ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ
«АЛМАТЫ ЭНЕРГЕТИКА ЖӘНЕ БАЙЛАНЫС УНИВЕРСИТЕТІ»
коммерциялық емес акционерлік қоғамы
«Ақпараттық қауіпсіздік жүйелері» кафедрасы

«ҚОРҒАУҒА ЖІБЕРІЛДІ»
Кафедра меңгерушісі с.ғ.к., доцент Бердібаев Р. Ш.
_____ «_____» _____ 2019 ж.
(қолы)

ДИПЛОМДЫҚ ЖОБА

Тақырыбы: «Ақпарат пен оқиғалар қауіпсіздігін басқару жүйесінің (SIEM-система) деректерді жинау және алдын ала өңдеу компонентін құру»
Мамандығы: 5В100200 – «Ақпараттық қауіпсіздік жүйелері»
Орындаған: Уәрбеков Ә. Б. Тобы: СИБк-15-1
Ғылыми жетекші: т.ғ.к., доцент, Омар Тұрғанбек Қалиұлы

Кеңесшілер:
Экономикалық бөлім бойынша:
_____
(ғылыми дәрежесі, атағы, аты-жөні)
_____ «06» 05 2019 ж.
(қолы)

Тіршілік қауіпсіздігі бөлімі бойынша:
_____
(ғылыми дәрежесі, атағы, аты-жөні)
_____ «22» 04 2019 ж.
(қолы)

Есептеу техникасын қолдану бойынша:
_____
(ғылыми дәрежесі, атағы, аты-жөні)
_____ «20» 05 2019 ж.
(қолы)

Мөлшер бақылаушы:
_____
(ғылыми дәрежесі, атағы, аты-жөні)
_____ «03» 06 2019 ж.
(қолы)

Пікір беруші:
_____
(ғылыми дәрежесі, атағы, аты-жөні)
_____ «_____» _____ 201__ ж.
(қолы)

Алматы 2019

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ
«АЛМАТЫ ЭНЕРГЕТИКА ЖӘНЕ БАЙЛАНЫС УНИВЕРСИТЕТІ»
коммерциялық емес акционерлік қоғамы

Басқару және ақпараттық технологиялар институты
Ақпараттық қауіпсіздік жүйелері кафедрасы
5В100200 – «Ақпараттық қауіпсіздік жүйелері» мамандығы

Дипломдық жобаны орындауға берілген
ТАПСЫРМА

Студент: Үзбеков Энеман
(аты-жөні)

Жобаның тақырыбы: ______________________________

2018 ж. «___»____ №____ универститет бұйрығымен бекітілді.

Аяқталған жұмысты тапсыру мерзімі: «____»______________20___ ж.

Жобаға алғашқы деректер (талап етілетін зерттеу (жоба) нәтижелерінің параметрлері және зерттеу нысанының алғашқы деректері): Қолданыстағы SIEM-жүйелердің қалыпқа келтіру компоненті (нормализация) жасаудың даму жолдарын іздестіру. Антивирустар, маршрутизаторлар, желіаралық экрандар, операциялық жүйелер және т.б. әртүрлі құрылғылар мен қосымшалардан келуші деректерді (лог-файлдарды) талдау. Киберқауіпсіздікке оқиғаны анықтауға қажетті деректерді бірыңғай форматқа келтіру. Деректерді қалыпқа келтіру қызметі үшін бағдарлама жасау.

Диплом жобасындағы әзірленуі тиіс мәселелер тізімі немесе диплом жобасының қысқаша мазмұны:
1. Аса маңызды инфрақұрылым;
2. SOC жүйесінің құрылымын және функциясын талдау;
3. SIEM жүйесінің функционалдық қызметін талдау;
4. Корреляция алгоритмін талдау;
5. Жүйені басқарушы ақпараттық-бағдарламалық құралдардың лог-файлдарын талдау, қалыпқа

келтіру форматын жасау;
6. Қайтадан келтіру компонентінің жұмыс алгоритмін әзірлеу және Python тілінің құралдарын қолдана отырып іске асыру;
7. Техникалық-экономикалық негіздеме;
8. Өміртіршілік қауіпсіздігі;
9. Қорытынды

Графикалық материалдардың (міндетті түрде дайындалатын сызбаларды көрсету) тізімі:
1. SIEM жүйесінің функционалдық құрылымы;
2. Лог-файлдарды өңдеу процесі;
3. Деректерді жасаған формат сұлбасы;
4. Бағдарламаның блок-сұлбасы;
5. Шыңдар диаграммасы

Негізгі ұсынылатын әдебиеттер:

1. Котенко И.В., Федорченко А.В., Саенко И.Б., Кушнеревич А.Г. Технологии больших данных для корреляции событий безопасности на основе учета типов связей // -М: изд. Кибер, 2017. №5(24) 2-16б.
2. Федорченко А.В., Левшун Д.С., Котенко И.В. Анализ методов корреляции событий ИБ в SIEM // - СПб.: изд. Петр, 2016 208б.
3. Ерохов А.Л., Карасёв С.В., Подход к формированию модели данных событий ИБ // -Воронеж: изд. Сара, 2017, 124-129б.

Жоба бойынша жобаның бөлімдеріне қатысты белгіленген кеңесшілер

Бөлімдері	Кеңесшілері	Мерзімі	Қолы
	Омар Т.К		[signature]
	Аренбаева Ж.Г.	04.03-08.05.19	[signature]
	Торгаев Д.Д.	01.04-22.04	[signature]

Диплом жобасын дайындау
КЕСТЕСІ

Бөлімдердің атауы, әзірленетін мәселелердің тізімі	Ғылыми жетекшіге ұсыну мерзімдері	Ескерту
1. Іс шаралар спецификациясы	14.02.2019	
2. SOC жүйесінің құрылымын және функциясын талдау	27.02.2019	
3. SIEM жүйесінің функционалдық қосымшын талдау	06.03.2019	
4. Корреляция алгоритмін жаз	12.03.2019	
5. Жүйені басқарудың аппаратты-бағдарламалық құрылғының log-файлдарын талдау, қалыпқа келтіру фрагментін талдау	17.03.2019	
6. Қалыпқа келтіру компонентінің жұмыс алгоритмін құрып және Python тілінің құралдарын қолдана отырып іске асыру	03.04.2019	
7. Техникалық-экономикалық негіздеме	22.04.2019	
8. Өнірлік қауіпсіздігі	06.05.2019	
9. Қорытындылау, жұмыс нәтижесі	21.05.2019	

Тапсырманың берілген уақыты «_____»_____20___ж.

Кафедра меңгерушісі _____ (с.ғ.к., доцент Бердібаев Р.А.)
(қолы) (аты-жөні)

Жобаның
ғылыми жетекшісі _____ (т.ғ.к., доцент Омар Т. Қ.)
(қолы) (аты-жөні)

Орындалатын тапсырманы
қабылдаған студент _____ (Урбеков Д. Б.)
(қолы) (аты-жөні)

АҢДАТПА

Дипломдық жұмыс «Ақпарат пен оқиғалар қауіпсіздігін басқару жүйесінің (SIEM-система) деректерді жинау және алдын ала өңдеу компонентін құру (жасау)» тақырыбына арналған. Бұл дипломдық жұмыс аса маңызды объектілер бөлімінен, SIEM-жүйесі бөлімінен, бағдарламалық бөлімнен, өмір тіршілік қауіпсіздігі бөлімінен және экономикалық бөлімнен тұрады.

Аталған жұмыста SIEM-жүйесінің компонеттерінің қызметі талданып, қалыпқа келтіру кызметінің функционалына айрықша назар аударылды. Деректерді жинақтаушы бағдарламалар талданып, қалыпқа келтіру қызметі үшін бағдарламалық шешім ұсынылды. Бағдарламалық шешім Python 3.6 бағдарламалық тілінде жазылды. Бағдарламаның негізгі қызметі ретінде әр түрлі дерек көздерінен келген логтарды бір форматқа келтіру болып алынды. Логтарды өңдеуге дейін бірыңғай форматтағы логтарды жеке бөлу қарастырылған.

АННОТАЦИЯ

Дипломная работа посвящена теме «Разработка компонента сбора и предварительной обработки данных системы управления информацией и событиями безопасности (SIEM-система)». Дипломная работа состоит из раздела наиболее важных объектов, раздела SIEM-системы, программного раздела, раздела безопасности жизнедеятельности и экономической части.

В данной работе особое внимание было уделено функционалу нормализации и анализу деятельности компонентов SIEM-системы. Были проанализированы и представлены программные решения для службы восстановления данных. Программное решение написано на программном языке Python 3.6. Основной функцией программы является нормалицаия логов из различных источников в один формат. До обработки логов предусматривается отдельное разделение логов на схожие форматы.

ANNOTATION

The thesis is devoted to the topic “Development of a component for the collection and preprocessing of data management information systems and security events”. The thesis consists of the section of the most important objects, the section of the SIEM system, the program section, the section of life safety and the economic part.

In this paper, special attention was paid to the functional normalization and analysis of the activities of the components of the SIEM system. Software solutions for data recovery services were analyzed and presented. The software solution is written in Python 3.6 software. The main function of the program is normalits logs from various sources in one format. Prior to log processing, a separate log separation is provided for similar formats.

Мазмұны

Кіріспе

Жаһандық ақпараттандыру қазіргі уақытта әлемдік қоғамдастық мемлекеттерінің өмір сүруі мен тіршілік әрекетін белсенді басқарады, Ақпараттық технологиялар ұлттық, әскери, экономикалық қауіпсіздікті қамтамасыз ету міндеттерін шешу кезінде қолданылады. Сонымен қатар, мемлекеттік және әскери құрылымдар Ғаламдық ақпараттандырудың іргелі салдарының бірі мемлекеттердің жаңа ортада бәсекелесуі туындауы, және ол - киберкеңістік, географиялық болып табылмайды, бірақ толық көлемде халықаралық болып табылады.

Жаһандық киберкеңістікті қалыптастыру процесінде әскери және азаматтық компьютерлік технологиялардың конвергенциясы жүреді,жетекші шет мемлекеттерде әлеуетті қарсыластардың ақпараттық инфрақұрылымына белсенді әсер етудің жаңа құралдары мен әдістері қарқынды әзірленуде, түрлі мамандандырылған кибернетикалық орталықтар мен басқару және басқару бөлімшелері құрылады, олардың негізгі міндеті мемлекеттік және әскери Ақпараттық инфрақұрылымды қорғау, қарсыластың ақпараттық жүйелерінде белсенді деструктивті іс-қимылдарды дайындау және өткізу болып табылады. Мәселен, жеке ресми киберәскер АҚШ, Қытай, Англия, Франция, Германия, Израиль және басқа да бірқатар мемлекеттерде бар.

Киберқауіпсіздік – бұл цифрлық шабуылдардан жүйелерді, желілерді және бағдарламалық қосымшаларды қорғау жөніндегі шараларды іске асыру. Мұндай шабуылдар әдетте құпия ақпаратқа қол жеткізуге, оны өзгертуге және жоюға, пайдаланушылардан ақша бопсалауға немесе компаниялардың қалыпты жұмысын бұзуға бағытталған.

Киберқауіпсіздік – қоғамның барлық топтарын қозғайтын мемлекеттік маңызы бар стратегиялық проблема. АҚШ-тың киберқауіпсіздіктің мемлекеттік саясаты (National Cyber Security Strategy - NCSS) мемлекеттің ақпараттық жүйелерінің қауіпсіздігі мен сенімділігін күшейту құралы болып табылады. АҚШ-тан кейін, киберқауіпсіздік стратегиялары Канадада, Жапонияда, Үндістанда, Австралияда, Жаңа Зеландияда, Колумбияда және кейбір басқа мемлекеттерде қабылданды. Киберқауіпсіздік стратегиясына Еуроодақ мүше елдердің қатарына Швеция (2008 ж.), Эстония (2008 ж.), Финляндия (2008 ж.), Словакия (2008 ж.), Чехия (2011 ж.), Франция (2011 ж.), Германия (2011 ж.), Литва (2011 ж.), Люксембург (2011 ж.), Голландия (2011 ж.), Ұлыбритания (2011 ж.) қабылданды. Елдер тізімі киберқауіпсіздік проблемасы бүкіл әлемде маңызды болып танылатынын айқын көрсетеді.

