I wish to thank Professor Rishat Usmanov under Department of Computer Systems for his support over the period in which this paper was written. I would like to express my gratitude towards my colleagues, Tashkent University of Information Technologies for giving me the opportunity to make its facilities available for me.

References

1. A. R. Rivera, B. Ryu, and O. Chae, "Content-Aware Dark Image Enhancement Through Channel Division" IEEE Transactions On Image Processing, Vol. 21, No. 9, September 2012.

2.Vinay Kumar and HimaniBansal, "Performance Evaluation of Contrast Enhancement Techniques for Digital Images", International Journal of Computer Science and Technology, Vol. 2, No. 1, pp.23-27, 2011.

3. Menotti D., Najman L., Facon J. and Araujo A., "Multi-Histogram Equalization Methods for Contrast Enhancement and Brightness Preserving", IEEE Transactions on Consumer Electronics, Vol. 53, No. 3, pp.1186-1194, 2007.

4. Joung-Youn Kim, Lee-Sup Kim and Seung-Ho Hwang, "An advanced contrast enhancement using partially overlapped sub-block histogram equalization," IEEE Trans. Circuits Syst. Video Technol., Vol. 11, pp.475-484, April 2001.

5. Y.-T. Kim, "Contrast enhancement using brightness preserving bi-histogram equalization," IEEE Trans. on Consumer Electronics, Vol. 43, pp.1-8, February 1997.

6. David Menotti, Laurent Najman, Jacques Facon, and Arnaldo de A. Araújo" Multi-Histogram Equalization Methods for Contrast Enhancement and Brightness Preserving" IEEE Transactions on Consumer Electronics, Vol. 53, pp.1186-1194, August 2007.

7. Kotkar V. A. and Gharde S. S. "Review of various image contrast enhancement techniques", International Journal of Innovative Research in Science, Engineering and Technology Vol. 2, Issue 7, July 2013.

8. S. S. Pathak, P. Dahiwale and G. Padole. "A combined effect of local and global method for contrast image enhancement, ". *ICETECH. IEEE,* 2015.

9.http://homepages.inf.ed.ac.uk/rbf/CAVIARDATA1/

10. http://cvrr.ucsd.edu/aton/shadow/

11. Akmalbek Abdusalomov, Taeg Keun Whangbo "An improvement for the Foreground Recognition Method using Shadow Removal Technique for Indoor Environments" World Scientific Publishing Company, *International Journal of Wavelets, Multiresolution and Information Processing*, Indexed in SCIE. Vol. 15, No. 4(2017)May. www.worldscientific.com/worldscinet/ijwmip

Akmalbek Abdusalomov*
Assistant professor in Department of Computer systems
Тел.: +998 (90) 1005046
Эл. почта: akmalbekabdusalomov@gmail.com

Mukhriddin Mukhiddinov
Assistant professor in Department of Hardware and Software of Control Systems in Telecommunication
Тел.: +998 (97) 7049318
Эл. почта: mmuhriddinm@gmail.com

Ichki atrof-muhit obyektlari uchun histogramni tenglashtirish asosida tasvir sifatini takomillashtirish

Annotatsiya *Video ketma-ketlikdagi tasvirlarni takomillashtirish kompyuterni ko'rishda muhim muammo bo'lib, obyektlarni ajratish va harakat segmentatsiyasi kabi turli sohalarda qo'llaniladi. Ushbu maqolada obyektlarni ajratib olishda tasvir sifatini yaxshilash uchun rang ma'lumotlaridan foydalanadigan samarali va oddiy metod taklif qilinadi. Taklif etilgan uslub boshida sun'iy yorug'lik manbai sharoitida bino ichki muhitlari uchun yuqori sifatli tasvirlarni yaratish uchun tasvir ranglarini RGB rang kanalidan YCbCr rang kanaliga o'zgartiradi. Metod uchta ma'lumotlar bazasidan foydalangan holda amalga oshiriladi va sinovdan o'tkaziladi. Bizning tizim obyektni aniqlash vazifalariga ko'maklashish uchun ichki muhit sahnalarda yaxshi ishlashi isbotlangan tasvir kontrasti muammolarini hal etishga erishdi.*

Kalit so'zlar: *Obyektni ajratish, kontrast, rang kanali, histogramni tenglashtirish, tasvirni takomillashtirish.*

УДК 004.056

Н.Б.Насруллаев, Ш.З.Исломов, Д.С.Файзиева

Ахборот хавфсизлиги мониторинги тизими архитектураси

Ушбу мақолада ахборот коммуникация тизимларинминг олдин номаълум бўлган таҳдид ва ахборот хавфсизлиги ҳодисалари ҳақидаги сезиларли миқдордаги маълумотларни оператив ишлаш имконини берувчи ахборот хавфсизлиги мониторинги тизими архитектураси ва ушбу тизимни ташкил этувчи модуллар таклиф этилган, мониторинг тизими архитектураси ва унинг алоҳида қурилмалари ишлаш принципларининг таҳлили асосида тизим ишлашининг муолажавий модели келтирилган.

Калит сўзлар: мониторинг, ҳимоя, конфиденцияллик, тармоқ, ахборот хавфсизлиги, инцидент, муолажавий модел.

