Tarmoqlardagi hujumlarni aniqlash tizimlarida foydalaniladigan qatorlarni tezkor solishtirish algoritmlarini ishlashini o'rganish

Аннотация *- So'ngi yillar davomida satrlarda so'zlarni qidirish algoritmlari xujjatlarni taxririda, kerakli ma'lumotlarni qidirishda, plagiatlarni aniqlashda, matnlarni tahlilida, bioinformatika va boshqa sohalar uchun kerakli ilovalar juda zarur qurol bo'lganligi sababli ushbu algoritmlar ommobobligi oshmoqda.*

Ushbu maqola satrlarni solishtirish algoritmlarining bir necha xilini ekspremental tahlil asosida ishlashi solishtirilgan. Jumladan, ketma-ket qidiruv, Boeyer-Mur, xeshlash va ikkilik qidiruv algoritmlari asosida dastur ishlashi uchun sarf qilinadigan mashina vaqti xamda tezkor xotira xajmi tahlil qilingan.

Kalit so'zlar: *satrlarda so'zlarni qidirish algoritmlari, tarmoqlarda xujumlarni aniqlash tizimlari, ketma-ket qidirish algoritmlari, Boeyer-Mur algoritmi, xeshlash algoritmi, ikkilik tizimida satrlarda so'zlarni qidirish algoritmi.*

УДК 004.056.52

Ш.Р. Ғуломов, Н.Қ Ахмедова

ТРАФИКНИ МАХСУС ФИЛЬТРЛАШ ҚОИДАЛАРИДА АНОМАЛИЯЛАРНИ АНИҚЛАШ УСУЛИ

Ушбу мақолада тармоқ трафигида аномалияларни пайдо бўлиш сабаблари ва оқибатлари тавсифланган. Ушбу масалаларни ечиш учун трафикни махсус фильтрлаш қоидалари аномалиясини аниқлаш усули таклиф этилган. Таклиф этилаётган усулнинг афзаллиги шундаки, фильтрлаш қоидалари наборидаги аномалияларни аниқлайди ҳамда фильтрлаш қоидалари наборини ишлаб чиқиш жараёнини ҳам соддалаштиради. Таклиф этилган усулни амалга оширишда тармоқ трафигини ушлаб олиш модули, расмий қоидалар генерацияси модули ва тармоқ пакетларининг ажратиш модулидан фойдаланилади. Натижада аномалияларини аниқлаш усули қоидаларни нотўғри созлаш билан боғлиқ ахборот хавфсизлиги хавф-хатарларини ва фильтрлаш қоидаларида аномалиялар сонини камайтириш имконини беради.

Калит сўзлар: аномалия, фильтр, Rootkit, DoS, DDoS, TCP SYN Flood, Ping of Death, Tribe Flood Network (TFN), Stacheldraht, IP Spoofing.

Трафикни фильтрлаш қоидаларини тузишда унинг мураккаблигини асословчи бир қатор омиллар мавжуд: кўп сонли алоҳида узеллар ва тармоқда ишлашдаги ҳужжатларнинг йўқлиги ҳамда трафикни фильтрлаш қоидалар синтаксисининг турлилиги. Тажрибадан маълумки, ҳатто малакали мутахассислар ҳам аномалиялар ва турли қоидалар орасида номутаносиблик пайдо бўлишига олиб келувчи тармоқлараро экран қоидаларини конфигурациялашда йўл қўядилар.

Тармоқ трафигида аномалиялар сабаблари ва манбалари. Жорий вақт онида тизимни нотўғри ишлашига ўзини кўрсатадиган ва жорий вақт онида ўзини кўрсатадиган белгиларга эга бўлмаган, лекин маълум вақт ўтгандан кейин тизимни узилишига олиб келадиган аномалиялар мавжуд. Бунда тармоқ ҳужумини амалга ошириш натижасида пайдо бўлувчи аномалиялар хавфлироқдир [1-2-3]. Жадвалда тармоқ трафигида аномалияларни пайдо бўлиш сабаблари ва оқибатлари тавсифланган.