Ресей ФҚҚ-ның кибершабуылдардан Ақпараттық жүйелерді қорғауды жетілдіру жөніндегі жұмысы шеңберінде ГосСОПКА жүйесі жетілдірілуде. Бұл аббревиатура компьютерлік шабуылдардың салдарын анықтау, алдын алу және жою мемлекеттік жүйесі ретінде түсіндіріледі. Өзінің мәні бойынша ГосСОПКА – бұл өзіндік антихакерлік құрылым, компьютерлік инциденттер, осалдықтар және хакерлік шабуылдар туралы деректерді сақтау, сондай-ақ

ақпараттық желілерді қорғау жоспарында өз қатысушылары үшін ұсынымдар мен қауіпсіздік шараларын әзірлеуші.

Бұл құрылымды құрудың мақсаты-әртүрлі компьютерлік инциденттер туралы барлық ақпаратты жинақтау, осындай сыртқы шабуылдарға қарсы әрекет ету бойынша шаралар әзірлеу, сондай-ақ киберқылмыскерлердің іс-қимылдарымен байланысты салдарларды жою немесе азайту бойынша ұсынымдар. Идеяның негізіне басқа мемлекеттердің осындай шешімдері алынды, олар мамандарға деректерді орталықтандырып жинауға және талдауға, ал талдау негізінде аса маңызды Ақпараттық жүйелерді қорғау үшін шешімдер әзірлеуге мүмкіндік берді.

1 Аса маңызды объектілердегі киберқауіпсіздік

"Аса маңызды объектілер" ұғымы жұмыс істеуінің бұзылуы (немесе тоқтатылуы) елдің, субъектінің немесе әкімшілік-аумақтық бірліктің экономикасын басқаруды жоғалтуға, оның биржола теріс өзгеруіне (немесе бұзылуына) немесе осы аумақтарда тұратын халықтың тіршілік әрекетінің қауіпсіздігінің елеулі төмендеуіне әкеп соқтыратын объектілерді білдіреді.

Кез келген индустриялық дамыған елдің аса маңызды объектілерінің тізбесі мыңдап есептеледі. Бұған атом электр станциялары, ядролық отын, мұнай-газ, энергетикалық және қорғаныс кешендерінің объектілері, ірі инженерлік құрылыстар, гидротораптар, Металлургиялық және химиялық өндірістер, су үсті, әуе және құбыр көлігі және т. б. кіреді.

Елдің аса маңызды объектілерінің қауіпсіздігі үшін өзекті шешімдерді іске асыра отырып, терроризмге қарсы тұрақтылық - бұл ең алдымен, террористік актілердің алдын алу. Террористік актілердің алдын алу жөніндегі іс-әрекеттегі басым бағыттар:

- террористік шабуылдардан аса маңызды объектілердің қорғалуын бағалау;
- объектілердің терроризмге қарсы қорғалуын кешенді талдау негізінде террористік қатерлерді болжау және террористік актілерге қарсы іс-қимылдың тиімділігін бағалау;
- террористік акциялардың жолын кесудің заманауи тиімді техникалық құралдарын және жүйелерін құру [1].

Аса маңызды нысандардың АТ-инфрақұрылымының сыртқы периметрі неғұрлым осал болып табылады, өйткені оған технологиялық процесті басқарудың автоматтандырылған жүйелерін бұзуға бағытталған шабуылдардың ең көп үлесі тиесілі. Екінші кезекте басқарудың барлық автоматтандырылған жүйесі жұмысына жауап беретін АТ-инфрақұрылымының сыни элементі ретінде басқару серверлері осал.

Сонымен қатар, технологиялық процестер операторларының АЖО қорғау қажет. Статистикаға сілтеме жасай отырып, дәл осы жұмыс орындары ең осал болып табылады деп айтуға болады, бұл ең алдымен олардың жұмыс істеу режиміне байланысты. Олар операциялық жүйелерді, қолданбалы және қорғау БҚ жаңартуға уақыт қалдырмай, тәулік бойы жұмыс істеуі тиіс, бұл үшін АЖО жүйелерін қайта жүктеу қажет. Сондықтан мұндай жаңартулар жылына бір-екі рет пайда болуы мүмкін технологиялық терезелер кезінде ғана жүзеге асырылады. Кең таралған АЖО осалдығына кіру парольдерінің төмен күрделілігі немесе толық болмауы да жатады.

Шабуылдың басқа ықтимал векторы корпоративтік және технологиялық сервистер мен ақпараттық жүйелер үшін ортақ желілік инфрақұрылым болып табылады. Мұндай жағдай зиянкестерге корпоративтік және керісінше технологиялық желіге шабуыл жасауға мүмкіндік береді. Желілік жабдықтың осалдығы жақсы сипатталған, ал оның жаңарту шектеулері технологиялық процесс операторларының АЖО сияқты болып табылады.

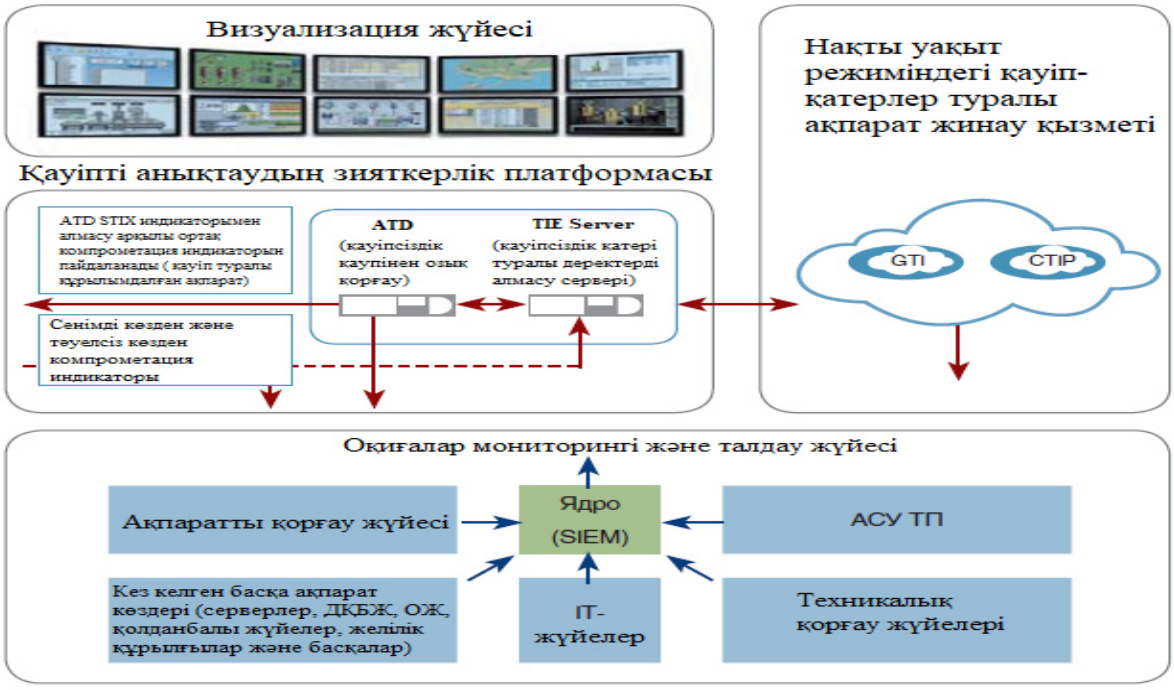
Виртуалдау ҚТ-да әлі кең қолданылуда, бірақ АТ саласындағы үрдістер жақын арада және онда виртуализацияланған орталарға тән өзекті қауіптер болатыны туралы айтады: технологиялық және басқа да АТ-ресурстарды бірыңғай виртуалды ортада пайдаланған жағдайда виртуалдандырудың жалпы платформасы арқылы корпоративтік сегменттерден технологиялық сегменттерге ену қатері туындайды.

Сарапшылар қашықтан қол жеткізу және басқару жағдайын теріс бағалайды. Жүйеге қызмет көрсету бойынша кейбір операциялар аутсорсингке беріледі, егер "корпоративтік желі – аутсорсер" жүйесі қорғалған деп санауға болса, онда аутсорсердің ат ортасының қорғалуына кепілдік беру қиын. Бұл аса маңызды нысандардың АТ-инфрақұрылымына шабуылдардың тағы бір векторын жасайды. Ал, алыстан кіру нүктесі (мысалы, басқару немесе техникалық қолдау үшін) қаскүнем тұрғысынан осал.

Аса маңызды объектілердің қорғалуын техникалық қамтамасыз етудің маңызды құрамдас бөліктерінің бірі техникалық құралдар мен қауіпсіздік жүйелері болып табылады. Қауіпсіздік жүйелерінің негізі ретінде SOC жүйесін қолдану қолайлы [2].

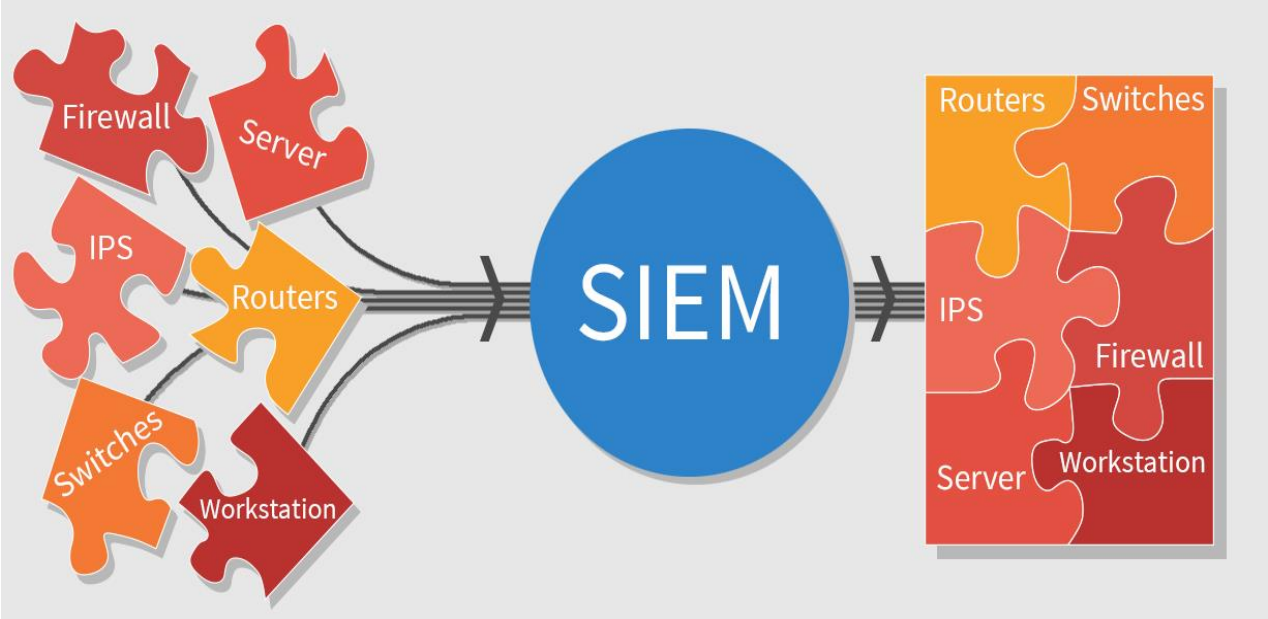
1.1 Security Operation Center

SOC – бұл ақпараттық қауіпсіздіктің критикалық инциденттеріне әрекет ету орталығы (АҚ), негізгі қызметі барлық деңгейлерінде шабуылдарды болдырмауды және толық мониторингті жүзеге асыруға мүмкіндік береді: желілік пакеттер, желілік ағындар, операциялық жүйенің белсенділігі, контент, пайдаланушылардың мінез-құлқы (1.1-сурет).