Кириш

Маълумки, ахборот-коммуникация тизимлари (АКТ) ҳар хил технологик жараёнларни ёки унинг қисмини амалга оширади. Равшанки, ахборот оқимлари ҳаракатидаги ҳар қандай янглишиш ёки улардан фойдаланиш қоидаларининг бузилиши ишдаги муаммоларга ва қўшимча ҳаражатларга ёки фойданинг бой берилишига олиб келиши мумкин. Шунинг учун, ҳар қандай ташкилот ёки компания ахборот соҳасидаги ўз қизиқишларини ҳимоя қилиш мақсадида ахборотни суистеъмол қилиш, фирибгарлик, муҳим амалларнинг барбод бўлишини ва конфиденциал ахборотни рухсатсиз ошкор этилиши каби ҳолатларни олдини олиш учун АКТ хавфсизлигини таъминлаш бўйича кучайтирилган чораларни қўллайдилар.

Шу сабабли ўз вақтида ва самарали мониторингнинг аҳамиятини сезиларли даражада аниқлайдиган ахборот хавфсизлигини (АХ) таъминлаш билан боғлиқ, қуйидаги жиҳатларни белгилаб олиш мумкин.

Биринчидан, АХ бузилишларини вақтнинг реал режимида аниқлаш ва уларга адекват реакция кўрсатиш. Бу ахборот хавфсизлиги маъмурларининг кўп сонли ахборотни ҳимоялаш воситаларидан(антивируслар, тармоқлараро экранлар, хужумларни аниқлаш тизимлари ва ҳ.) келиб тушадиган маълумотларни қабул қилиш ва кейинги таҳлиллаш жараёнларига зарур ва тегишли эътибор қарата олмасликлари билан боғлиқ.

Иккинчидан, персонал фаолияти (тизимга кириш, киритиш/чиқариш портларидан фойдаланиш, ахборотни ташқи элтувчиларга ёзиш ва ҳ.) билан боғлиқ ҳодисалар ва ташқи бузғунчилар (тармоққа рухсатсиз суқилиб киришга уринишлар, вирусли ҳужумларни ўтказиш, хизмат кўрсатишдан воз кечишга ундаш ва ҳ.)мониторингининг узлуксизлигини таъминлаш.

Учинчидан, ахборот коммуникация технологияларини ривожланиши натижасида жиноятчилар томонидан конфиденциал ахборотни рухсатсиз ва ноқонуний олиши учун қўлланиладиган янги усул ва воситаларни аниқлаш имконияти. Бу имкониятни амалга ошириш ахборот хавфсизлиги тизимида маълум интеллектнинг мавжудлигини талаб қилади.

Асосий қисм

Ўз вақтида АХ бузилишларини аниқламаслик ва конфиденциал ахборотни ҳимоялаш бўйича адекват чораларни кўрмаслик ахборот хавфсизлиги тизими томонидан таъминланадиган мавжуд ҳимояланганлик даражасини жиддий пасайишига олиб келади. Шунинг учун, ҳар хил, хусусан олдин маълум бўлмаган, ахборот хавфсизлиги тахдидларини ўз вақтида аниқлашга имкон берадиган мониторинг муолажасини яратиш ва кейинчалик уни амалга ошириш зарур. Бундай жараённинг мавжуд эмаслиги натижасида ташкилот ёки корхона ички ва ташқи жиноятчилар

ҳаракатидан бир неча қадам орқада қолади, хамда ташкилотнинг йирик молиявий йўқотишига ва обрўсизлантирилишига сабаб бўладиган ташқи манбаларда юз берадиган ахборотнинг сирқиб чиққанлиги ҳақида билмайди.

Мониторинг ёрдамида ҳал қилинадиган вазифалар белгиланган [1]:

– хавфсизлик сиёсати бузилишида инцидентларни текширишда ҳодисалар орасидаги сабаб-оқибат алоқаларини аниқлаш;

– хавфсизлик сиёсатидаги камчиликлар, номукаммалликлар ва хатоликларни таҳлил қилиш;

– АКТнинг базавий дастурий-аппарат ва АХни таъминлаш воситаларининг нотўғри ишлаши (хатоликлар, янглишишлар) сабабларининг таҳлили;

– тармоқ ахборот структураси фойдаланувчилари томонидан ресурслардан самарасиз ва оқилона бўлмаган фойдаланиш фактларини аниқлаш.

Юқорида таъкидланганидек, доимий тарзда мониторинг ўтказиш ахборотни ҳимоя қилишнинг зарур даражасини сақлаб туришнинг кафолати ҳисобланади, мониторинг тизими фаолияти доирасидаги натижалар эса ахборот хавфсизлигини таъминлаш тизимини такомиллаштиришга асос бўлиб ҳисобланиши лозим.

АХнинг тўлиқ ва самарали мониторингини ташкил қилишда бир қатор одатий муаммалорга дуч келиш мумкинлигини ҳисобга олиш лозим[2]:

– компания ёки ташкилот ихтиёридаги бўлган ахборотни таҳлиллашда тизимли ёндашувнинг йўқлиги;

– дастурий-аппарат воситалар ҳимоялаши керак бўлган активларни идентификациялашда нотўғри ҳисоблашларнинг мавжудлиги;

– электрон журналларда қайд этилган кўплаб ҳодисалар ичидан хавфсизликни таъминлаш учун аҳамиятга эга бўлган ахборотни аниқлашдаги қийинчиликлар;

– ахборот ресурсларидан ва уларни ишловчи воситалардан максимал фойдаланиш имконияти мавжуд ходимларнинг (дастурчилар, маъмурлар) фаолияти назоратини автоматлаштирилган воситалар томонидан қамраб ола олмаслиги.

Ушбу муаммолар кўплаб сабабларга кўра содир бўлиши мумкин:

– персоналнинг мониторинг жараёнига расмий муносабати;

– маълумотларни сифатли таҳлиллаш учун ушбу персонал малакасининг етарли эмаслиги;

– кирувчи маълумотлар хажмининг катталиги ва ҳ.