Тармоқ трафигида аномалияларнинг пайдо бўлиш сабаблари ва оқибатлари

1-жадвал

Аномалиянинг пайдо бўлиш сабаблари	**Аномалиянинг пайдо бўлиш кўриниши**	**Оқибатлар**
Иловалар даражасидаги ҳужумлар.	Дастурий таъминотдаги хатоликлар ва маълум заифликлар эксплуатацияси, заиф иловалар билан ассоцияланган портларни сканерлаш ва улардан фойдаланиш.	Нияти бузуқ тармоқдан фойдаланиши мумкин, имтиёзларини ошириши ва маъмурий фойдаланишга эга бўлиши мумкин.
Автороутерлар (бузиш жараёнини автоматлаштирадиган дастур).	Оқим бўйича трафикни ўзгариши.	Суқилиб кириш жараёнини автоматлаштириш учун Rootkit ни ўрнатиш ва тизимдан фойдаланиш нияти бузуқга қисқа вақтда юз минглаб тизимни сканерлаш имконини беради.
DoS ва DDoS хилидаги ҳужумлар.	Маршрутизаторлар ва серверлар портларига кўплаб IP-адреслардан трафикнинг жадал оқими кузатилади.	Тизимнинг нормал ишлаши бузилади, тармоқ, операцион тизим ёки иловалар ишлаши учун одатда керакли ресурсларни етишмаслигини тўлдирадиган сервислар ва маълумотларнинг фойдаланувчанлиги бузилади.
TCP SYN Flood.	Қисман очиқ уланишларнинг катта сонининг	Тизимнинг нормал ишлашини бузилиши.

	яратилиши, SYN-пакетлар сонининг ошиши.	
Ping of Death ҳужумлари.	Ниҳоятда кўп IP-пакетларнинг қабул қилиниши.	Тизимнинг адашиши, ишлашдан бош тортиши, осилиб қолиши ва қайта юкланиши.
Tribe Flood Network (TFN) ва Tribe Flood Network (TFN2K).	Манбанинг ўзгартирилган IP-адресларидан пакетларни генерациялаш, манбанинг портлари ва IP-адресларида пакетлар ҳажмининг динамик ўзгариши, трафикда битта IP-адресга кўп сонли пакетларни пайдо бўлиши.	Битта ёки бир нечта мақсадли кўплаб манбалардан одатий ишга туширилувчи мувофиқлаштирилган DoS-ҳужумларнинг тақсимланган асбобий воситалари ҳисобланади.
Stacheldraht ҳужуми.	Ноқонуний шифрланган трафик манбасининг ўзгартирилган IP-адресли пакетларини генерациялаш, манбанинг портлари ва IP-адресларида пакетлар ҳажмининг динамик ўзгариши, трафикда битта IP-адресга кўп сонли пакетларнинг пайдо бўлиши.	Ҳужумда улардан кейинчалик фойдаланиш учун кўп сонли тизимларга бузиб кириш рўй беради. Бундан кейин бир ёки бир неча объектларга ҳужум қилиш учун эгалланган тизимлардан фойдаланиладиган DoS-ҳужум фазаси келади.
IP Spoofing ҳужумлари.	Манба IP-адресларини ишончли зонадаги адресларга ўзгартириш.	Тармоқ ичида ёки ташқарисида нияти бузуқ ўзини ишончли компьютер қилиб кўрсатади.
«Man-in-the-middle» ҳужумлари.	Тармоқ пакетлари, маршрутлаш ва транспорт протоколларини ушлаб олиш, узатилувчи маълумотларни бузилиши ва тармоқ сессиясига янги ахборотни киритиш.	Ахборотни ўғирлаш, шахсий тармоқ ресурсларидан фойдаланиш учун жорий алоқа сеансини бузиш, тармоқ ва фойдаланувчилар ҳақида ахборот олиш учун трафикни таҳлил этиш, DoS-ҳужумлар, тармоқ сессияларига янги ахборотни киритиш ва узатилаётган маълумотларни бузиш.
Тармоқ разведкаси.	DNS-серверига сўров юбориш, портлар ва IP-адреслар диапазонини сканерлаш.	Нияти бузуқлар хостларда амалга ошираладиган иловар хусусиятларини ўрганишлари ва очиқ портларни топишлари мумкин.
Пакетларни снифферлаш.	Тармоқ орқали очиқ ҳолда юборилувчи пакетларни ушлаб олиш (Telnet, FTP, SMTP, POP3 ва бошқа хизматлар), масалан фойдаланувчилар номлари ва пароллари, трафик оқимини бир тармоқ қурилмасидан (хизматлар) бошқасига кўчириш.	Нияти бузуқ тизимли фойдаланувчининг қайд ёзувидан фойдаланиши мумкин.
Паролларга ҳужумлар.	IP-пакетларни сохталаштириш ва пакетларни эшитиш, оқим бўйича трафикни ўзгариши.	Нияти бузуқлар бузиб олинган маълумотларни мумкин бўлган кейинги ўзгаришларига боғлиқ бўлмаган ҳолда тармоққа киришларини таъминлаши мумкин.
Қайта йўналтирилган портларга ҳужумлар.	Тармоқ трафигини қайта адреслаш, трафикнинг битта оқимида пакетларда ёки байтларда пасайиш.	Нияти бузуқлар томонидан тармоқлараро экран орқали норасмий трафикнинг узатилиши.
Вирусли ва троян ҳужумлари.	Трафикда асосий бўлмаган белгиланган адресни олиб ташлаш.	Вирусга аниқлаши мумкин бўлган, яъни command.com файлининг барча бошқа версияларини зарарлайдиган ва баъзи тармоқ файлларини ўчирадиган дастур мисол бўла олади.
Ишончли мулклардан фойдаланишдаги ҳужумлар.	Тармоқ ташқарисида кимдир ишончли муносабатлар устунлигидан фойдаланганда юз беради.	Ички тармоққа ҳужум.