Сурет 1.1 – SOC платформасы

SOC платформасы әдетте SIEM-нің (1.2-сурет) бас тартуға төзімді конфигурациясына негізделген, оған шабуылдарды табумен және киберқылмысқа қарсы әрекет етумен айналысатын жетекші зертханалардан алынатын ақпараттық қауіпсіздіктің өзекті қатерлері туралы деректер көздері қосымша қосылған (IP, URL, бот-желілерде сенім туғызбайтын). Бұл қатерлер туралы ақпаратты біріктіруге, көп оқыс оқиғаларды анықтауға және ең қысқа мерзімде нөлдік күннің (zero day) шабуылдарын анықтауға мүмкіндік береді.Визуализация жүйесі мүдделі тұлғаларға операциялық және жиынтық ақпаратты шығаруға мүмкіндік береді.



Сурет 1.2 – SIEM жүйесінің қызметі

Қазіргі заманғы ақпараттық әлемнің болмысы SOC құрал-сайманына қосымша талаптар қояды. Олардың ең маңыздысы-үлкен деректердің инфрақұрылымы (big data). Компанияның барлық жүйелері генерациялайтын ақпарат көлемі баяғыда нашар құрылымдалған бытыраңқы массаны көрсете отырып, деректер терабайттарын аттай алады. Қазір оқиғалар мониторингін жүргізу жеткіліксіз – мақсатты шабуылдардан қорғау үшін қауіпсіздіктің бейімделген архитектурасын құру туралы көп айтылады. Gartner зерттеу және консалтинг компаниясының талдаушылары қорғауға қарағанда табу және жылдам әрекет ету жүйелеріне көбірек инвестиция салуды ұсынады; желілік қауіпсіздік, жұмыс станциялары мен қосымшалардың қауіпсіздігі үшін контекстік-бағытталған платформалар ұсынатын өндірушілерге артықшылық беру, сондай-ақ шабуылға талдау, болдырмау, анықтау және әрекет етуге біріктірілген көзқарас беру. Оқиға анықталғанға дейін оны тексеру үшін қандай деректер қажет екенін болжау қиын. Әртүрлі және байланысты емес ақпаратты жинау, талдау және сақтау маңызды. Осылайша, SOC техникалық құралы барлық технологияларды біріктіретін және түрлі жабдықтар мен ақпараттық жүйелерден жиналған жармалар бойынша жанама белгілер

бойынша шабуылдарды немесе зұлымдық қызметті анықтауға мүмкіндік беретін бірыңғай құралға айнала отырып, үлкен деректерді талдауға қабілетті болуы тиіс. Тек SOC құрамдас бөліктерінің (адамдар, технологиялар мен процестер) барлық үш тығыз өзара әрекеттесуі кезінде ғана қысқа мерзімде қауіпті анықтауға және бейтараптандыруға болады. Мысалы, SIEM жүздеген және мыңдаған құрылғылар мен жүйелерден миллион оқиғалар АҚ инциденттерін анықтайды. Бұл туралы мәліметтер талдаушыға оны жинауға, контексті анықтауға және бұзушылық фактісін анықтауға уақыт үнемдеуге мүмкіндік беретін байланысты ақпаратпен автоматты түрде толықтырылады.

Дұрыс құрылған жұмыс тәртібі бірнеше оқиғалардың өзара байланысын анықтауға мүмкіндік береді. Талдаушыға ұсынылған

өкілеттіктер мен алдын ала бекітілген іс-қимыл сценарийлері қысқа мерзімде қауіп-қатерге қарсы тұруға және одан әрі тергеуді ұйымдастыруға мүмкіндік береді.

1) "CSIRT" тарихи анықтамасына қайта қарай отырып, CSIRT деп есептелу үшін ұйым орындауы тиіс үш критерийді баяндайды. Біз оларды SOC қатысты қарастырамыз. Ұйым SOC деп саналуы үшін, ол:

2) Тұтынушыларға киберқауіпсіздік оқиғалары туралы хабарлау үшін қаражат беру.

3) Клиенттерге инциденттерді өңдеуге көмек көрсету.

4) Инциденттерге байланысты ақпаратты SOC қызметінің тұтынушыларына және сыртқы қатысушыларға беру [3].

SOC клиенттерге оқыс оқиғаларды анықтау және әрекет етудің негізгі миссиясымен байланысты қызметтер жиынтығын ұсынады-мысалы, қауіпсіздік туралы хабардарлықты арттыру немесе осалдықты бағалау саласында. SOC тұтынушыларға ұсынатын қызметтерді өрт қызметі немесе жедел жәрдем қалай жұмыс істейтінін салыстыруға болады. Өрт сөндірушілер мен авариялық-құтқару қызметтерінің басқа да қызметкерлерінің басты міндеті – төтенше жағдайларда адамдарға көмек көрсету, бірақ олардың жұмысында зиян келтірудің алдын алуға баса назар аударылады. Бұған қоса өрт қауіпсіздігін оқыту, тұрғын үйлер мен кәсіпорындардың инспекциясы, сондай-ақ алғашқы көмекті оқыту кіреді. Ақпараттық қызмет өрттен, сондай-ақ ақпараттық қауіпсіздік инциденттерінен залалды болдырмау үшін үлкен маңызға ие.

Кейбір өрт сөндіру бөлімдерінде өрттің шығу себептері мен таралу жолдарына егжей-тегжейлі тексеру жүргізу үшін ресурстар бар. Ұқсас, кейбір SOC компрометирленген жүйелерге қатысты толық сараптама жүргізу үшін дағдылар мен ресурстарға ие. Басқа, алайда, егер тереңдетілген тергеу жүргізу қажет болса, SOC-серіктестеріне немесе сыртқы ұйымдарға жүгінуге мәжбүр.

SOC ішкі бөлімшелерді (ат, HR) қоса алғанда, АҚ басқару процесінің басқа қатысушыларымен өзара әрекеттесуі өте маңызды. SOC-та бұзушылықтар туындаған кезде жауап шараларын қабылдаудың алты кезеңі қарастырылған.

Дайындау кезеңі:

- тәжірибелі дипломды мамандарды тарту;
- АҚ қамтамасыз ету жоспарын әзірлеу және ресімдеу;
- клиенттермен және серіктес ұйымдармен SLA шарттарын әзірлеу;
- қажетті құралдарды сатып алу;
- АҚ қамтамасыз ету рәсімдерін енгізу;
- SOC персоналын құралдармен және процедуралармен жұмыс істеуге оқыту;
- тұрақты пайдалану үздіксіздігін тексеру;
- өндірушілермен / жеткізушілермен бірге алып жүру туралы тұрақты қолданыстағы шарттардың болуы;
- сараптамалық бағалау және процесті жақсарту дәрежесін сандық өлшеу.

Сәйкестендіру кезеңі, өз клиенттеріңіздің желілерін қозғағанға дейін ақ саласындағы инциденттерді анықтау үшін NetFlow, SNMP хаттамасы бойынша сауалнамалар, SNMP-trap хабарламалары және syslog хабарламалары арқылы алынатын талдау құралдары мен мониторинг деректерін пайдаланылады.

Жіктелу кезеңі, шабуыл сәйкестендірілгеннен кейін оның күрделілік дәрежесін және ауқымын бағалау қажет – ол бір немесе бірнеше клиенттерді немесе барлық инфрақұрылымды қозғайды.

Ақпарат көзін бақылау кезеңі, шабуылда объект және субъект болады. Қауіп жіктелген соң оның ену нүктесін табу керек: бұл серіктес-ұйымның желісі, жоғары немесе төмен деңгейдегі желідегі сервер, деректерді өңдеу орталығында бұзылған желілік құрылғы болуы мүмкін.

Қарсы жауап кезеңі, шабуылды жіктеп және оның көзін анықтап, SOC мамандары басу құралдары мен рәсімдерін қолданады. Бұл жұмыс табысты болуы үшін желі жағдайының көрнекі бейнесі қажет және жақсы жазылған стандартты операциялық рәсімдер. Осы рәсімдерді ұстанса, проблеманы ушықтырып алу қауіпі жойылады.

Талдау кезеңі, мамандар АҚ-ның әрбір оқиғасының бастапқы себептерін талдап, кезекті бұзушылық туындаған кезде оларды анықтама үшін пайдалану үшін инциденттерді шешу жөніндегі жұмыс нұсқаулықтарына табылған шешімдерді енгізуі тиіс. Егер мамандар оларды дұрыс қолдану тәжірибесі немесе жеткілікті кәсіби дағдылары жоқ болса, тіпті тосын жағдайларға әрекет етудің мінсіз рәсімдері аз пайда әкеледі.

SOC-та кибершабуыл жағдайында қызметкерлермен, клиенттермен және өзара іс-қимыл жасайтын провайдерлермен байланыс рәсімдері болуы тиіс. Нақты байланыс ақпаратынан бұрын, жылдам және тиімді сипатталған оқиғаға әрекет етудің алты кезеңінен өтуге көмектеседі. Сондықтан келесі деректерді жинау және уақтылы жаңарту қажет:

- маңызды электрондық пошта мекен-жайлары, телефон нөмірлері және пейджерлер, web-беттердің URL мекен-жайлары;

- барлық өзара байланысты провайдерлердің байланысқан тұлғалары – сіздің ұйымыңызбен бір деңгейдегі және неғұрлым жоғары деңгейдегі, сондай-ақ өндірушілер, жеткізушілер және клиенттер;

- өнім қауіпсіздігін қамтамасыз етудің жедел топтарынан сіздің жеткізушілердің байланыстағы тұлғалары және жауап шараларын қабылдауға жауапты тұлғалар;

- клиенттерді қолдау деңгейін, шабуыл көздерін жіктеу және қадағалау тәртібін, жауап шараларын қабылдау әдістерін белгілейтін саясат.

1.2 DLP жүйесі

DLP-ақпараттық ортада деректердің ағуын болдырмау жүйесі. Бұл арнайы құрал болып табылады, оның көмегімен корпоративтік желілердің жүйелік администраторлар ақпаратты рұқсатсыз беру әрекеттерін қадағалай және бұғаттай алады. Сонымен қатар, мұндай жүйе ақпаратты заңсыз иелену фактілерін болдырмауы мүмкін, ол сондай-ақ әлеуметтік желілерді пайдаланумен, чаттарда қарым-қатынас жасаумен, электрондық пошта арқылы хабарламалар жіберумен және т.б. байланысты желінің барлық пайдаланушыларының әрекеттерін қадағалауға мүмкіндік береді. DLP құпия ақпаратының жылыстауын болдырмау жүйелері бағытталған негізгі мақсат қандай да бір ұйымда, компанияда, кәсіпорында бар ақпараттың құпиялылығы мен қауіпсіздігі саясатының барлық талаптарын қолдау және орындау болып табылады. DLP жүйелерін іс жүзінде қолдану құпия деректердің тарауына үлкен қаржылық шығындарға, беделі бойынша елеулі соққы, сондай-ақ клиенттік база мен жеке ақпаратты жоғалтуға әкеп соқтыруы мүмкін ұйымдар үшін аса өзекті болып табылады. Мұндай жүйелердің болуы өз қызметкерлерінің "ақпараттық гигиенасына" жоғары талаптар қоятын компаниялар мен ұйымдар үшін міндетті.