Ахборот хавфсизлигини тўлиқ таъминлаш учун ҳар куни қуйидаги ахборот манбаларини ишлаш лозим:

– антивирус дастурий таъминоти, почта серверлари, хужумларни аниқлаш тизимлари, тармоқлараро экранларнинг лог файллари;

– операцион тизимларнинг хавфсизлик журналлари;

– лахзали хабар алмашиш учун дастурлардан фойдаланиш ҳақидаги маълумотлар;

– телефон алоқаси хизматини кўрсатиш ҳақидаги ёзувлар ва ҳ.

Таъкидлаш лозимки, хавфсизлик ҳодисалари ҳақидаги ахборотни ўз вақтида қабул қилиш ва таҳлиллаш қуйидагиларни таъминлашга имкон беради:

– АКТ ахборот ресурсларининг конфиденциаллигини, яхлитлигини ва фойдаланувчанлигини бузишга қаратилган жиноятчиларнинг атайин ва беҳосдан қилинган ҳаракатларини аниқлаш;

– кўзда тутилмаган вазиятларни пайдо бўлишини огоҳлантириш ҳисобига АКТ ишлашининг барқарорлигини ва ишончлигини ошириш;

– АКТ ахборот ресурсларини бузиш ва йўқотиш билан боғлиқ хавфларни камайтириш.

Бу ҳолда турли ахборотни ҳимоялаш воситалари мониторинг воситалари ҳисобланади. Айрим ҳодисаларни аниқлаш фактига қандай реакциясига боғлиқ ҳолда актив ва пассив ахборотни ҳимоялаш воситалари фарқланади.

Пассив воситалар бўлиб ўтган ҳодисага қарши ҳеч қандай чора кўрмайди, фақат ушбу ҳодиса фактини қайд этади ҳамда маъмурга бу хусусида хабар беради. Актив воситалар ушбу фактни аниқлабгина қолмайди, балки ундан келадиган салбий оқибатларни блоклаш ва нейтраллаш бўйича кейинги чораларни аниқлашга киришади.

Ташкилотларда ахборот хавфсизлиги ҳолатини баҳолашда мониторинг жараёнида ахборотни ҳимоялашнинг қуйидаги дастурий ва аппарат воситаларидан олинадиган маълумотлардан фойдаланилади [3]:

– хавфсизлик сканерлари;

– антивирус дастурий таъминоти;

– контентли таҳлил воситалари;

– киритиш/чиқариш портларини назоратлаш воситалари;

– тармоқлараро экранлар;

– хужумларни аниқлаш тизимлари ва ҳ.

Келтирилган ахборотни ҳимоялаш воситалари ахборотни узлуксиз йиғади, аммо уларни ҳар хил вақт онида ишлайди. Маълумотларни қайд этиш ва таҳлиллашнинг иккита асосий механизми фарқланади:

1. Интервал – мўлжалланган механизм. Бунда локал машинада жойлашган дастурий агентлар, кейинчалик автоматик тарзда ёки қўлда таҳлилланувчи, инцидентлар хусусидаги ахборотни лог файлларда(журналларда) қайд этадилар. Таҳлиллаш жараёнида реал вақт режимидаги таҳлиллашга нисбатан тизимга кам юклама тўғри келади, аммо ахборотни йиғиш ва сақлаш учун дискли хотиранинг катта хажми талаб қилинади.

2. Реал вақт механизми. Бунда ахборотни узлуксиз йиғиш, уни таҳлиллаш ва мос хабарларни бериш имконияти мавжуд. Хужумларни етарлича тез аниқланиши уларни тўхтатишга имкон берсада, бундай таҳлиллаш асосий хотира ва процессор ресурсларининг катта хажмини талаб этади.

Ахборот коммуникация тизимларинминг олдин номаълум бўлган таҳдид ва заифликлар сонининг доимий ўсиб бориши шароитида кўплаб ахборотни ҳимоялаш воситаларининг пайдо бўлиши, ахборот хавфсизлиги ҳодисалари ҳақидаги сезиларли миқдордаги маълумотларни оператив ишлаш муаммосини келтириб чиқармоқда. Маъмур учун бундай ишлашни қўлда амалга ошириш мумкин эмас, шунинг учун ҳозирги вақтда ахборот хавфсизлиги мониторинги тизими(АХМТ) деб номланадиган автоматлаштирилган ёки тўлиқ автомат тизимлари қўлланилмоқда.

АХМТ алоҳида ахборотни ҳимоялаш воситаларининг ишлаши ва ишга лаёқатлиги имкониятининг бузилиши ҳамда нияти бузуқларнинг ахборот конфиденциаллигини, яхлитлигини ёки фойдаланувчанлигини бузишга қаратилган ҳаракатлари билан боғлиқ ахборот хавфсизлиги ҳодисаларини қайд этишга имкон беради.

Ҳозирги кунда ахборот хавфсизлигини таъминлаш воситалари бозорида Symantec, Prism Microsystems, Novell, ArcSight, Alien Vault каби ишлаб чиқарувчиларнинг АХМТлари тақдим этилган [4].

