлар томонидан тўпланган маълумотлар яхлитлигини таъминлашдир. Айниқса, бу маълумотлар умумфойдаланувчи ёки ишончсиз ҳисоблаш тармоқлари орқали узатилса долзарб саналади. Агент-протоколларнинг аксарияти транспорт сатҳининг ишончсиз UDP протоколи устида ишлайди. Шундай қилиб, N-модул томонидан қабул қилинишини ва узатиш вақтида алмаштирилмаслигини кафолатлаш учун узатилувчи маълумотларни ҳимояланган туннелга инкапсуляциялаш зарур. Ишончли маълумотларни узатишни

Унумдорликни яхшилаш учун кўрсатилган маълумот-лар базаси хотирага олдиндан ўрнатилган бўлиши лозим. Узатиш протоколларига боғлиқ ҳолда хабарларнинг турли генераторлари турли хабар форматларидан фойдаланганлиги сабабли, маълумотлар базаси ўзида ҳар жуфт “G-модул тури, узатишнинг транспорт протоколи”ни ноёб идентификациялайдиган кетма-кетлик наборини сақлаши лозим.

Диспетчер қуйидаги автоном амалларни бажаради:

– номланган каналлар, соккетлар, навбатлар кетма-кетлиги ва ҳ. орқали агент-протоколлардан кирувчи маълумотларни олади;

– ахборот хавфсизлиги маълумотлар манбалари кетма-кетлигини идентификациялайдиган

– мос маълумотлар базасига кирувчи маълумотларда маълум

– идентификацияланган маълум G-модулдан олинган кирувчи маълумотларни мос чиқувчи канал орқали маълумотларни ишлашга қодир агентга юборади.

Илова агентлари ҳар бир жуфт "G-модул, узатишнинг транспорт протоколи" учун ўзига хос ҳисобланади. Улар кирувчи хабарларни DB-модулда сақлаш учун ягона форматга келтиришни амалга оширади.

Илова агентлари қуйидаги автоном амалларни бажаради:

– номланган каналлар, соккетлар, навбатлар кетма-кетлиги ва ҳ. орқали диспетчердан кирувчи маълумотларни олади;

– кирувчи хабарларни стандарт форматдаги хабарларга ўзгартиради;

– форматланган хабарларни мос DB-модулга юборади.

Бу ҳолда DB-модулининг хусусиятига боғлиқ ҳолда ахборот узатиш каналларининг турли вариантлари ҳам ишлатилиши мумкин. Юқорида тавсифланган маълумотларни йиғиш жараёни 2-расмда келтирилган.

Расмда маълумотларни йиғишнинг тақсимланган(2-расм “а”) ва локал(2-расм “б”) архитектураси кўрсатилган. Маълумотларни йиғишнинг локал архитектурасидан пилот лойиҳа-амалга ошириш учун транспорт сатҳининг TCP протоколидан ва агент-протоколларига ўрнатилган криптография хизматларидан(бундай хизматлар, масалан, SMTP ёки HTTPда ўрнатилган бўлиши мумкин) фойдаланиш зарур. Юқори даражадаги унумдорликни, юқори фойдаланув-чанликни ва юкланишни мувозанатлашни таъминлаш зарур бўлса, ажратилган қурилмада криптографик ҳимоя функцияларини бажариш лозим.

Диспетчер мақсади - кирувчи хабарнинг манбаси турини аниқлаганидан сўнг уни мос илова учун агентга юбориш. Буни амалга ошириш учун ҳар бир манбадан олинган маълумотларда маълумот манбасини идентификациялайдиган қандайдир ноёб кетма-кетлик сақланиши лозим. Кетма-кетликларни сақлаш учун махсус маълумотлар базаси керак.

кетма-кетлик мавжудлигини текши-ради; ларни амалга оширишда ёки кам миқдордаги ахборотни ҳимоялаш воситаларига эга ҳисоблаш муҳитида фойдаланилади.

Иловалар учун агент-протокол, диспетчер ва агентларнинг тақсимланган архитектураси масштаблилик ва юқори фойдаланувчанликни таъминлаш учун универсал ечим ҳисобланади, бироқ бунда диспетчер ва илова агентлари функцияларининг такрорланиши содир бўлиши мумкин. Шундай қилиб, баъзи ҳолларда амалга оширишни соддалаштириш ва тизим унумдорлигини яхшилаш мақсадида диспетчер ва иловалар учун агент жараёнларини бирлаштириш маънога эга.