Аномалияни аниқлаш масаласининг наборида катта миқдордаги қоидалар вақтинчалик ресурсларни талаб қилиши мумкин, ҳамда бу масалани ҳал қилувчи мутахассиснинг хатоликни ўтказиб юбориши ёки хатолик юз бермаган жараённи хато деб ҳисоблаши эҳтимоллиги ҳам мавжуд [4-5-6.]. Ушбу масалаларни ечиш учун трафикни махсус фильтрлаш қоидалари аномалиясини аниқлаш усули таклиф этилган.

Таклиф этилаётган усулнинг мавжуд усуллардан фарқли томони шундаки, таклиф этилаётган усул нафақат фильтрлаш қоидалари наборидаги аномалияларни аниқлайди, балки фильтрлаш қоидалари наборини ишлаб чиқиш жараёнини ҳам соддалаштиради.

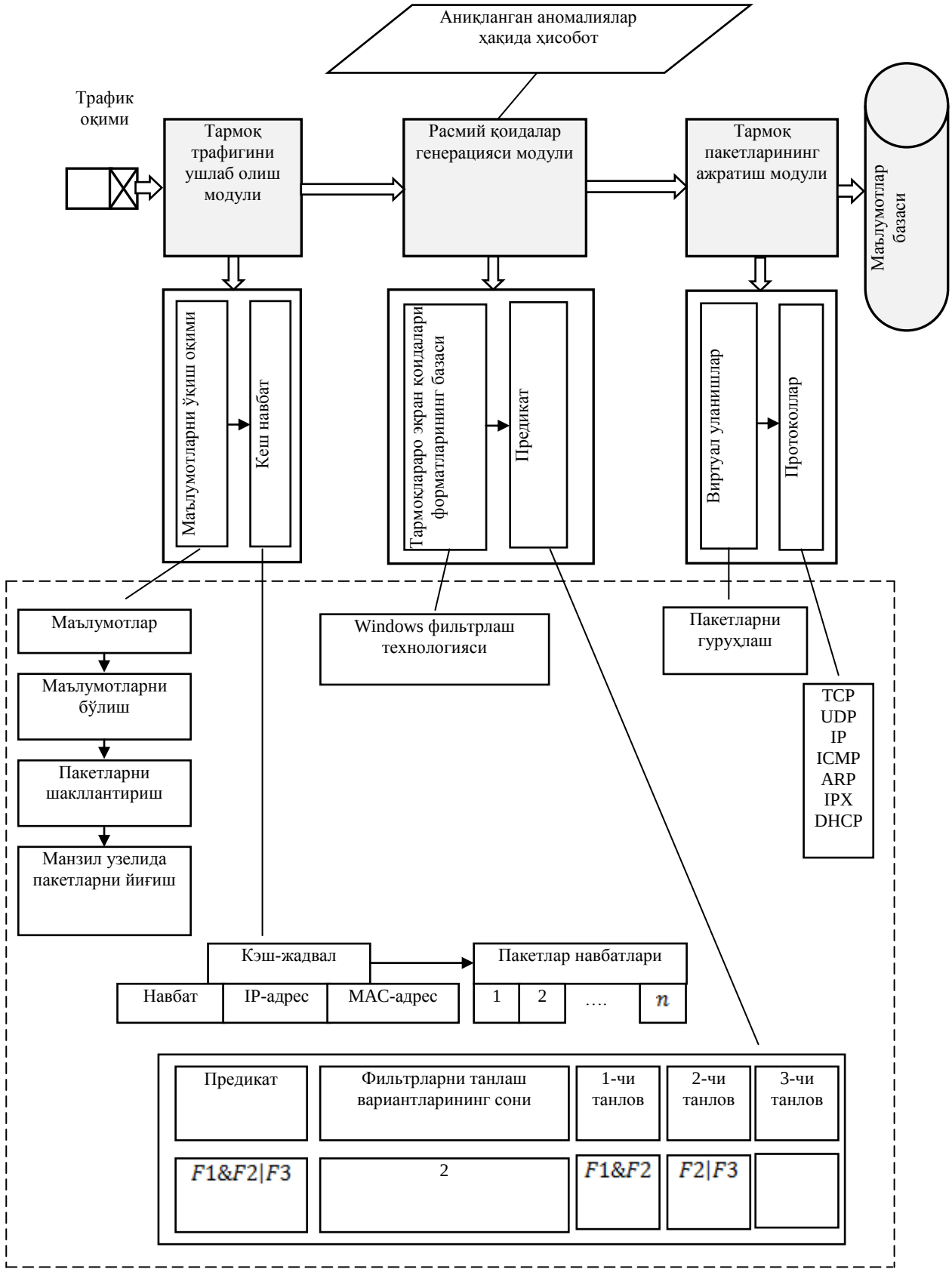
Таклиф этилган усулни амалга ошириш қуйидаги кетма-кет бажариладиган модуллардан иборат:

- тармоқ трафигини ушлаб олиш модули;
- расмий қоидалар генерацияси модули;
- тармоқ пакетларининг ажратиш модули.

Расмда трафикни махсус фильтрлаш қоидаларида аномалияларни аниқлаш модулларининг ўзаро таъсир схемаси келтирилган.

Тармоқ трафигини ушлаб олиш модули. Тармоқ трафигини ушлаб олиш модули ёрдамида