АХМТнинг асосий функцияларига қуйидагилар тааллуқли:

– хавфсизлик журналларини (лог-файлларни) йиғиш – уларни марказлашган ҳолда ягона серверга жамлаш;

– нормаллаштириш – ҳар хил журналлар ёзувларини ягона форматга келтириш;

– тўлдириш – олинган ахборотга ахборот-коммуникация тизимларидан олинган бошқа малумотларни, ҳамда тахдид ва заифликлар ҳақидаги оммавий фойдаланиладиган маълумотларни қўшиш;

– тахдидларни аниқлаш – журналлардаги хавфсизлик ходисалари ичидан ахборот хавфсизлигининг бузилиши аломатларини аниқлаш учун сунъий интеллектни қўллаш;

– инцидентларни бошқариш – тахдидлар аниқланганидан сўнг қўлланиладиган ҳаракатлар. Бу хавфсизлик маъмурига хабарнома юбориш, инцидентга автоматик тарзда реакция кўрсатиш (масалан, қандайдир дастурни бажариш) ва бошқалар бўлиши мумкин;

– ҳисоботларни яратиш – аниқланган тахдидлар ва тизим ишлашининг самарадорлиги ҳақидаги маълумотларни тақдим қилиш.

Келтириб ўтилган функциялар АХМТга хавфсизлик ходисаларига реакция кўрсатиш бўйича ечимни қабул қилишда маъмурга мос мададни таъминлашга имкон беради.

Мониторинг самарадорлиги АХМТнинг ҳар қандай компонентида бузилишлар пайдо бўлиши билан пасайиши мумкин, бироқ амалиёт кўрсатадики, мониторинг тизими таркибидаги ахборотни ҳимоялаш воситалари ишидаги хатоликлар содир бўлганида энг салбий таъсир бўлади. Бу ҳолда ахборотни ҳимоялаш воситаларининг бекор туриши ёки нотўғри ишлаши мобайнида ахборот-коммуникация тизимлари ишлаши самарадорлигининг пасайишига олиб келадиган ахборот хавфсизлиги инцидентларини ўтказиб юборувчи қўшимча тахдидлар пайдо бўлади. Шу сабабли, ахборот хавфсизлиги маъмури учун қийинчилик туғдирадиган баъзан имконсиз бўлган, ахборотни ҳимоялаш воситалари ишлашининг бузилиши сабабларини оператив аниқлаш ва бартараф этиш лозим. Бу АХМТнинг ишлаши ва юқори даражадаги ноаниқликлар (ташвишлар) туғдирадиган ва маъмурнинг қарор қабул қилиш жараёнига таъсир қилувчи жуда кўп эътиборга олиш қийин омиллар мавжудлиги билан изоҳланади [5].

Шунинг учун, АХМТ таркибига кирувчи ахборотни ҳимоялаш воситаларининг ҳозирги ишончлилик ҳолати ҳақида маъмурнинг етарлича маълумотга эга эмаслиги билан боғлиқ ноаниқликларни камайтириш ҳисобига янада самаралироқ ахборот хавфсизлиги мониторингини таъминлайдиган АХМТни ишлаб чиқиш вазифаси долзарб ҳисобланади. Ахборот хавфсизлиги мониторинги тизими (АХМТ) архитектураси нуқтаи назаридан мухокама қилиш ва таҳлиллаш учун мониторинг тизимининг беш сатҳли архитектураси ва ахборот хавфсизлиги мониторинги тизимларида маълумотларни ишлаш жараёни энг муҳим ҳисобланади. Маълумотларни ишлаш жараёнида қуйидаги бешта асосий техник амаллар ажратилади:

– ахборот хавфсизлиги ходисалари хусусидаги хабарларни қайд этиш (ахборот хавфсизлиги хабарларини);

– ахборот хавфсизлиги хабарларини йиғиш;

– ахборот хавфсизлиги хабарларини сақлаш;

– ахборот хавфсизлиги хабарлари кетма-кетлигини таҳлиллаш;

– ахборот хавфсизлиги хабарларига жавоб реакцияларини ишлаб чиқиш.

– АХМТ доирасида ушбу амалларнинг ҳар бирининг бажарилиши учун алоҳида модуллар жавоб беради(1-расм). Қулайлик учун қуйидаги белгилашлардан фойдаланилди:

– G-модул: ахборот хавфсизлиги хабарларини генерациялайди;

– DB-модул: ахборот хавфсизлиги хабарларининг маълумотлар базасини сақлайди;

– R-модул: жавоб реакциясини ишлаб чиқади;

– A-модул: ахборот хавфсизлиги хабарларининг таҳлилига жавоб беради;

– N-модул: ахборот хавфсизлиги хабарларини йиғиш ва нормаллаштириш учун жавоб беради.

Бундан ташқари, заифликларни, суқилиб киришларни аниқлаш ва бартараф қилиш тизими сигнатураси маълумотлари базасини мададловчи ва инцидентлар ҳақидаги билимларни бошқаришга жавоб берувчи M-модулни кўзда тутиш лозим.

Ҳар бир модул маълум ҳаракатларни бажарадиган функционал модуллар гуруҳини тавсифлайди. Масалан, N-модул Syslog (UDP/514) стандарт интерфейси воситасида ахборот хавфсизлиги ходисалари ҳақидаги хабарларни яратадиган кўплаб иловалардан иборат бўлиши мумкин. Бундан ташқари N-модуль суқилиб киришларни аниқлаш ва бартараф қилиш тизимлари, тармоқлараро экранлар, почта хабарларини фильтрлаш тизимлари ва ахборотни ҳимоялашнинг барча воситалари сифатида тақдим этилиши ҳам мумкин.