DLP-жүйелердегі құпия ақпаратты тану екі тәсілмен жүргізіледі: формальды белгілерді талдау (мысалы, құжат грифі, арнайы енгізілген таңбалар, хеш-функцияны салыстыру) және контентті талдау. Бірінші әдіс жалған іске қосылудан (бірінші түрдегі қателер) құтылуға мүмкіндік береді, бірақ құжаттарды алдын ала жіктеуді, белгілерді енгізуді, сигналдарды және т.б. жинауды талап етеді. Екінші әдіс жалған жұмыс істеуді береді, бірақ құпия ақпаратты тек грифтелген құжаттардың арасында ғана емес, жіберуді анықтауға мүмкіндік береді. Жақсы DLP жүйелерінде екі тәсіл де үйлеседі.

DLP-жүйелердің құрамына желілік деңгейдің компоненттері (модульдері) және хост деңгейінің компоненттері кіреді. Желілік компоненттер ақпараттық жүйенің шекарасын кесіп өтетін трафикті бақылайды. Әдетте олар прокси-серверлерде, электрондық пошта серверлерінде, сондай-ақ жеке серверлер түрінде тұрады. Хост деңгейінің компоненттері әдетте қызметкерлердің дербес компьютерлерінде тұрады және ақпаратты компакт-дискілерге, флэш-жинақтағыштарға және т. б. жазу сияқты арналарды бақылайды. Сондай-ақ, хостық компоненттер желілік параметрлердің өзгеруін, туннелдеуге арналған бағдарламалардың

инсталляциясын, стеганографияны және бақылауды айналып өту үшін басқа да ықтимал әдістерді қадағалауға тырысады. DLP-жүйенің көрсетілген екі түрінің компоненттері және орталықтандырылған басқару модулі болуы тиіс.

DLP-жүйелер, сондай-ақ персоналдың іс-әрекетін бақылаумен байланысты басқа да бірқатар міндеттерді шешу үшін жақсы қолайлы. Ең жиі DLP жүйелері келесі негізгі емес міндеттерді шешу үшін қолданылады:

- қызметкерлердің жұмыс уақыты мен жұмыс ресурстарын пайдалануды бақылау;
- ұйымға зиян келтіруі мүмкін конфликттерді анықтау мақсатында қызметкерлердің қарым-қатынас мониторингі;
- қызметкерлердің іс-әрекеттерінің заңдылығын бақылау (жалған құжаттарды басып шығаруды болдырмау және т. б.);
- босаған лауазымға жедел түрде резюме жіберетін қызметкерлерді анықтау [4].

Көптеген ұйымдар осы міндеттердің бірқатарын (әсіресе жұмыс уақытын пайдалануды бақылау) ақпараттың таралып кетуінен қорғауға қарағанда анағұрлым басым деп есептейтіндіктен, дәл осы үшін арналған, алайда бірқатар жағдайларда жұмыс істеуге қабілетті және ұйымды таралып кетуден қорғау құралы ретінде бірқатар бағдарламалар пайда болды.

Клиенттердің банктік карталарының нөмірлері, олардың банктік шоттары, тендерлердің шарттары туралы мәліметтер, жұмыстар мен қызметтерді орындауға тапсырыстар сияқты деректерді қорғауға арналған үздік құрал DLP жүйесі болып табылады – мұндай қауіпсіздіктің экономикалық тиімділігі айқын.

1.3 IDS/IPS жүйелері

IDS IPS зиянкестердің ақпараттық деректерді белгілі әдістермен өзгертуге әрекет ету мүмкіндігін беретін басып кіруді анықтау және алдын алу жүйелері-кешендері. Сондай-ақ кешен желі ішінде жүргізілетін зиянды белсенділікті таниды және бұғаттайды. Жүйенің жұмыс істеу принципі – белгілі шабуылдарды талдау үшін ережелерді қолдану. Нақты уақыт режимінде қауіп-қатерлерді қадағалау және бұғаттау жүреді. Жедел қорғаныс шараларының бірі: жүйенің зарарланған трафигін бұғаттау, қосылыстың үзілуі, желі әкімшісін жедел хабардар ету болып табылады.

Шабуылдарды оқшаулау кешендерінің ерекшеліктерінің бірі кез келген іс-әрекеттің тұрақты мониторингі және талдауы тұрақты функцияларға жатады. Сонымен қатар, басып кіруді анықтау жүйесі келесі міндеттерді орындайды:

1) ақпарат жинау, оны жазу;

2) басқарушыны және пайдаланушыларды қауіпсіздікпен байланысты кез келген өзгерістер туралы жедел хабарлау;

3) қауіпсіздік туралы ақпаратты есептеумен және іріктеумен есептерді жасау.

Кеңейтілген функционал нақты уақыт режимінде маңызды файлдарға қолжетімділікті жабуға; қорғау ортасының конфигурациясын өзгертуге; шабуыл құралдарын бұғаттауға, жоюға мүмкіндік береді. Қазіргі заманғы желіаралық экрандар – бұл кешенді шешімдер, өйткені олар бір-бірімен IDS және IPS технологияларды біріктіреді. Мұндай жүйелік қондырғылардың бірі UserGate өнімі болып табылады.

IDS жүйелері network-based және host-based болып бөлінеді.

Network-based IDS желілік пакеттерді басып, талдай отырып, шабуылдарды анықтайды. Желілік сегментті тыңдай отырып, NIDS желілік сегментке қосылған бірнеше хостардан желілік трафикті көре алады және осы хостарды қорғайды.

Host-based IDS жалғыз компьютердің ішінде жиналған ақпаратпен жұмыс істейді. Мұндай тиімді орын HIDS OS нақты шабуылға қатысы бар процестер мен пайдаланушыларды ғана анықтай отырып, үлкен сенімділікпен және дәлдікпен қызметті талдауға мүмкіндік береді. IDS әдетте екі түрдегі ақпараттық көздерді қолданады: ОЖ аудитінің нәтижелері және жүйелік логтар.

Басып кіруді анықтау жүйелері белгілі оқиғалар негізінде салынған үлгілермен жұмыс істейді. Бақылауға не жатады: кіріс және шығыс трафик, электрондық хаттар, операциялық жүйенің проблемалары мен тәуелділігі. Шабуыл жасаудың барлық әрекеттері қатерлерді мониторингілеу және анықтау үшін қосылады және одан әрі қолданылады. Әдістеме белгілі араласулармен жұмыс істеу кезінде тиімді. Белгісіз вирусты бағдарламалар болған жағдайда анықтаудың тағы бір нұсқасын қолдану немесе кез келген түрдегі шабуылдарды жеңетін кешенді енгізу қажет. Соңғы шешім оңтайлы болып саналады [5].

Функционалдық ерекшеліктерге сәйкес, IDS және IPS-ақпараттық желінің құрауыштарына талдау жүргізуге, осындай іздестірудің нәтижесіне уақытында және әрекет етуге қабілетті қуатты құралдар. Технология үлкен және өте үлкен емес корпоративтік желілерде енгізуге ұсынылған. Ақпараттық жүйенің қауіпсіз жұмыс істеуін қамтамасыз ету үшін белгісіз шабуылдар да бақыланады.

1.4 Желіаралық экран

Желіаралық экран, желілік экран-берілген ережелерге сәйкес ол арқылы өтетін желілік тра0фикті бақылау мен сүзуді жүзеге асыратын компьютерлік желінің бағдарламалық немесе бағдарламалық-аппараттық элементі.

Желі арасындағы экрандарды шешетін міндеттердің арасында негізгі болып желі сегменттерін немесе жекелеген хостарды OSI желілік моделінің хаттамаларында немесе желі компьютерлерінде орнатылған бағдарламалық қамтамасыз етуде осал жерлерді пайдалана отырып, рұқсатсыз қол жеткізуден қорғау болып табылады. Желі арасындағы экрандар берілген үлгілермен салыстыра отырып, трафикті өткізеді немесе тыйым салады.

Желіаралық экрандар ең кең тараған орнату жері – lan шекара периметрі. Ол ішкі хосттардың сырттан жасалатын шабуылдардан қорғау үшін орнатылады. Бірақ шабуылдар ішкі тораптардан да басталуы мүмкін, бұл жағдайда, егер шабуылдаушы хост сол желіде орналасқан болса, трафик желілік периметрдің шекарасынан өтпесе желіаралық экран іске асырылмайды. Сондықтан, қазіргі уақытта желіаралық экрандар тек шекарада ғана емес, сонымен қатар желінің әр түрлі сегменттерінің арасында да орналастырылады, бұл қосымша қауіпсіздік деңгейін қамтамасыз етеді.

Трафикті сүзгілеу алдын ала теңшелген ережелерді теру негізінде жүзеге асырылады. Ақпарат ағынын өңдейтін сүзгілер тізбегі ретінде желіаралық экранды ұсынуға ыңғайлы. Әрбір сүзгілер жеке ережені түсіндіруге арналған. Жинақтағы ережелер тізбегі желіаралық экранның өнімділігіне айтарлықтай әсер етеді. Мысалы, көптеген желіаралық экрандар трафикті сәйкестік табылғанша ережелермен дәйекті салыстырады. Мұндай желіаралық экрандар үшін, трафиктің ең үлкен санына сәйкес келетін ережелер тізімде мүмкіндігінше жоғары болуы керек, осылайша өнімділікті ұлғайтады.

Келіп түсетін трафикті өңдеудің екі принципі бар. Бірінші қағидат: "не анық тыйым салынбаған, онда рұқсат етілген". Бұл жағдайда, егер желіаралық экран бірде-бір ережеге түспейтін пакетті алса, онда ол одан әрі беріледі. Қарама-қарсы принцип – «не анық рұқсат етілмеген, онда тыйым салынады» әлдеқайда үлкен қорғауға кепілдік береді, өйткені ол ережемен анық рұқсат етілмеген барлық трафикке тыйым салады. Алайда, бұл принцип әкімшіге қосымша жүктемені айналдырады.

Сайып келгенде желіаралық экрандар келіп түсетін трафик үстінде екі операцияның бірін орындайды: пакетті одан әрі өткізіп жіберу немесе пакетті лақтыру (deny). Кейбір желіаралық экрандар тағы бір операцияға ие – «reject», ол кезде пакет алынып тасталынады, бірақ жіберушіге ол алуға тырысқан сервистің қолжетімсіздігі туралы хабарланады. Осыған қарама-қарсы, «deny» операциясы кезінде жіберуші сервистің қол жетімсіздігі туралы хабарланбайды, бұл қауіпсіз болып табылады.

Осы уақытқа дейін желіаралық экрандардың бірыңғай және жалпыға танылған жіктемесі жоқ. Бірақ көп жағдайда OSI желілік моделінің қолдау деңгейі оларды жіктеу кезіндегі негізгі сипаттама болып табылады. Осы үлгіні ескере отырып, желіаралық экрандардың келесі түрлерін ажыратады:

1) басқарылатын коммутаторлар;
2) пакеттік сүзгілер;
3) сеанстық деңгейдегі шлюздер;
4) қолданбалы деңгейдегі делдалдар;
5) жай-күй инспекторлары.

Желіаралық экрандарды орындаудың екі нұсқасы бар – бағдарламалық және бағдарламалық-аппараттық. Өз кезегінде бағдарламалық-аппараттық

нұсқаның екі түрі бар - коммутаторда немесе маршрутизаторда жеке модуль түрінде және мамандандырылған құрылғы түрінде.