ушлаб олинган пакетлар расмий қоидалар генерацияси модулининг киришига келиб тушади. Кейин пакетлар расмий қоидалар генерацияси модулига, яъни аниқ бир тармоқлараро экран моделига боғланмаган қоидаларда шаклланади.[6]



1-расм. Трафикни махсус фильтрлаш қоидаларида аномалияларни аниқлаш модулларининг ўзаро таъсир схемаси

Расмий қоидалар генерацияси модули. Қоидаларни расмий кўринишда шакллантириш

жараёнида тармоқлараро экран қоидалари форматлари тавсифи кутубхонасидаги ахборотдан фойдаланилади. Тармоқлараро экран қоидалари формати расмий қоидаларни муайян бир тармоқлараро экран форматига ўтказувчи схемага эга XML-файлни ўз ичига олади. Фильтрлаш набори тўпламининг иккилик форматига эга ва уни матнли форматда экспорт/импорт қилиш имкониятини таклиф этмайдиган бир қатор тармоқлараро экранлар учун форматлар базасида нафақат XML-файлни ўзгартириш схемалари қатнашади, балки қоидалар тўпламининг иккилик форматини матнли ва тескари форматга ўзгартириш имконини берувчи функциялар кутубхонаси ҳам бўлиши мумкин. Агар мададловчи тизимда зарурий тармоқлараро экран бўлмаса, фойдаланувчи мустақил равишда XML-файлларни яратиш ва кутубхоналарни ўзгартириш имкониятига эга бўлади. Бундан кейин фильтрлар тўплами орасида фильтрлаш қоидаларининг тақсимланиши юз беради:

1. Агар қоида рухсат берувчи бўлса, бу қоида ҳар бир фильтрга қўшилиши керак.
2. Агар қоида тақиқловчи бўлса, кетма-кет фильтрлар занжири учун битта қоида етарли ва параллел фильтрлар занжири учун ҳар бир занжирдаги битта фильтрга қоида қўлланилиши етарли ҳисобланади.[5-6]
3. Агар қоида тақиқловчи бўлса, унга фильтрларнинг предикат формаларини аниқлаш керак. Битта занжирдаги фильтрлар учун исталган фильтрларга қоидалар қўлланилади ва бу ерда фильтрлар ЁКИ(|) орқали предикатда ёзилади. Параллел занжирлардаги фильтрлар учун қоидалар ҳар бирига қўлланилади ва бу ерда фильтрлар ВА(&) орқали предикатда ёзилади. Қабул қилинган расмий қоидалар тўплами таҳлил қилинади ва шундан сўнг аниқланган аномалиялар ҳақида ҳисобот шакллантирилади.

Тармоқ пакетларининг ажратиш модули. Тармоқ пакетларининг ажратиш модулида виртуал уланишлар бажарилади. Ҳар бир виртуал уланиш тугаши билан манба ва манзил IP-адрес, манба ва манзил порт, трафикни узатиш/қабул қилиш ҳажми маълумотлар базасида сақланади. Бундан фақат ICMP ва ARP пакетлари мустасно – улар ҳақидаги маълумотлар виртуал уланишларни бирлаштирмасдан базада сақланади. Маълумотлар базаси SQL-сўровлар ёрдамида амалга оширилади, бу SQL тилидан тўлиқ даражада ва барча имкониятларидан фойдаланиш имкониятини яратади. Таҳлил этилаётган тармоқ трафигини ушлаб олиш нуқтасида, маълумотлар базасига керакли сўровларни шакллантириб фильтрлаш қоидалари наборини қуриш учун барча керакли ахборотни олиш мумкин.

Шундай қилиб, таклиф этилаётган трафикни махсус фильтрлаш қоидаларида аномалияларини аниқлаш усули қоидаларни нотўғри созлаш билан боғлиқ ахборот хавфсизлиги хавф-хатарларини ва фильтрлаш қоидаларида аномалиялар сонини камайтириш имконини беради.

Адабиётлар

1. Wool A. A quantitative study of firewall configuration errors // IEEEComputer Society. Vol.37. 2004. –P.62-67.
2. Марьенков А.Н., Ажмухамедов И.М., «Обеспечение информационной безопасности компьютерных сетей на основе анализа сетевого трафика», Вестник АГТУ. Серия «Управление, вычислительная техника и информатика» №1 / 2011 г. – С.141-148.
3. Оладько В.С., Микова С.Ю., Нестеренко М.А., Садовник Е.А. Причины и источники сетевых аномалий // Молодой ученый. – №22. 2015 г. – С.158-161.
4. Микова С.Ю., Оладько В.С. Обзор алгоритмов выявления сетевых атак// Актуальные проблемы гуманитарных и естественных наук. 2015. №9-1. – С.59-62.
5. Шелухин О.И., Сакалема Д.Ж., Филинова А.С. Обнаружение вторжений и компьютерные сети // О.И. Шелухин — М.: Горячая линия-Телеком, 2013 г. – С.220.
6. Гольдштейн Б.С. Протоколы сети доступа. Том 2.3 – е издание–СПб.: БХВ-Петербург, 2014 г. – С.288.

Ғуломов Шерзод Ражабоевич
техника фанлари доктори (PhD), ТАТУ “Ахборот хавфсизлигини таьминлаш” доценти в.б., Тел: +998(90)9708464
Эл почта: sherhisor30@gmail.com
Ахмедова Наима Қодировна
ТАТУ “Ахборот хавфсизлиги” I- курс магистранти, Тел: +998(90)3554232
Эл почта: naima212@mail.ru

Method for detection anomalies on specific traffic filtering rules

Abstract: In this article the reason appearance and consequences of anomalies in the network traffic has been described. To solve these problems a method for detecting an anomaly of traffic filtering is proposed. It is preferable that filtering rules define deviations and simplify the process of developing filtering rules. The proposed method uses a network traffic management module, a code generation module and a network packet distribution module. As a result, a method for detecting an anomaly allow reduce the number of anomalies in

information security risks and filtering rules associated with improperly configured.