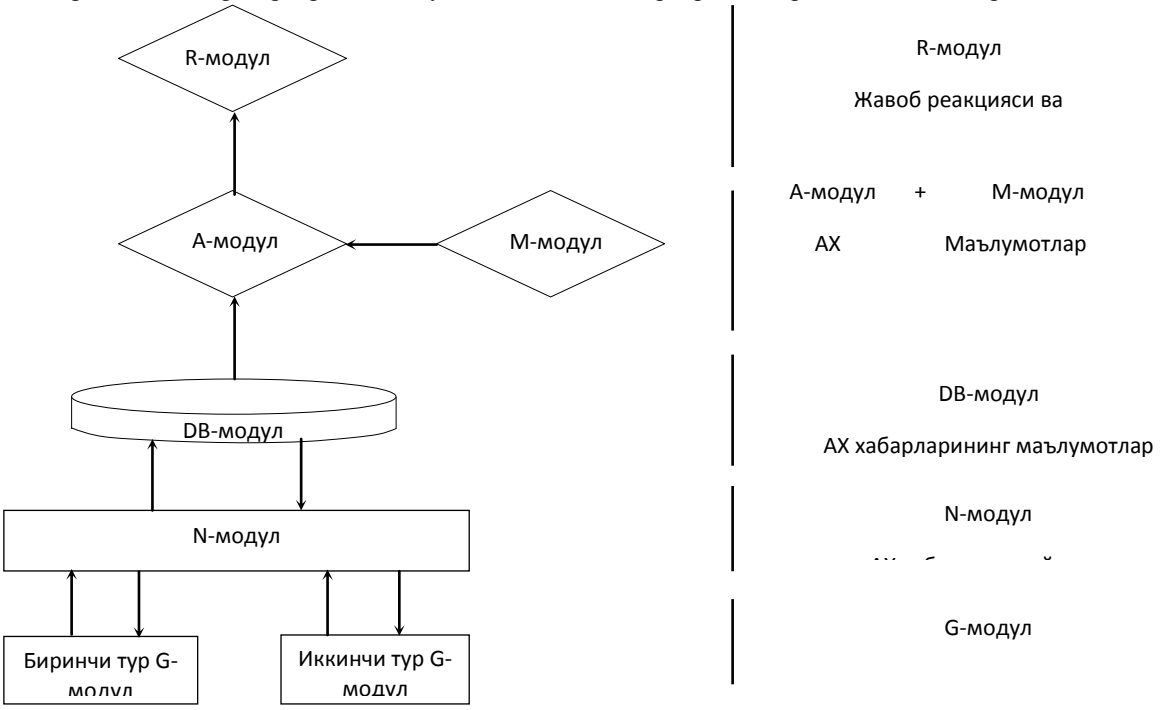
G-модуллар иккита турга ажратилади:

Биринчи тур G-модуллар – ходисаларга асосланган(event-based) хабарлар генератори. У операцион тизимларда, иловаларда ёки тармоқда содир бўлувчи маълум ходиса натижасидаги хабарларни генерациялайди. Бундай G-модулларга Syslog-хабарлар генератори, сенсорлар ва ҳ. мисол бўла олади.

Энг кўп тарқалган биринчи тур G-модуллар – тармоқ ва хост сатҳидаги суқилиб киришларни аниқлаш ва бартараф қилиш тизимлари. Бу категорияга ўзининг таркибига протоколлаш хизматини киритадиган ҳар қандай амалий фильтрация(тармоқ, амалий ва фойдаланувчи) тизимини қўшиш мумкин. Масалан, тармоқлараро экранлар, фойдаланишни назоратлаш рўйхати мавжуд маршрутизаторлар, MAC-адрес бўйича фильтрлайдиган симсиз фойдаланиш нуқталари, RADIUS-серверлари, SNMP traps хизмати ва бошқалар. Honeypots синф тизимлари ва тармоқ пакетлари снифферларини ҳам биринчи тур G-модулларга киритиш мумкин.

Иккинчи тур G-модуллар – баъзи бир ташқи рағбат ёки сўровга реакция сифатида хабарларни генерациялайдиган, ҳолатга асосланган (status-based) хабарлар генератори. Бундай G-модулларга

объект яхлитлигини ёки фойдаланувчанлигини текшириш, PING-пакетларни юбориш, SNMP-poll функцияларини бажариш натижасида хабарларни шакллантирадиган генераторлар мисол бўла олади. Ушбу блоклар етарлича ўзига хос хабар генераторларидир. Уларнинг вазифаси масофадаги учинчи тизимда аниқланган ҳолатни қайд этганда хабарларни генерациялашдан иборат.



1- расм. Ахборот хавфсизлиги мониторинги тизими архитектураси

N-модуллар. Модулларнинг асосий вазифаси (N-модуллар) – ҳар хил G-модуллардан хабарларни қабул қилиш ва хабарларнинг гомоген маълумотлар базасига эга бўлиш учун уларни стандарт форматга келтириш. Сервер томонидаги хизматларни (кластерлаш, компонентни такрорлаш, юкни тақсимлаш ва ҳ) ҳимоялаш учун фойдаланиладиган стандарт усулларни амалга ошириш учун бу модулларнинг фойдаланувчанлигини ва масштаблилигини таъминлаш муҳим. Йиғилган маълумотларни форматлашнинг стандартига эга бўлиш ҳам зарур.