Қазіргі уақытта көбінесе бағдарламалық шешім қолданылады, ол бірінші қарағанда тартымды көрінеді. Бұл оны қолдану үшін тек желіаралық экранның бағдарламалық жасақтамасын сатып алу және ұйымдағы кез келген компьютерге орнату жеткілікті болып көрінгендіктен туындайды. Алайда, тәжірибе көрсеткендей, ұйымда әрдайым еркін компьютер болмайды, сонымен қатар жүйелік ресурстар бойынша жоғары талаптарды қанағаттандырады. Компьютер табылған соң (көбінесе-сатып алынған) операциялық жүйені орнату және баптау, сондай – ақ желіаралық экранның бағдарламалық қамтамасыз ету процесі қажет. Қарапайым дербес компьютерді пайдалану оңай емес, ол көрінуі мүмкін. Сондықтан, әдетте, FreeBSD немесе Linux негізінде security appliance деп аталатын арнайы бағдарламалық-аппараттық кешендер тек қажетті функцияларды орындау үшін "кесілген" кең тарала бастады. Осы шешімдердің артықшылықтары [6]:

1) енгізу оңай: бұл құрылғылар алдын ала орнатылған және бапталған операциялық жүйеге ие және желіге енгізгеннен кейін ең аз параметрлерді талап етеді;

2) басқару қарапайымдылығы: бұл құрылғыларды кез келген жерден SNMP немесе Telnet сияқты стандартты протоколдар бойынша немесе SSH немесе SSL сияқты қорғалған протоколдар арқылы басқаруға болады;

3) өнімділік: бұл құрылғылар тиімді жұмыс істейді, өйткені олардың операциялық жүйесінен барлық пайдаланылмайтын сервистер алынып тасталды;

4) бас тарту тұрақтылығы және жоғары қол жетімділік: бұл құрылғылар жоғары қол жетімділігі бар нақты міндеттерді орындауға арналған.

1.5 SIEM жүйесі жайлы жалпы түсінік

Түрлі ақпараттық жүйелердегі (АЖ) қауіпсіздік қатерлеріне жауап беру үшін нақты уақыттық оқиғаларды талдауға мүмкіндік беретін құралдардың болуы қажет және олардың саны әрдайым өсіп келеді. Бұл мәселенің шешімі SIEM-жүйелерді пайдалану болып табылады.

SIEM жүйесінің негізгі қағидасы ақпараттық жүйенің қауіпсіздігі туралы ақпаратты әртүрлі дереккөздерден жинақтап, өңдеу нәтижесінде қауіпсіздік талдаушыларына бірыңғай интерфейспен ұсынуында, бұл қауіпсіздік оқиғаларына сәйкес келетін ерекшеліктерді зерттеуді жеңілдетеді. SIEM - ақпараттық қауіпсіздікті басқару (SIM) және қауіпсіздік оқиғаларын басқаруды (SEM) бірыңғай біріктірілген қауіпсіздікті басқару жүйесі болып табылады. SIM сегмент негізінен деректерді талдауға, жүйенің ұзақ мерзімді тиімділігін арттыруға және деректерді сақтауды жүйелендіруге тырысады. Ал SEM сегментінде қазіргі уақыт мезетіндеші деректерді жүктеуге және сол деректер негізінде қауіпсіздік инциденттерін дереу анықтауға мүмкіндік береді. Қосымша мүмкіндіктерге қажеттілік өсіп келе жатқандықтан, осы өнім санатының функционалдығы үнемі кеңейтіліп, толықтырылады.

SIEM жүйелерін пайдаланудың негізгі мақсаттарының бірі қауіпсіздік туралы ақпараттарды басқару мүмкіндігін қамтамасыз ету және оқиғаларды қауіпсіздік оқиғаларын жақын уақытта нақты режимде басқару арқылы ақпараттық қауіпсіздіктің деңгейін арттыру болып табылады.

Қауіпсіздік оқиғаларын басқарудағы басты міндет – бұл жағдайды критикалық деңгейге жеткізбей тұрып алдын-ала шешім қабылдау. Мұндай басқару жүйесі бұрыңғы деректерге сүйене отырып оқиғаларды алдын-ала болжайтын автоматтандырылған тетіктерді пайдалану арқылы түзету немесе белгілі бір жүйе жағдайына оқиғалардың мониторинг параметрлерін автоматты түрде түзету арқылы жүзеге асады.

SIEM жүйесі қосымшалардан, құрылғылардан немесе қызметтерден тұруы мүмкін, сондай-ақ деректерді тіркеу және басқа бизнес-деректерімен үйлесімділік үшін есептерді жасау үшін пайдаланылады.

SIEM жүйесін алғаш 2005 жылы Gartner компаниясының мамандары Марк Николетт Амрит Уильямс ұсынған. Ол ақпаратты жинақтау функционалдылығын бақылау, желінің және қауіпсіздік құрылғыларының мәліметтерін талдау және ұсыну, сәйкестендіру бағдарламалары (деректерді басқару) және кіруді бақылау, қауіпсіздік саясаты және осалдылықты бақылау құралдары, операциялық жүйелер, дерекқорлар және қосымшалар журналдары және сыртқы қауіптер туралы ақпаратты визуализациялайтын жүйе ретінде көрсетілді.

2 SIEM жүйесі

SIEM-жүйесі "агенттер" – "деректер қоймасы" – "қосымшалар сервері" архитектурасы бойынша құрылған. Агенттер қауіпсіздік оқиғаларын жинауды, оларды бастапқы өңдеуді және сүзуді орындайды. Қауіпсіздік оқиғалары туралы жиналған және сүзілген ақпарат деректер қорына немесе репозиторийге түседі, онда ол қосымшалардың серверімен кейіннен пайдалану және талдау мақсатында ішкі пішімде сақталады. Қосымшалар сервері ақпаратты қорғаудың негізгі функцияларын іске асырады. Ол репозиторияда сақталатын ақпаратты талдайды және оны ақпаратты қорғау жөніндегі ескертулерді немесе басқарушылық шешімдерді әзірлеу үшін құрады. Осылайша, SIEM жүйесінде келесі үш архитектуралық деңгейді бөліп көрсетуге болады: деректерді жинау; деректерді басқару; деректерді талдау.

Бірінші деңгейде деректерді жинау әр түрлі көздерден жүзеге асырылады. Олардың қатарына: файлдық серверлер, деректер қорының серверлері, Windows-серверлер, желіаралық экрандар (firewall), жұмыс станциялары, шабуылдарға қарсы әрекет ету жүйелері (IPS, intrusion prevention systems), антивирустық бағдарламалар және т. б. жатады.

Екінші деңгейде репозиторияда сақталатын қауіпсіздік оқиғалары туралы деректерді басқару жүзеге асырылады. Репозиторияда сақталатын деректер деректерді талдау үлгілерінің сұраулары бойынша беріледі.

Үшінші деңгейде алынған SIEM-жүйедегі ақпаратты өңдеу нәтижелері алдын ала анықталған және аралық нысандағы есептер, оқиғалар туралы деректерді жедел (on-line) корреляциялау, сондай-ақ on-line режимінде өндірілетін және (немесе) электрондық пошта арқылы берілетін ескертулер болып табылады.

2.1 SIEM жүйесінің функционалды қызметтері

Деректерді жинау және қалыпқа келтіру: әртүрлі ақпарат көздерінен деректер жинақталады (ақпараттық қауіпсіздік оқиғалары және жүйелік оқиғалар): ақпараттық қауіпсіздіктің техникалық құралдары (барлық түрлердегі брандмауэрлер, кірудің алдын-алу жүйесі, антивирустар, спамнан қорғау жүйесі, деректерді заңсыз жіберуден қорғау жүйесі, бағдарламалардың алдын ала орындалу жүйелері, тұтастық мониторингі және т.б.), серверлер, қолданбалы жүйелер және т.б.

Деректер корреляциясы: атрибуттар бойынша сәйкестендіру және іздеу, белгілі бір өлшемдерге сәйкес топтау және индекстеу. Іс жүзінде корреляция SIEM-тің басты функциясы болып табылады, ол корреляциялық оқиғалардың тізімін шығарады.

Ескерту: ақпараттық қауіпсіздік оқиғаларын анықтау және осы оқиғаларға ескерту үшін өзара байланысты оқиғалардың тізімін тексеру. SIEM басқару консоліне индикация ретінде немесе корреляция ережелеріне негізделген автоматтандырылған хабарландыру ретінде де ескертпе келу мүмкіншілігі.

Бақылау тақталары (dashboards): әртүрлі типтегі графиктер және форматтар, кестелер, тізімдер және ағымдағы оқиғалар мен оқиғалардың басқа визуализациялары. Визуализация өнімнің жалпы қабылдануына айтарлықтай әсер етеді және оқиғалар мониторингі немесе қадағалау процесінің маңызды элементі болып табылады.

Деректерді сақтау: нақты уақыт кезеңі үшін деректерді сақтау. Сақталған деректер ретроспективті талдау, инциденттерді тексеру, экспертиза үшін қажет. Заманауи SIEM процестердің көпшілігі шикі оқиғаларды (іс-әрекеттің функционалдық өрістерін танудан бұрын) және нормаланған оқиғаларды (танылған өрістермен оқиғаларды) сақтайды және өңдейді [7].

Іздеу және талдау: инциденттерді және сараптамалық зерттеулерді контекстік іздеу. Шикізатты және қалыпты оқиғалар бойынша іздеу айтарлықтай өзгеше болуы мүмкін екендігін атап өткен жөн.

Деректерді талдау бірнеше кезеңдерден тұрады:

1) нормализация – әр түрлі көздерден жиналған журнал жазбаларының форматтарын бірыңғай ішкі форматқа әкеледі, содан кейін оларды сақтау және кейіннен өңдеу үшін пайдаланылатын болады;

2) фильтрация – жүйеге келіп түсетін ағындардан артық оқиғаларды жою болып табылады;

3) классификация – қауіпсіздік оқиғаларының атрибуттары үшін олардың белгілі бір класқа жататынын анықтауға мүмкіндік береді;

4) агрегация – белгілі бір белгілерге ұқсас оқиғаларды біріктіреді;

5) корреляция – әртүрлі оқиғалар арасындағы өзара байланысты анықтайды;

6) приоритезация – басымдық жүйеде анықталған ережелер негізінде қауіпсіздік оқиғаларының маңыздылығы мен сындылығын анықтайды;

7) талдау – оқиғаларды, инциденттерді және олардың салдарын талдау оқиғаларды, шабуылдарды және олардың салдарын модельдеу, жүйенің осалдығы мен қорғалуын талдау, бұзушылардың параметрлерін анықтау, тәуекелді бағалау, оқиғалар мен инциденттерді болжау рәсімдерін қамтиды;

8) генерация – есептер мен ескертулерді генерациялау жұмыс істеу нәтижелерін қалыптастыруды, беруді, көрсетуді немесе басып шығаруды білдіреді;

9) визуализация – қауіпсіздік оқиғаларын талдау нәтижелерін және қорғалатын жүйе мен оның элементтерінің жай-күйін сипаттайтын деректерді графикалық түрде ұсынуды көздейді.

Есеп беру: ағымдағы оқиғалар, оқиғалар мен трендтер туралы ақпараттық қауіпсіздік қызметі туралы мезгіл-мезгіл ақпараттандыру мақсатында жеке есептерді жасау. Әдетте, есептер жүктеледі және ақпараттық қауіпсіздік қызметтерінің жан-жақты есептерінің бөлігі ретінде пайдаланылады.

Ақпарат көздері:

- access control, authentication: ақпараттық жүйелерге қолжетімділікті және артықшылықтарды пайдалануды бақылау үшін қолданылады;

- DLP жүйесі, ақпараттың инсайдерлік тасымалдау әрекеттері туралы ақпарат, ақпаратқа қол жеткізу құқығын бұзу;

- IDS / IPS жүйелер. Желілік шабуылдар, конфигурациялық өзгерістер және құрылғыларға қол жеткізу туралы деректерді беру;

- антивирус қосымшалары. Бағдарламалық жасақтаманың, дерекқордың, конфигурацияның және саясаттың өзгеруінің, зиянды код күйі туралы оқиғаларды мәлімдеу;

- серверлер және жұмыс станциялары бойынша оқиғалар журналдары, олар ақпаратқа қол жеткізуді бақылау, үздіксіздікті қамтамасыз ету, ақпараттық қауіпсіздік саясатын қамтамасыз ету үшін қолданылады;

- брандмауэрлер: шабуылдар, зиянды бағдарламалар туралы ақпарат;

- желі жабдықтары: ақпаратқа қол жеткізуді бақылау, желілік трафикті есепке алу үшін қолданылады;

- осалдылық сканерлері: инвентаризация активтері, қызметтер, бағдарламалық қамтамасыз ету, осалдықтар, түгендеу деректері туралы және топологиялық құрылымды жеткізу;

- инвентарлық жүйелер және asset-management (активтерді басқару), инфрақұрылымдағы активтерді қадағалау және жаңа активтерді анықтау деректерін мәлімдеу;

- веб-сүзу жүйелері: қызметкердің күдікті немесе тыйым салынған веб-сайттарға кіруі туралы мәліметтерді қамтамасыз ету.