АХ хабарларини таҳлиллаш АХМТ маълумотларини аналитик таҳлиллаш билан боғлиқ асосий амаллар - АХ хабарларини корреляциялаш, структурали таҳлил, ҳужумларнинг тарқалиш йўлларининг таҳлили ва ҳолат таҳлили ҳисобланади.

АХ хабарларини корреляциялаш - бутун кейинги таҳлилни бажариш мумкин бўлган мос контекстни яратишга олиб келувчи турли АХ хабарлари орасидаги ўзаро статистик боғланишларни қидириш амали(Контекст – АХ хабарини АХ инцидентига алоқадорлигини аниқловчи умумий мезонларни қаноатлантирувчи форматланган маълумотлар контейнери). Таҳлил контекстларнинг ҳужум характеристикаларига мослигини текшириш орқали амалга оширилади.

Структурали таҳлил АХ хабарларини олдиндан маълум шаблонларга мувофиқлигини текширувчи комплекс жараён ҳисобланади. Структурали таҳлил маълум бир контекст доирасидаги ҳодисаларнинг ҳужумга олиб келишини аниқлаш учун ишлатилади [5].

Ҳужум тарқалиши йўлининг таҳлили – бу кейинги босқич бўлиб, унинг натижасида аниқланган ҳужум бўйича ҳимояланган тизимнинг обрўсизлантирилиши даражаси ҳамда ҳужумнинг турли босқичлари бир-бири билан қандай боғланганлиги хусусида ахборот олинади.

Ҳолат таҳлили ҳужумни аниқлаш учун хавфсизлик сиёсатини қўллайди. Тайёргарлик босқичида хавфсизлик сиёсатини қаноатлантирадиган ҳолат профили яратилади - бу автомат ёки автоматлашган жараён бўлиши мумкин. Шундан сўнг, барча хабарлар ва тизим ҳодисаларининг

яратилган профилга мослиги текширилади ва оғиш ҳолатида огоҳлантирувчи сигнал генерацияланади. Шундай қилиб, нафақат ҳужумни ва унинг турини аниқлаш жараёни амалга оширилади, балки ҳимоя объектининг ҳимояланганлик даражасини баҳолашга имкон берувчи хавфсизлик сиёсатининг бажарилишини текшириш ҳам амалга оширилади [6].

Фойдаланувчи билан алоқанинг икки хил интерфейси мавжуд: АХМТнинг бошқарув консоли ва фойдаланиш портали. АХМТнинг бошқарув консоли (R-модул) АХ инцидентларининг таҳлилини ўтказишда ёрдамлашиш учун ишлатилади ва М-модулнинг турли қисмларидан келган маълумотларни интеграциялайди. Бошқарув консоли ўзида қуйидаги интерфейсларни бирлаштиради:

– вақтнинг реал режимида АХ хабарларини мониторинглаш - М-модулда сақланаётган хабарларнинг дастлабки маълумотларини тақдим этади. Ушбу интерфейс қидирув ва тартиблаш мақсадида АХ хабарларининг таянч функцияларини фильтрлашни амалга оширишга имкон беради. АХ хабарларининг мониторинги интерфейси вақтнинг реал режимида созлаш, берилган ҳодисаларни батафсил таҳлили ва ходисаларни қайта кўриб чиқиш учун ишлатилади;

– АХ инцидентларининг таҳлили – АХ инцидентлари тарихини яратиш ва кейинчалик хизмат кўрсатиш ва уларга реакция кўрсатиш жараёни учун ишлатилади. Ушбу интерфейс олинган огоҳлантирувчи сигналлар хусусидаги малакали ахборотни, носозликларни тузатиш учун кўплаб маълумотларни ва тиклаш учун текширув нуқталарини тақдим этади. АХ инцидентларини ишлаш интерфейсига турли талаблар қўйилиши мумкин: унумдорлик бўйича, эргономика ва фильтрлаш бўйича, бу эса унинг тўлиқлигини оширади. Ушбу интерфейс АХ инцидентларига тезкор ва адекват таъсир кўрсатиш элементи бўлиб ҳисобланади;

– статистик таҳлил - АХнинг дастлабки маълумотларини вақтнинг қисқа, ўрта ва узоқ муддатли оралиқларида аналитик ишлаш натижаларини тақдим этади. Ушбу интерфейсга ахборотни (графиклар, диаграммалар ва ҳ. шаклида) график ифодалаш учун махсус қисмсатҳ талаб қилинади.