DB-модуллар. DB-модуллар АХМТ архитектурасида энг стандартлашган модул ҳисобланади ва ўзида маълумотлар базасини ифодалайди. Бу модуллар томонидан бажариладиган АХМТ учун ўзига хос асосий амал – бу ахборот хавфсизлиги хабарларини агрегатлаш. Агрегация жараёнида йиғилган маълумотлар оптималлаштирилади, битта ёки бир нечта манбаларда такрорланган хабарлар идентификацияланади ва йўқ қилинади. Агрегация иккити усулда амалга оширилиши мумкин:

– ҳодисалар сатҳида - DB-модули бир ёки бир неча манбалардан олинган хабарлар манбаи, тури ва вақтини таҳлиллайди ва битта ходиса ҳар хил воситалар томонидан қайд этилган бўлса, ягона нормаллаштирилган хабарни маълумотлар базасида қолдириб, такрорланган хабарларни ўчириб юборади;

– ходисалар оқими сатҳида - DB-модули хабар вақти ва вазифасини, манбалар манзилини таҳлиллайди ва хабарнинг мавжуд алоқаларини ягона хабар оқимига йиғади. Бу усул АХМТни бошқариш консолида ахборотнинг тасвирланишини оптималлаштириш имконини беради.

Маълумотлар базаси билан боғлиқ классик муаммолардан (фойдаланувчанлик, яхлитлик, конфиденциаллик) DB-модул учун асосий мауаммо унумдорлик ҳисобланади. G-модуллар миқдори юзлар ёки мингларда ўлчаниши мумкин. G-модулларнинг ҳар бири секундига ўнлаб хабарларни генерациялаши мумкин. Хужумга уриниш вазиятларида жавоб реакциясига вақт қолиши учун ушбу хабарларни ишлаш, базага жойлаштириш ва имкон борича тез таҳлиллаш лозим.

А-модуллар. А-модуллар DB-модулида сақланаётган ходисаларни таҳлилига жавоб беради. Улар ўз вақтида тревога сигналини генерациялаш учун хужумларни аниқлаш бўйича турли амалларни бажаради. Ушбу модуллар ишида фойдаланиладиган механизмлар корреляция алгоритмлари, биринчи ва иккинчи хил хатоликларини аниқлашга, хужумларнинг математик моделларини қуришга ёки

ҳимоянинг тақсимланган воситаларидан фойдаланиб хужумларни аниқлашга асосланган.

А-модулларнинг аксарият амалга оширишлари ностандарт ва ёпиқ ҳисобланади. Тадқиқотлар кўп олиб борилган, лекин уларнинг жуда ҳам кам қисми амалга оширилган. Қолган амалга оширилганлари тўлиқ бўлмай, фақатгина ёндашишини намойиш қилиш, бошқача айтганда концепциясини тасдиқлаш учун етарлидир.

R-модуллар. R-модуллар ўзида ахборот хавфсизлиги инцидентларига жавоб реакциясини амалга ошириш ва ҳисоботни шакллантириш учун инструментлар жамланмасини ифодалайди. R-модул қуйидагиларни ҳисобга олиши лозим: график интерфейс эргономикасини, хавфсизлик сиёсатини амалга ошириш стратегиясини ва ташкилотда мавжуд ҳуқуқий чекловларни. Бу чекловлар жавоб реакцияси сифатида вақт мобайнида тўпланган реал ҳаёт тажрибасига асосланган маслаҳат ёки энг яхши амалиётдан бошқа хеч нарсани виртуал тасаввур қилишнинг деярли мумкин эмаслигига олиб келиши мумкин. Бу билан R-модулларнинг муҳимлигига етарлича баҳо бермаслик керак эмас, чунки ҳужум тўғри таҳлил қилинган ва баҳоланган бўлиши мумкин, аммо ўз вақтида тегишли чоралар қабул қилинмаса ундан қочиб бўлмайди. Ушбу ҳолда ягона реакция фақатгина ходиса сабабини таҳлил қилиш бўлади.

M-модуллар. Таҳлил жараёни ўзида ҳар хил хужумлар хусусиятларини ва сигнатурасини, ҳимояланган тизимнинг эталон моделини, хавфсизлик сиёсатини ва ҳ ўз ичига олган баъзи кирувчи маълумотларни талаб қилади. Ахборот хавфсизлиги инцидентлари тарихини сақлаб қолиш ҳам яхши тажриба ҳисобланади. Ушбу мақсадлар учун M-модуллар ишлатилади.

АХМТнинг беш сатҳли архитектурасининг таҳлили ҳозирги вақтда ахборотни химоялаш воситаларини созлаш усуллари ва воситаларининг тизимга интеграциялашмагани ҳақида фикрлашга имкон беради. АХМТ доирасида ахборот хавфсизлигини бошқариш жараёнини бирлаштириш ва ишлаш қулайлигини ошириш мақсадида бундай функционални қўшиш мақсадга мувофиқ ҳисобланади. Унинг устига, мониторинг тизимида ахборот хавфсизлиги ходисаларига автомат тарзда ёки автоматлаштирилган реакция кўрсатиш имконияти ахборот хавфсизлиги инцидентларига жавоб ҳаракатларига кетадиган вақтни сезиларли камайтиришга ва натижада АКТ ҳимояланганлигини оширишга имкон беради.

Мониторинг тизими структурасининг, унинг алоҳида қурилмалари ишлаш принципларининг таҳлили асосида АХМТ ишлашининг муолажавий модели таклиф этилди(2-расм).

Қуйида АХМТ ишлашининг асосий босқичларининг қисқача тавсифи келтирилган.

1. G-модул ахборот хавфсизлиги инциденти бўлиши мумкин бўлган ахборот хавфсизлиги ходисасини аниқлаганидан сўнг бу хусусида хабарни шакллантиради ва уни мос N-модулга юборади.

2. Хабарлар мос йиғувчи N-модулга юборилаётган вақтда улар миқдорини баҳолаш амалга оширилади.

3. N-модул ахборот хавфсизлиги ходисаси таҳлили учун хабардан зарур маълумотларни чиқариб олади ва уларни АХМТда фойдаланиладиган форматга олиб келади, яъни маълумотларни нормаллаштиришни амалга оширади.