SIEM жүйесі қорғалынатын ақпараттық жүйеге орнатылып және «дерек көздері» - «деректерді сақтау» - «бағдарлама сервері» архитектурасы бойынша құрылады. SIEM-бағдарламалары интеграцияланған құрылғы (all-in-one) күйінде немесе екі-үш компоненттік кешен ретінде құрылады. Бірнеше компонентті кешен функционалды басымдылық пен үлкен аумақты қамтуға қамтамасыз етеді, сондай-ақ, бірнеше бөлшекті IT-инфрақұрылымдарда орналастыруға мүмкіндік береді [8].

Агенттер бастапқы өңдеуді және сүзуді жүзеге асырады, сондай-ақ қауіпсіздік оқиғаларын жинайды.

Дерек көздерінен ақпаратты жинау бірнеше жолмен жүзеге асырылуы мүмкін:

- ақпарат көзі өзі оқиғалар бойынша ақпаратты жібереді (мысалы, syslog-протокол арқылы);

- ақпарат көздерінен оқиғалар бойынша ақпарат пассивті қабылданады.

Ақпарат көзі өзі жіберу келесі жолмен іске асырылады: ақпарат көзі оқиғаларды жинайтын құрылғының IP мекенжайын көрсетеді және оқиғалар адресатқа жіберіледі.

Ақпарат пассивті қабылданған жағдайда агент арқылы немесе ақпарат жинау бойынша деректер жиналады, ал кейбір SIEM екеуі де қамтылады. Агентке негізделген әдіс арнайы агенттік бағдарламаны пайдалану арқылы жүйеге

асады, агентсіз әдіс қашықтан кіруге немесе қосымша хаттамаларды пайдалануға мүмкіндік беретін қосымша бағдарлама орнату арқылы іске асады.

Қауіпсіздік оқиғалары туралы жиналған және сүзілген ақпарат деректер қоймасына кіреді, онда ол қосымша серверді қолдану және талдау мақсатында ішкі көрсетілім форматында сақталады.

Бағдарлама сервері ақпараттық қауіпсіздіктің негізгі функцияларын орындайды. Ол репозиторийде сақталған ақпаратты талдайды және ақпаратты қорғау туралы ескертулер немесе басқару шешімдерін жасау үшін оны түрлендіреді.

2.2 Жетекші жүйелерді шолу

HPE ArcSight Hewlett Packa rd Enterprise (HPE) ArcSight – Ресей нарығындағы ең таралған SIEM-жүйе. Ұзақ уақыт бойы ол эталон болып саналды. 2007 жылдан бастап жүйені енгізу бойынша 400-ден астам жоба іске асырылды. HPE ArcSight Мемлекеттік қормен интеграцияны қолдайды. HPE ArcSight платформасы орта және ірі кәсіпорындар мен қызмет көрсетушілерге бағытталған. Платформа үш түрлі нұсқада қол жетімді:

- arcsight Data Platform деректер платформасы, журналдарды жинауды, есептерді басқаруды және генерациялауды қамтамасыз етеді;
- arcsight Enterprise Security Management (ESM) бағдарламалық жасақтамасы кең ауқымды қауіпсіздік мониторингін өрістетуге арналған;
- "барлығы бірде" құрылғыларына негізделген және алдын ала құрастырылған мониторинг пен есептілікпен, сондай-ақ деректерді оңайлатылған басқарумен пайдалануға бағытталған arcsight express бағдарламалық-аппараттық кешені.

HPE ArcSight платформасы құрылғы, бағдарламалық жасақтама немесе виртуалды дана ретінде кеңейтілуі мүмкін. HPE ArcSight N-деңгейлі HPE ArcSight Management Center масштабталатын архитектураны қолдайды. HPE ArcSight Express тек құрылғы ретінде қол жетімді. ArcSight Express орта деңгейдегі SIEM ретінде қарастыру керек, оны өрістету үшінші тарап коннекторларының кең қолдауын талап етеді. HPE ArcSight ESM үлкен масштабты өрістету үшін және арнайы SOC құрастырғысы келетін ұйымдар үшін жақсы. 2017 жылы жаңа ArcSight Investigate өнімі шықты. Қосымша HPE ArcSight банктерде қаржылық алаяқтықпен күрес, АҚ/АТ жедел басқару, АҚЖ тиімділігінің метрикасын бақылау, SAP интеграциясы, және әлеуметтендіру (ArcSight Marketplace) сияқты қолданбалы міндеттерді шешу жағына қарай дамиды.

HPE ArcSight артықшылықтары: Arcsight ESM ірі масштабты SOC қолдау үшін пайдаланылатын SIEM мүмкіндіктерінің толық жиынтығын ұсынады, соның ішінде инциденттерді тексеру мен басқарудың толық жұмыс процесін, сондай-ақ арнайы өрістетуді басқару консолі. HPE User Behavior Analytics пайдаланушылардың мінез-құлқын талдау негізінде аномалияларды анықтайды және arcsight базалық функциясы болып табылатын дәстүрлі

корреляцияны толықтырады. DNS Malware Analytics DNS-трафик талдайды және АТ-инфрақұрылымының толық көрінуін қамтамасыз етеді, бұл зиянкестер пайдаланғанға дейін желілік осалдықтарды анықтауға көмектеседі. Зиянды белсенділікті анықтау мақсатында DNS-трафикті талдау идеясы HP Labs зерттеу бөлімшесінде бес жыл бұрын пайда болды. Arcsight Threat Central қауіп-қатерлерді білудің интерактивті базасын қамтиды және оларды табу және жою тәсілдері туралы мәліметтермен алмасуға мүмкіндік береді. ArcSight Marketplace порталында ережелер (қауіпсіздік пакеттері) және қосымша бағдарламалар бар. HPE әзірлеушілері мұндай қауіпсіздік пакеттерін қалыптастыруға және қосымша қосымшаларды құруға компанияның серіктестері де қосылады деп үміттенеді. HPE arcsight пайдалануға дайын бөгде технологиялар мен коннекторлардың кең таңдауы бар.

IBM QRadar Security Intelligence Platform бір-бірімен біріктірілген оқиғалар жинау, мониторинг, қорғау талдау және инциденттерді тексеру жүйелерін қамтиды: Log Manager; SIEM; Flow Processor; Vulnerability Manager; Risk Manager; Network Insights; Watson Advisor for Cyber Security; Packet Capture and Incidents Forensics. Ақылы компоненттерге қосымша IBM QRadar тұтынушылары X-Force and App Exchange ішінен тегін контентке, бағдарламаларға және беделдік базаларға қатынаса алады, мұнда инциденттерді кеңейтілген визуализациялау үшін қолданбаларды, UBA, IBM (мысалы, i2 Analysis Notebook) және басқа өндірушілердің басқа қауіпсіздік жүйелерімен интеграциялық модульдерді, сондай-ақ дайын SIEM-мазмұн түріндегі корреляция ережелерін табуға болады. QRadar IaaS (Infrastructure-as-a-Service) қызметі ретінде немесе IBM Managed Security Services оқиғаларының қосымша мониторингімен бірге IBM толық басқаратын SaaS (software-as-a-Service) ұсынысы ретінде ұсынылған физикалық және виртуалды құрылғылар арқылы өрістетілуі мүмкін. Сондай-ақ, 2017 жылы бірқатар ресейлік компаниялар IBM-мен QRadar шешімдеріндегі АҚ инциденттеріне мониторинг және әрекет ету бойынша қызметтер көрсетуге әріптестік келісімдер жасады. QRadar платформасы қауіпсіздік аудит журналдарынан АҚ оқиғалары туралы деректерді жинауға және өңдеуге, желілік статистиканы талдауға (NetFlow және т.б.), желілік трафикті және берілетін ақпаратты дербес талдауды жүзеге асыруға, желі топологиясын құруға және желілік жабдықтың конфигурациялық файлдарындағы өзгерістерді эмуляциялауға, жүйенің осалдығын және қауіпсіз емес баптауларын анықтауға, трафикті толығымен басып алуға және желі тораптары арасындағы байланыс тізбегін қайта келтіруге мүмкіндік береді. Соңғы уақытта IBM бірнеше жаңа мүмкіндіктер мен мүмкіндіктерді, оның ішінде IBM Watson Advisor for Cyber Security және SOC талдаушыларының жүктемесін азайту, инциденттерге әрекет ету процестерін жүйелеу және автоматтандыру үшін IBM Resilient инциденттеріне әрекет ету платформасымен біріктіруді ұсынды.

IBM QRadar Security Intelligence Platform артықшылықтары:

- SOC-ті жоспарлы құруға арналған бірыңғай платформа: АҚ-ның оқиғаларын жинау мен талдаудан бастап, аномалды желілік белсенділікті анықтаудан бастап, осалдықтарды сканерлеу және қауіпсіз конфигурацияларды анықтаудан бастап, IBM Watson жасанды интеллектімен, желілік форензикамен және IBM Resilient-дегі инциденттерге әрекет ету процестеріне көшумен аяқталады;

- QRadar Platform икемді архитектурасы платформа модульдерінің рөлі мен функцияларын қайта анықтауға мүмкіндік береді және Клиент-компанияларды бір рет таңдалған схеманың қатты жақтауларымен шектемейді;

- UBA және IBM X-Force командасынан сенімсіз IP беделді базасын қоса алғанда, тегін қосымшалар, мазмұн және интеграциялық модульдері мол;

- бүкіл әлем бойынша және Ресейде жоғары жүктеме көрсеткіштері мен жұмысқа қабілеттілігіне қойылатын талаптар бар инсталляциялардың саны үлкен.

McAfee Enterprise Security Manager (ESM) физикалық және виртуалды құрылғылар және бағдарламалық қамтамасыз ету ретінде жеткізіледі. SIEM құрамына кіретін үш негізгі компонент – ESM, Event Receiver және Enterprise Log Manager. Қосымша компоненттер Advanced Correlation Engine, Database Event Monitor, Application Data Monitor және Global Threat Intelligence болып табылады. Соңғы уақытта енгізілген кеңею қосымша ішкі немесе сыртқы көздерден бақылау тізімдерін динамикалық толтыру мүмкіндігін, Hadoop-мен неғұрлым терең екі жақты интеграцияны және қауіптер және оларды басқару туралы ақпарат көздеріне қосымша қол жеткізуді қолдауды қамтиды. McAfee Active Response бар ESM интеграциясы енді соңғы жұмыс істеу нүктелерінің көрінуін қамтамасыз етеді [9].

McAfee Enterprise Security Manager артықшылықтары:

- Enterprise Security Manager өнеркәсіптік басқару жүйелері (ICS) мен диспетчерлік басқару және деректерді жинау құрылғылары (SCADA) жақсы қамтылған;

- Intel Security-тен McAfee Data Exchange Layer (DXL) API пайдаланбай бөгде технологиялармен интеграцияны қамтамасыз етеді. Бұл тәсіл ESM SIEM платформасы ретінде пайдалануға мүмкіндік береді;

- McAfee Global Threat Intelligence SIEM-жүйесі Enterprise Security Manager мүмкіндіктерін кеңейтуге мүмкіндік береді, күдікті немесе зиянды IP-мекенжайлармен байланыс сеанстарын қамтитын оқиғаларды тез анықтауға мүмкіндік беретін қауіп-қатерлер туралы үздіксіз жаңартылған ақпарат көзін қосады.