Фойдаланиш портали ахборот хавфсизлиги соҳасида компаниянинг кўп сатҳли ҳисобот кўринишидаги фаолияти хусусида форматланган ахборотни тақдим этади. Портал турли тоифали фойдаланувчилар учун мўлжалланган: ахборот хавфсизлиги соҳасидаги мутахассислардан бошлаб то ахборот хавфсизлиги учун маъсул бўлган компаниянинг юқори лавозимдаги раҳбариятигача. Фойдаланиш портали қуйидаги интерфейсларни ўз ичига олади:

– ахборот хавфсизлигининг бузилиши рискини баҳолаш – ҳимояланганлик даражаси хусусида, ахборот обектларининг характеристикаси ҳақида, уларнинг жорий вақтдаги созланмалари хусусида ва заифлик даражаси хусусида ҳамда содир бўлиши мумкин бўлган ҳужумлар сценарийси хусусида умумий ахборотни акс эттиради. Ушбу интерфейс ҳимоянинг техник хусусиятларини ахборот активларининг қиймати кўрсаткичлари билан боғлаш қобилиятига эга бўлиши лозим, натижада ахборот хавфсизлиги бузилиши рискларини қандайдир сифатий баҳосини тақдим этади;

– АХ ходисалари - ташкилотдаги АХ вазиятларига макро қарашни ҳосил қилишга имкон берувчи ҳимояланувчи тизимларда ўрта ёки узоқ вақт мобайнидаги ҳужум турлари, уларнинг частоталари, манбалари ва оқибатлари хусусида ҳисоботдорликни тақдим этади. Ушбу интерфейс янада қуйироқ сатҳда ҳужумларнинг кейинги ҳаракатларини ва ахборот хавфсизлигининг ўзига хос таҳдидларини аниқлашда қўлланилади, масалан, аниқ бир тармоқ хизматлари ва хостларига йўналтирилган.;

– тизим мақоми - ушбу интерфейс охирги фойдаланувчига вақтнинг псевдореал режимида АХ жорий инцидентлари, ҳужумга учраган тизимлари, нияти бузуқлар ишлатадиган ҳужумлар бўйича батафсил маълумотномани тақдим этади. Шу билан бир қаторда жавоб реакциясини ва ҳужумларни нейтраллаштириш учун мавжуд АХ инцидентларининг эскалация муолажаларини ҳам тақдим этади.

Хулоса

Маълумотларни таҳлил қилиш жараёнида АХ хабарларини ошиши билан АХМТ компонентларининг иш унумдорлигига қуйилган талаблар ҳам ортади, чунки маълумотлар базасига структураланган-сўровларни ишлаш учун вақт ва ресурс талаб этилади. Замонавий ҳужумларнинг жуда тез кечиши сабабли АХ хабарларини ўз вақтида таҳлиллаш ва жавоб ҳаракатларини кўриш керак бўлади. Шунинг учун структураланган-сўровларни бажаришга талаб этиладиган вақт қатъий чекловларга эга. Бу эса маълумотларни ишлаш жараёнида АХ хабарларини таҳлиллаш тезлигини янада ошириш соҳасини кўрсатиб беради.

Умуман олганда, юқорида келтирилган АХМТ элементларининг таҳлили кўрсатадики, АХМТни тўлдиришга имкон берувчи ва ахборот хавфсизлиги маълумотларини ишлаш ва сақлаш, архитектура ва функционаллиги соҳасида ишлаш самарасини оширувчи бир қатор сифатли ўзгартиришларни ишлаб чиқиш талаб этилади.

Фойдаланилган адабиётлар

1. Kitsos P. (ed.). Security in RFID and sensor networks. – CRC Press, 2016.

2.Dhanabal L., Shantharajah S. P. A study on NSL-KDD dataset for intrusion detection system based on classification algorithms //International Journal of Advanced Research in Computer and Communication Engineering. – 2015. – Т. 4. – №. 6. – С. 446-452.

3.Bahl S., Sharma S. K. Performance Analysis of User to Root Attack Class Using Correlation Based Feature Selection Model //International Joint Conference. – Springer, Cham, 2015. – С. 177-187.

4.Marchal S. et al. A big data architecture for large scale security monitoring //Big data (BigData Congress), 2014 IEEE international congress on. – IEEE, 2014. – С. 56-63.

5.Shrimpton T., Terashima R. S. A provable-security analysis of Intel's secure key RNG //Annual International Conference on the Theory and Applications of Cryptographic Techniques. – Springer, Berlin, Heidelberg, 2015. – С. 77-100.

6.Pan Z., Ling Q. I. U., Chao C. The Method of Detection Network Attacks Based on Particle Swarm

Optimization //Journal of Chongqing Normal University (Natural Science). – 2015. – Т. 1. – С. 021.