4. Ахборот хавфсизлиги ходисалари ҳақидаги нормаллашган маълумотлар ходисалар маълумотлари базасига ёзилади (DB-модулга).

5. Бу маълумотлар ходисалар маълумотлари базасидан А-модулга келиб тушади. Агар у бўш бўлса(модулда ишлаш учун жойлашган маълумотлар хажми унинг ўтказувчанлик қобилиятидан кам бўлса), 9-босқичга, акс ҳолда 6- босқичга ўтилади.

6. Ахборот хавфсизлиги ходисалари ҳақидаги маълумотлар А-модулда кейинги таҳлил учун навбатда туради.

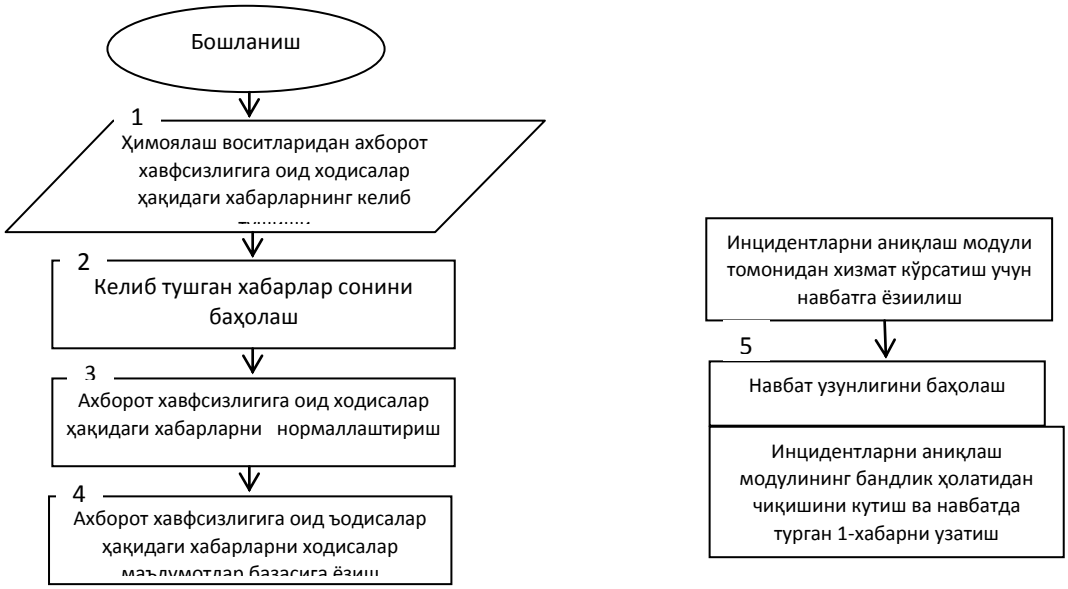
7. Навбат узунлигини баҳолашни амалга ошириш асосида АХМТнинг ўрта сатҳида жойлашган компонентлар ишида бузилишлар мавжуд ёки мавжуд эмаслиги тўғрисида хулоса қилинади.

8. А-модул “бўшаганидан” сўнг, унга навбатда биринчи турган маълумотлар ишланишга юборилади.

9. А-модул М-модулда сақланаётган эксперт билимлардан фойдаланиб, ахборот хавфсизлиги инцидентларининг формал аломатларини қидиришни амалга оширади.

10. Агар А-модул ахборот хавфсизлиги ходисаси қандайдир эҳтимоллик билан ахборот хавфсизлиги инциденти бўлиши мумкинлигини аниқласа 11 босқичга, акс ҳолда эса 14 босқичга ўтилади.

11. А-модул ушбу онда содир бўлган ахборот хавфсизлиги ходисалари ҳақида ахборотни ҳимоялашнинг бошқа воситаларидан қўшимча маълумотларни йиғишни амалга оширади ва шу маълумотларнинг таҳлили асосида ушбу ахборот хавфсизлиги ходисалари орасидаги корреляция мавжудлигини аниқлайди ва ахборот хавфсизлигининг потенциал инцидентларини кўриб чиқади.



14 -расм. АХМТ ишлашининг муолажавий модели

12. Агар инцидентларни таҳлил қилувчи модул таҳлил қилинган ахборот хавфсизлиги ходисаси ҳақиқатдан ҳам ахборот хавфсизлиги инциденти эканлигига ишора қилувчи корреляцияни аниқласа, 13-босқичга , акс ҳолда 14-босқичга ўтилади.

13.Содир бўлган ахборот хавфсизлиги инциденти хусусидаги маълумот инцидентлар маълумотлари базасига ёзилади, хавфсизлик маъмурига мос хабар ва қарши чора қабул қилиш учун тавсия юборилади. Маъмур олинган ахборот асосида аниқланган инцидентга реакция зарурлиги ҳақида қарор қабул қилади(R-модул).

14. А-модулда навбатда хизмат кўрсатиш учун ахборот хавфсизлиги ходисалари хусусидаги маълумотлар қолган бўлса, 6-босқичга ўтилади, акс ҳолда – АХМТ кейинги ахборот хавфсизлиги ходисалари ҳақидаги хабар келишини кутади.

15. АХМТ ишлашининг 1- ва 6- босқичларида катта эҳтимоллик билан унинг компонентлари ишида бузилишлар юзага келиши мумкин.