2.3 Жүйе компоненттері

SIEM-жүйесі компоненттерінің құрылымы мен іске асырылуы шешімнің архитектурасына, орындалу көлеміне, жүйенің географиялық таралуына және жұмыс параметрлеріне байланысты.

Әдетте, SIEM-жүйеде барлық негізгі функцияларды іске асыру үшін бірнеше негізгі компоненттер болуы керек.

Коллекторлар: өңделмеген деректерді жинауға жауапты. Олар Syslog, Windows Event Forwarding, SDEE, SNMP Trap, дерекқор клиенттері (MSSQL, Oracle және т.б.) және әртүрлі өндірушілердің басқа да арнайы қызметтеріне көптеген түрлі хаттамалар мен қызметтерді қолдана алады.

Оқиға жиынтығының өзі пассивті режимде (мысалы, syslog) және «сұраныс бойынша» режимінде болуы мүмкін. Коллектор қалыпты оқиғаларды жиі корреляцияға жібереді, ал өңделмеген оқиғалар деректер қоймасына жіберіледі. Түрлі өндірушілердің әр түрлі жүзеге асыруында коллектордың басқа компоненттермен өзара әрекеттесу сұлбасы әртүрлі болуы мүмкін.

Деректерді сақтау: өңделмеген оқиғаларды сақтауға жауапты. Нормаланған оқиғаларды сақтаумен іске асыру мүмкін.

Коррелятор (Correlator): қалыпты оқиғалар үшін өңдеу және корреляциялық функцияларды қамтамасыз етеді. Репозиторийде сақталатын өңделмеген оқиғаларын контекстік іздеуді жүзеге асыруға болады (2.1-сурет).

Сурет 2.1 – Өңдеу процесі

Басқару консолі: басқаруға, конфигурациялауға және визуализациялауға жауапты. Кейбір жағдайларда визуализация функциясын бөлек компонент арқылы орындалады. Корреляцияның сигнатуралық (rule based) және сигнатуралық емес әдістері бар. Сигнатуралық – адам инциденттерді анықтау ережелерін (басып кіруді анықтау жүйелерінің аналогы) қосуға тиіс.

Сигнатурасыз – қара жәшік, ол өзі қойылған ережелер бойынша талдау жасайлды (вендорлардың өзінің қойған ережелері бойынша); әрине, бұл әдісті сіз жүзінде басқара алмайсыз. Қағаз жүзінде өте көп әдістер айтылады, бірақ іс жүзінде тек бірнеше әдістер қолданылады. Олар:

- Statistical – екі немесе одан да көп айнымалыларды өлшеуге және олардың арасындағы статистикалық байланыс дәрежесін есептеуге негізделген оқиғалар корреляциясының күрделі сигналатуралық әдісі;
- RBR Rule-based (pattern based) (HP ECS, IMPACT, RuleCore) – оқиғалар арасындағы өзара байланыс алдын ала берілген арнайы ережелерде талдаушылармен анықталатын әдіс;
- CBR Codebook (case) based (SMARTS) – корреляция оқиғалардың алдын ала берілген матрицасынан лайықты векторлар бойынша жүргізіледі;
- MBR model based reasoning (тым үлкен MTR) – әдіс модель шеңберінде объектілерді абстракциялауға және оларды бақылауға негізделген.
- Bayesian (BDR) – бұл ерекше түсіндіруді талап етпейтін белгілі әдіс, іс жүзінде тиімді емес;
- NMBR – Normalized model based reasoning. MBR-ге ұқсас, baseline ретінде белгілі;
- Graph based. Корреляция графикалық көріністегі (network devices, hosts, services) жүйелік компоненттер арасындағы тәуелділікті іздеу және олардың негізінде баған құру болып табылады. Егер тәуелділік анықталса, бағандар мәселенің пайда болуының негізгі себептерін іздеу үшін пайдаланылады("HTTP server not responding" желілік линканың болмауынан).

Әдетте, бір шешімде бір немесе екі корреляция әдісі қолданылады. Корреляцияны өтірік корреляциямен шатастырмау маңызды, экранға шығару немесе бір типті оқиғалар немесе берілген кластағы оқиғалар есебі болуы мүмкін. Мысал: "failed access for last 24 hour".

Технология алға жылжыған сайын алгоритм адамның қатысуынсыз «жақсыдан нашар ажыратады» деген қате пікір бар, себебі сигналатуралық әдістер өте көп жалған әрекет етуі мүмкін. Егер жүйе инфрақұрылымға және міндеттерге теңшелмесе жалған әрекет ету көп туындайды. SIEM вендорлары сигналатуралық әдістерге үнемі қайтып келеді, себебі олар икемді, қауіп-қатерлерді анықтаған кезде үлкен тиімділігі бар, MTTR-і төмен.

Сигнатуралық әдісте инцидент (немесе қауіп) – бұл "проблема" (инцидент - менеджментке қатысты емес, онда проблемалар жиі кездесетін бір типті инциденттер деп аталады). Мәселенің (problem, P) себебі болады (cause, C). Бұл тәуекелдерді талдау кезінде де ұсталынатын тәртіп. Бірақ біздің жағдайда келіп түскен оқиғалар туындаған немесе туындау үстіндегі мәселе туралы айтады, яғни симптомдар (symptoms, S) болып табылады. Көп жағдайда себеп инцидентке барабар реакция үшін қажет немесе инцидент контексінде жүзеге асырылады (мысалы, пайдаланушы демонды іске қосу параметрлерін өзгертті, себебін анықтау керек). Оқиға себептерін анықтау немесе корреляциялау үшін жинақталған білім базасын пайдаланатын

вендорлар өте аз. Инфрақұрылымға кіру әр түрлі оқиғалар алдында болады: сканерлеу, жабық порттар бойынша байланыс орнату әрекеттері, пошта серверіндегі салымдарды бұғаттау, жоғары артықшылықтары бар есептік жазбаның пайда болуы. Барлығы тек симптомдар, ереже инциденттің пайда болуына әкелетін симптомдарды біріктіреді(проблема, Problem). Бір мәселеге оқиға нәтижесінде пайда болатын бір немесе бірнеше симптомдар әкелуі мүмкін. Бір оқиғадан жиі бірнеше симптомдар алуға болады. Бір проблеманың симптомдары құрамдас және өзара әсер етуі мүмкін.

Бір симптом бір немесе бірнеше проблемаларға әкелуі мүмкін. Бұл ретте мәселе мен симптом арасындағы ықтимал (probabilistic model) байланыс болуы мүмкін. Қажетті корреляция ережесін сипаттай отырып, оңай бақылауға мүмкіндік туады, мысалы, желідегі IT-активтердегі антивирустық БҚ қызметін (және оның бар болуын) бақылау өте оңай. Осындай аз симптомдарды сигнатуралық емес корреляция әдістерімен анықтау қиын. Мысалы, graph based әдісі қандай да бір қызмет пен актив арасындағы байланыс ақауымен байланысты оқиға пайда болса, оларды анықтай алады. NMBR әдісі сервистер жағдайының жаппай өзгеруін ғана анықтайды (әлбетте, бұл – жалғыз жағдайлар). Проблемаларсыз симптомдар – SIEM-де бір немесе бірнеше қарапайым оқиғалар. Проблемаларсыз симптомдарды бір класске біріктірсе болады, мысалы, "қатынау саясатын бұзу" (Policy login violation) классы. Мұндай сынып бойынша оқиғаларды таңдауға болады, бірақ арнайы ереже болмаса, олар бойынша корреляция жүргізілмейді. Сигнатуралық әдіс идеясы жасалған сәйкестік ережелері бойынша іздеу болып табылады. Бір ереже бір мәселеге теңеледі (SIEM терминдеріндегі"инцидент"). Алайда, бір симптом немесе оқиға бойынша бірден бірнеше ереже жұмыс істей алады. Әр түрлі вендорлардың әрекет принципі бірдей, кейбір бөлшектер ғана ерекшеленеді. Есептеуіштер бір ереже (симптом) бойынша сәйкестік санын есептеуге арналған. Мысалы, 5 минут ішінде бір есептік жазбаның атынан операциялық жүйеге 5 сәтсіз кіру әрекеті – оқиға (инцидент). Тіркелуге кіру сәтсіз әрекеті туралы бірінші оқиға түскеннен кейін есептегіш пен триггер іске қосылады. Есептегіш 5 минут ішінде тағы төрт сәтсіз әрекет күтеді. Егер бұл оқиғалар түспесе, онда есептегіш алынып тасталады. Егер олар кешігіп түссе (мысалы, агентпен байланыс болмаса), онда ереже қайтадан іске қосылады, ал бар оқиға пайдаланылады және оқиға (инцидент) жасалады. Және сонымен қатар есептеуішетр оқиға санын санап отырады (t-sql, select count where командасына ұқсас).

Триггер жағдайлардың бірі корреляция ережелері сәйкес келген кезде іске қосылады (немесе матрицада алгоритмдер үшін). Мысалы, "сәтсіз кіру әрекеті" және "белгісіз орындалатын файлды іске қосу". Келтірілген мысалда екі симптом – кіру әрекеті және процесті іске қосу. Осы оқиғалардың кез келгені корреляция ережесінде көрсетілген уақыт аралығында екінші өлшемнің орындалуын күтетін триггерді іске қосады. Берілген уақыт өткеннен кейін триггер жойылады. Егер триггер жойылмаса, бұрыннан өзектілігін

жоғалтқан оқиғаларға байланысты оқиғаларды алу қауіпі туындайды. Сценарий ережелерді орындауға жауап береді. Сценарийлердің мысалдары: SIEM-де кіріктірілген workflow бағдарламасында инцидентті жасау, команданы орындау, электрондық хат жіберу, SNMP Trap жіберу. SIEM инциденттерді кеңейтілген басқару мүмкіндігі басқа өнімдермен біріктіру қажет емес. Инциденттер өте маңызды және компанияның қаржылық шығындарын болдырмауға мүмкіндік береді. Шын мәнінде маңызды және басым оқиғаларға назар аудару үшін активтің басымдылығы мен проблеманың өзі пайдаланылады. Басымдылық (немесе салмақ) әрбір IT-актив үшін қолмен тағайындалады және бір сан (1-3, 1-5) немесе құпиялылық, тұтастық және қол жетімділік параметрлерін талдау нәтижесі болып табылады. Бұл мәндер GRC-жүйелермен интеграциялау кезінде тәуекелдерді талдау үшін пайдаланылады. Кейбір SIEM бір оқиғаларды қайта тіркеуді болдырмауы, сондай-ақ тәуелділігі бар осындай оқиғалардың болуын анықтауы және жаңа инцидентті ашық байланыстыруы мүмкін. Мысалы, жүйеде "Server # down" инциденті ашылды, бұл ретте "Users cannot access to asset", "Multiple SYN packets to # from #"жаңа ережелері жұмыс істейді. Әдетте оқиғалар ұзақ уақыт бойы сақталады (халықаралық стандарттардың талаптары бойынша, инциденттерді тексеру үшін дәлелді база мен материалды қамтамасыз ету үшін). Терабайттық деректер қорына сұраныстарды орындау мүмкін емес. Сондықтан, триггер үшін уақытша шектеуді (корреляция тереңдігі) қосылады немесе базаны онлайн және мұрағаттық етіп бөлінеді, ережелерде қандай мәліметтерді пайдалануға рұқсат етіледі. Бұл ретте онлайн базаның сақтау мерзімі бойынша қатаң шектеулері бар (мысалы, тәулік немесе апта). Корреляция тереңдігі бойынша шектеу теория тұрғысынан өте орынды. Корреляция ережелерінің шамамен 70% тәулік ішінде болған Оқиғалармен, 20% бір аптаға дейін, 5% бір айдан артық емес оқиғалармен жұмыс істейді.