Ташев Комил Ахматович
ТАТУ, Компьютер инжиниринги факултети декани, доцент, т.ф.н.
Тел.: +998 (71) 238-64-13
Эл. почта: k.tashev@tuit.uz
Насруллаев Нурбек Бахтиёрович
ТАТУ, Ахборот хавфсизлигини таъминлаш кафедраси катта ўқитувчиси
Тел.: +998 (71) 238-65-25
Эл. почта: n.bakhtyarovich@gmail.com
Исломов Шахбоз Зокир ўғли
ТАТУ Phd талаба
Тел.: +998 (71) 238-65-38
Эл. почта: shaxboz4044@gmail.com

Tashev K.A., Nasrullaev N.B., Islomov Sh.Z.
Architecture Of The System Of Information Security Monitoring
In this article is reviewed an assessment of the level of security of information and communication systems in the information security monitoring system, which allows you to successfully carry out incidents in the system and determine the degree of criticality associated with this incident, generation of information security messages, collect them from different types of security tools and database storage as well as the stages of message analysis
Keywords: monitoring, protection, confidentiality, risk, attack, vulnerability, protocol, filter.

УДК 639.311

И. Каримов, Б.Э.Элмуродова

МЕТОДЫ ПОСТРОЕНИЯ МАТЕМАТИЧЕСКОЙ МОДЕЛИ ЭКОСИСТЕМЫ РЫБОВОДНОГО ПРУДА

Рассматриваются вопросы построение математической модели процесса выращивание рыб с учетом специфических особенностей экосистемы, а также региональных особенностей рыбоводного пруда, видов рыбных ресурсов, соленостей дренажных водоемов, исследуются климатические факторы: температура воды и интенсивность солнечной радиации на поверхности водоема.

Ключевые слова: модель, концептуальное моделирование, экосистема, рыбоводный пруд, устойчивость, концентрация, белый толстолобик, карп.

При построении математической модели любой экосистемы первоочередной задачей является выбор переменных. Это наиболее субъективная и наименее формализованная часть работы, и определяется она следующими факторами: цели и задачи исследования; доступная экспериментальная и теоретическая информация; «обозримость модели». Для оценки рыбохозяйственных возможностей пруда требуется подробное описание, как рационов, так и трофических взаимодействий между различными видами рыб и между рыбами и другими компонентами экосистемы. С другой стороны, для описания процессов, происходящих в экосистеме водоема, требуется достаточно полное представление о протекающих в рыбоводном пруду гидробиологических процессах /1,3/.

В пруду выращивается карп, белый толстолобик и буффало. Последние два вида в модель пока не включены в силу их относительной независимости от других компонентов экосистемы и их незначительной биомассы в общем количестве выращиваемых рыб. Исходя из кормовой базы карпа - *C* и толстолобика - T, в модель включены следующие переменные: *F* - фитопланктон, *E* - бентос, Z - зоопланктон и *B* - бактерии. Для описания круговорота биогенных веществ, способных лимитировать продукционный процесс, в модель включены: *P* - растворенный минеральный фосфор и *N* - растворенный минеральный азот. Циклы биогенных элементов замыкаются детритом - D, который, кроме того, иногда входит в рацион толстолобика. Для описания мелководного пруда глубиной порядка 1 м, эффектами пространственного распределения организмов и веществ можно пренебречь, поэтому строят точечную модель. Все переменные рассматриваются в виде концентраций (единица измерения - *г/м*^{3} или *г/м*^{2}). Под концентрацией живых объектов понимается отношение их суммарной живой биомассы к общему объему водоема. Основные процессы трансформации вещества качественно примерно одинаковы для большинства пресноводных экосистем. Поэтому за основу при построении данной модели принимались модели экосистем водохранилищ, озерных экосистем и рыбоводных прудов.

Переход вещества с одного трофического уровня на другой описывается S-образными функциями. Скорости процессов потребления и роста определяются количеством доступного субстрата и такими физическими условиями среды, как температура и освещенность. Предполагается, что лимитирование светом и температурой можно задать мультипликативными членами в общей функции потока вещества:

$$Q_{ij} = Q\,(t, i, j, TT, I) = f_i(TT) * g_i * \Phi_{(i,\,i)} * (1 - M\,B_i),$$

где Q_{ij} - функция, определяющая поток вещества из *i*-й в *j*-ю переменную (например, из *F* в Z), *t* - время, f_i *(TT)* - функция, описывающая лимитирование *j*-го организма температурой *(j = F,Z,E,T* или C), g_j (I) - функция, описывающая лимитирование *j*-го организма светом *(j* = F), *TT* - температура воды, *I* - интенсивность солнечной