Шу сабабли муолажавий моделда АХМТга таъсир қилмайдиган 2- ва 7- қўшимча босқичлар киритилган. Бу босқичлардан чиқадиган ахборот (кирувчи ҳолатлар сони ва навбат узунлиги) ахборотни ҳимоялашнинг алоҳида воситаларининг ёки АХМТнинг умумий ишлашида бузишларнинг мавжуд ёки мавжуд эмаслиги хусусида хавфсизлик маъмурининг қарор қабул қилишига имкон беради.

Хулоса

Юқорида келтирилганлардан хулоса қилиш мумкинки, хавфсизлик маъмурининг АХМТ ишлашида иштирок этиши ноаниқлик шароитида қарор қабул қилиши билан бирга амалга оширилади. Ушбу ноаниқлик даражаси мониторинг тизимининг қуйи сатҳида жойлашган ахборотни ҳимоялаш тизимининг ҳақиқий ҳолатини билмаслик натижасида, АХМТда ахборот хавфсизлиги ходисаси хусусидаги хабарларни ишлашда пайдо бўлувчи вазиятларнинг маъмурлар томонидан турлича изоҳланиши мумкинлиги орқали аниқланади.

Адабиётлар

1. Bucci C. J. et al. Portable system for monitoring network flow attributes and associated methods: пат. 9344344 США. – 2016.

2. Kozisek S. E., Coppage C. M., Morrill R. J. System and method for monitoring and optimizing network performance to a wireless device: пат. 9241277 США. – 2016.

3. Chowdhury S. R. et al. Payless: A low cost network monitoring framework for software defined networks //Network Operations and Management Symposium (NOMS), 2014 IEEE. IEEE, 2014. – С.1-9.

4. Bennett M. A. et al. Real-time network monitoring and security: пат. 9769276 США. – 2017.

5. Hoque N. Et al. Network attacks: Taxonomy, tools and systems //Journal of Network and Computer Applications. – 2014. – Т. 40. – С. 307-324.

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.: +998998420601
Эл. почта: shaxboz4044@gmail.com

Файзиева Дилсора Салимовна
ТАТУ, Ахборот хавфсизлигини таъминлаш кафедраси ассистенти
Тел.: +998 (71) 238-65-25
Эл. почта: d.fayzieva@gmail.com

Nasrullaev N.B., Islomov Sh.Z., Fayzieva D.S.

Architecture of the system of information security monitoring

Abstract: *In this article is given the architecture of the information security monitoring system and modules that make up this system, which allows to process a significant amount of data on information security events and previously unknown threats in information and communication systems. Also, a procedural model of the system based on the analysis of the architecture of the monitoring system and the principle of operation of its individual devices is reviewed.*

Keywords: *monitoring, protection, confidentiality, network, information security, incident, therapy model.*

УДК 001.891.573

Р.Н.Усманов, Ш.К.Далиев.

SIMULINK МОДЕЛЬ ДЛЯ ОПРЕДЕЛЕНИЯ ПАРАМЕТРОВ ЛИНЕЙНОГО ВОДОЗАБОРА ДЛЯ УСЛОВИЙ ПОЛУОГРАНИЧЕННОГО ПЛАСТА

Рассматриваются вопросы имитационного моделирования процессов формирования запасов подземных вод, включая процессы их формирования ~~ьи~~ повышения качества в среде Simulink. Предлагаемые модели имеют важноую~~го~~ значимость для улучшения вод~~оа о~~обеспечения населения экологически неблагополучных регионов за счет запасов подземных вод.

Ключевые слова: водозаборы подземных вод, Simulink модель, технологические схемы, модель процесса формирования, геофильтрационный процесс.

Введение. В условиях острой нехватки водных ресурсов вопросы водообеспечения населения, особенно в экологически неблагополучных зонах Средней Азии, в том числе на территориях Каракалпакстана, являются особо актуальными. Одним из основных источников хозяйственно-питьевого водоснабжения населения в таких условиях являются подземные воды, формируемые путем строительства водозаборов подземных вод. Проектирование водозаборов подземных вод осуществляется путем проведения многочисленных вычислительных экспериментов на математических моделях геофильтрации и переноса солей в подземной гидросфере [2,4]. Перспективным для определения параметров водозаборов подземных вод представляется разработка имитационных Simulink моделей. Ниже рассматриваются некоторые вопросы разработки Simulink модели для решения задачи определения параметров и распреснения солоноватых вод водозаборов подземных вод.

Основная часть

Водозаборы подземных вод являются одними из основных, а на экологически неблагополучных территориях единственными источниками хозяйственно-питьевого водоснабжения населения.

При выборе конкретной местности для создания водозаборов подземных вод (ВПВ) основными параметрами являются мощность пласта, состоящего из песков, супесей, уровнепроводности и водоотдачи пород. Пусть n_0 - активная пористость пород; l - расстояние между скважинами, $м$; h - мощность водоносного горизонта, $м$; Q - дебит скважины, $м^3/сут$; d - расстояние от водозабора до контура питания, $м$.

Время начала поступления пресной воды от инфильтрационных каналов к скважинам водозабора определяется по формуле [2]

$$T = \frac{n_0 l h}{Q} \frac{1}{sh(2\pi d/l)} \left[d \cdot ch(2\pi d/l) - \frac{l}{2\pi} sh(2\pi d/l) \right] \quad (1)$$

Выбор параметров линейного водозабора для условий полуограниченного пласта с $H = const$ при формировании пресной воды связан с проведениям многовариантных вычислительных экспериментов. Стратегия проведения вычислительных экспериментов определяется, исходя из работ А.А. Акрамова [2].

При этом рассмотрены различные варианты задач, применительно к водоносным горизонтам различной мощность ($h = 20 \div 50 м$), расстояниям от водозабора до контура ($d = 50 \div 450 м$) между