Keywords: anomaly, Filter, Rootkit, DoS, DDoS, TCP SYN Flood, Ping of death, Tribe flood Network (TFN), Stacheldraht, IP Spoofing.

УДК 681.5.015.3

Ш.С.Каримов

ИНФОРМАЦИОННАЯ МОДЕЛЬ ТЕХНОЛОГИЧЕСКОГО МОНИТОРИНГА ПАРАМЕТРОВ НЕФТЕПЕРЕРАБАТЫВАЮЩИХ ПРЕДПРИЯТИЙ

В работе предлагается разработка информационной системы мониторинга состояния технологических агрегатов в составе АСУ. Предложена информационная модель системы, которая отображает основные информационные потоки, а также их взаимодействие и функции для решения задач технической диагностики технологических агрегатов нефтеперерабатывающих предприятий.

Ключевые слова: информационная модель, нефтеперерабатывающие предприятия, технологические агрегаты, мониторинг, декомнозиция.

Одной из характерных тенденций развития научных исследований является появление и использование информационно-технических систем большой сложности. Важным классом данных систем являются информационные системы мониторинга, обеспечивающие сбор и предварительную обработку данных, отражающих определенные характеристики состояния объекта наблюдения с последующей их передачей конечному множеству заинтересованных клиентов. В данном контексте одной из основных задач является построение информационной модели системы, обеспечивающей автоматизацию процессов предварительной обработки данных и информации, управления информацией и генерации рекомендаций о состоянии объекта исследования.

Проектирование информационной модели систем мониторинга состояния технологических агрегатов основано на принципе декомпозиции [1,2], как структуры рассматриваемой системы, так и ее функций. Процесс декомпозиции можно выразить в виде:

$$L \to \min \to D^* \text{ при}$$
$$D \in \{D\}, \quad D_i \cap D_j = 0, \quad i \neq j, \qquad (1)$$

где D - операция декомпозиции;

$\{D\}$-множество семейств декомпозиции;

D^* -оптимальная декомпозиция;

L - множество возможных принципов и алгоритмов, используемых для построения информационной системы мониторинга технологических агрегатов.

Для применения принципа декомпозиции будем рассматривать информационную систему (ИС) в виде совокупности основных подсистем, обеспечивающих выполнение определенных задач автоматизированной технической диагностики технологических агрегатов, представленной в виде:

$$IS = \langle ss^g, ss^{proc}, ss^{db}, ss^r, SS^{af} \rangle, \quad (2)$$

где ss^g - подсистема сбора первичной информации о технологических агрегатах;

ss^{proc} - подсистема обработки сообщений и управления ИС;

ss^{db} - подсистема хранения информации, касающейся диагностики технологических агрегатов и функционирования АСУ;

ss^r - подсистема создания отчетов, протоколирования и отображения информации о диагностируемом технологическом агрегате и функционирующей ИС;

SS^{af} - множество подсистем автоматизации функций мониторинга состояния технологических агрегатов:

$$SS^{af} = \{ss_{ip}^{af}, ss_{con}^{af}, ss_{dss}^{af}, ss_{prog}^{af}\}, \qquad (3)$$

где ss_{ip}^{af} - подсистема обработки изображений технологических агрегатов;

ss_{con}^{af} - подсистема определения состояния технологических агрегатов;

ss_{dss}^{af} - подсистема генерации управляющих рекомендаций при диагностике состояния технологических агрегатов;

ss_{prog}^{af}- подсистема прогнозирования изменения параметров технологических агрегатов.

Подсистему обработки сообщений и управления ИС будем рассматривать в следующем виде:

$$ss^{proc} = \{I^x, I^y, F, M, E, \Psi, A\}, \qquad (4)$$

где I^x - множество входных информациионных потоков;

I^y - выходной информационный поток;

F - множество функций отображения множества сообщений на множестве событий;

M - множество сообщений ИС;

E - множество событий ИС;

Ψ - модель выработки управлений;

A - множество управляющих воздействий.