Корреляция ережелері SIEM-де санаттарға бөлінген. Әрбір ережені бөлек қосуға немесе өшіруге болады. Іс жүзінде барлық жүйелер қолданар алдында корреляция ережелерін тестілеуге мүмкіндік береді (осы мүмкіндікті пайдалануды ұсынамын). Алдын ала берілген корреляция ережелерін Жеке жасау үшін үлгілер ретінде пайдалануға болады.

Екінші буынды SIEM-жүйелерде қосымша компоненттер болуы мүмкін: Flow және SPAN трафигінің жинағы, BI компоненттері, TI модулі, алаяқтықтықтан (фрод) қорғау модульдері, ақпараттық саясатты басқару.

Жоғарыда айтылғандай, іс жүзінде жүйе архитектурасы құрамдас компоненттер санын айқындайды және оларды жүзеге асырады. Мысалы, кішігірім іске асыруларда, барлық функциялар бір аппараттық құрылғыда орындалуы мүмкін, ал қамту аумағын кеңейту деген ең көп компоненттерден тұруды білдіреді.

3 Бағдарламалық бөлім

Ақпаратты жинауға келесі бағдарламалар қатысады: Windows операциялық жүйе үшін WMI қолданылады, ал басқа операциялық жүйелер үшін OSSEC. Нормализация кезеңі үшін бағдарламалық шешім ұсынылды. Бағдарламаға келесі талаптар қойылды:

1) бірыңғай көрсеткіштерді бір форматта жинақтау;

2) өңдеу кезінде өңделуші деректердің ақпараттылығын (информативность) жоғалтпау;

3) өңдеу процесін барынша уақыт бойынша ұтымды ойластыру;

4) келесі кезеңде ақпараттық қауіпсіздікке қатысын анықтауға қажетті ақпараттың барлығын жинақтау;

5) алдағы процестерге ыңғайлы форматта көрсету.

3.1 WMI жұмыс істеу принципі

WMI технологиясы (Windows Management Instrumentation) – бұл Windows басқаруымен компьютерлік желінің әр түрлі бөліктерінің жұмысын орталықтандырылған басқару және бақылау үшін Microsoft базалық технологияларының бірі. WMI технологиясы – бұл Web (Web-Based Enterprise Management, WBEM) базасында кәсіпорынды басқару моделін іске асыру, ол өз кезегінде тек Microsoft компаниясының қатысуымен ғана емес, басқа да бірқатар компаниялардың қатысуымен әзірленген. WBEM-нің міндеті нақты жабдыққа, желілік инфрақұрылымға, операциялық жүйеге, файлдық жүйеге және т. б. тәуелді емес кәсіпорынның ақпараттық ортасын қашықтан басқару стандарттарын әзірлеу болып табылады.

WMI-мен жұмысты Windows Script Host (WSH) сценарийлері көмегімен автоматтандыруға болады, сонымен бірге WMI және басқа да ActiveX-технологияларын (мысалы, ActiveX Data Object (ADO) деректер қорына немесе Active Directory Service Interface (ADSI) каталог қызметтерімен жұмыс істеу үшін) пайдалана отырып, осылайша жүйелік әкімші мен бағдарламашы үшін қуатты және ыңғайлы құрал алынады.

WMI технологиясы Windows 95 OSR 2 бастап Windows Server 2003 дейін барлық 32 биттік нұсқаларына арналған. Windows Me/2000/XP және Windows Server 2003 операциялық жүйелерінде ешқандай қосымша WMI орнатудың қажеті жоқ, мұнда 1.5 версиясының WMI ядросы жұмыс істейді. Windows 9x / NT операциялық жүйелері үшін WMI ядросын 1.5 нұсқасына дейін жаңарту қажет. Бұл үшін қажетті wmicore инсталяциялық файлы.exe Microsoft серверінен жүктеп алуға болады.

WMI келесі бөліктерден тұрады: CIM (Common Information Model Object Manager, CIMOM) нысандарының менеджері, ол WMI-ге барлық соңғы қосымшалардың сұрауларын өңдеуді және WMI-ден соңғы қосымшаларға ақпаратты жеткізуді қамтамасыз етеді. Барлық WMI провайдерлері соңғы қолданбадан алынған сұраныстарды қажетті провайдерге дұрыс бағыттау үшін CIMOM арқылы тіркелуі тиіс. CIMOM функционалдығы winmgmt

файлын қамтамасыз етеді.%SystemRoot%\System32\Wbem каталогында орналасқан exe. Бұл файл қызмет ретінде іске қосылады.

CIM Репозиторий (класс сақтау орны). Мұндай кластардың даналарын тұтынушының сұрауы бойынша WMI провайдері құрады. Windows Server 2003 және Windows XP репозиторий физикалық түрде %SystemRoot%\System32\Wbem\Repositiry\FS\objects файлдарында орналасқан.data (репозиторий), index.btr (индекс файлы), index.map және object.map (транзакцияларды бақылау файлдары). Windows репозиторийінің ерте нұсқаларында cim файлында орналасқан rep.

WMI провайдерлері, cimom осы нысандарға WMI API арқылы біркелкі кіруге мүмкіндік береді. Нақты провайдерлер %SystemRoot%\System32\Wbem \ каталогындағы dll-кітапханалармен ұсынылған COM серверлері болып табылады. WMI әртүрлі көздерден, мысалы, оқиғалар журналдары, жүйелік тізілім және т. б. деректерді алуға арналған көптеген кірістірілген провайдерлерді қамтиды.

Wbemdisp файлында орналасқан сценарийлерді қолдау кітапханасы (WMI scripting library).dll %SystemRoot%\System32\Wbem\каталогында.

Қолданба WMI орнатылған кез келген қашықтағы машинаға сұрау жасай алады. Бұл жағдайда қашықтағы машинада CIMOM-мен байланыс болады, содан кейін сұраныстар жергілікті машинамен бірдей өңделеді. CIMOM жергілікті немесе қашықтағы компьютерде WMI қызметтерін пайдалануға тырысатын пайдаланушының құқықтарын тексереді. WMI тұтынушылары (соңғы қолданбалар) басқарылатын объектілерге WMI Query Language (WQL) арнайы сұраныс тілі арқылы жүгіне алады. CIMOM басқарылатын Нысандар оқиғаларының өңдеушілерін жасауға мүмкіндік береді(мысалы, дискілік кеңістіктің көлемін берілген мәнге дейін төмендету, белгілі бір процесті іске қосу және т. б.). Бұл үшін CIMOM қажетті нысанды мезгіл-мезгіл сұратады (сауалнама аралығы соңғы қосымшада беріледі) және қажет болған жағдайда оқиғаны жасайды.

CIM кластарының саны операциялық жүйенің нұсқасына байланысты. Мысалы, Windows Server 2003 үшін CIM 5000 класс сақталады. CIM құрайтын сыныптар бір-біріне иерархиялық тәуелділікте болады және ұрпақтары ата-аналар сыныптарының қасиеттерін мұраға, қайта анықтауға және қосуға болады. CIM класстары иерархиялық реттелген аттар кеңістігіне (namespaces) топталады. Атау түбірі Root ретінде белгіленеді. WMI орнатудың кез келген нұсқасында cimv2, Default, Security және WMI есімдерінің түбірлік кеңістігінен бір деңгейге төмен болатын төрт атау кеңістігі бар.

WMI класстары туралы жалпы ақпарат

Бір кеңістіктің ішіндегі барлық класстар бірегей аттарға ие болуы тиіс (бұл ретте әртүрлі кеңістіктегі класстар аттары сәйкес келуі мүмкін). Класс аттардың басқа кеңістігінен алғы немесе кейінгі класс (предок, потомок) болуы мүмкін емес.

CIM класына толық жол келесі құрылымға ие: \\ComputerName\Namespace:ClassName.KeyProperty1=Value1, KeyProperty2=Value2.

Мұнда:

ComputerName – компьютердің желілік аты. Жергілікті компьютерді орнату үшін " таңбасын пайдалануға болады.".

Namespace – атау кеңістігінің атауы.

ClassName – сынып аты.

KeyProperty1=Value1, KeyProperty2=Value2 – объектінің "сипат-мәні" негізгі жұптарының тізімі.

Мысалы, жергілікті машинада іске қосылған 4 идентификаторы бар Cimv2 аттар кеңістігінен Win32_Process класының данасы осындай жолды анықтайды: \\.\Root\CIMV2:Win32_Process.Handle=4.

WMI көмегімен басқарылатын кез келген ресурс өз класына сәйкес келеді. Әр класстың қасиеттері, әдістері мен квалификаторлары бар. Сондай-ақ, әрбір қасиеттері мен әдісі болуы мүмкін.

Басқарылатын ресурстар туралы ақпаратты сақтау тәсілі бойынша сынып түрлері:

- абстрактілі класс (abstract class) – ұрпақтарды (абстрактілі және абстрактілі емес) құруға арналған үлгі, басқарылатын ресурстың данасын алу үшін пайдаланылмайды;
- статикалық класс (static class) – CIM репозиториясында физикалық сақталатын деректерді (мысалы, жеке WMI параметрлері туралы деректер) үлгілейді, статикалық кластардың даналарына кіру қандай да бір провайдерлердің көмегінсіз жүзеге асырылады;
- динамикалық класс (dynamic class) – тиісті провайдер арқылы басқарылатын ресурстың деректерін модельдейді;
- ассоциативті класс (association class) – класстар немесе басқару ресурстары арасындағы логикалық байланысты сипаттайтын класс, дерексіз, статикалық немесе динамикалық болуы мүмкін;
- жүйе кластары – WMI конфигурациясы мен ішкі функцияларын орындау үшін қызмет етеді (қауіпсіздікті қамтамасыз ету, провайдерлерді тіркеу, оқиғаларға жазылу және т.б.), дерексіз немесе статикалық болуы мүмкін;
- ядро моделінің кластары (core model) – барлық басқару аймақтарымен интерфейсті қамтамасыз ететін абстрактілі кластар (мысалы, Логикалық басқарылатын ресурсты сипаттайтын cim_logicalelement абстрактілі класы, мысалы, файл немесе каталог), мұндай класстардың аттары "CIM"префиксінен басталады;
- жалпы модельдің кластары (common model) – басқарудың арнайы міндеттеріне арналған, бірақ операциялық жүйенің нұсқасына байланысты емес класстар, мұндай класстардың аттары да "CIM"префиксінен басталады;

- кеңею моделінің кластары (extension model) – басқарудың арнайы есептері үшін класстар, мысалы, Win32 ортасының ресурстарына сәйкес келетін, "Win32"префиксінен басталатын класстар.

Класс аттардың басқа кеңістігінен алғы немесе ұрпағы жоқ болғандықтан, әртүрлі аттар кеңістіктерінде ядро моделінің және жалпы модельдің бірдей кластары бар.

Кластардың қасиеттері нақты басқарылатын ресурсты ұсынатын сынып данасын бір мәнді сәйкестендіру үшін, сондай-ақ осы ресурстың ағымдағы күйін сипаттау үшін пайдаланылады. Негізінен, WMI класс сипаттары тек оқу үшін қол жетімді, бірақ кейбір класс сипаттарының мәндерін Put әдісімен өзгертуге болады. Нақты сипатты өзгерту мүмкіндігі операциялық жүйенің нұсқасына байланысты болуы мүмкін. Сипат жазу үшін қол жетімді екенін білу үшін осы сипаттың write біліктілік мәнін тексеруге болады.

Класс әдістері осы классқа сәйкес келетін басқарылатын ресурстың қандай да бір әрекеттерін орындауға мүмкіндік береді. Әрбір ресурста қандай да бір операциялар жасауға болмайды, өйткені кез келген класта әдістер бар.

Квалификаторлар класс, сипат немесе анықталған әдіс туралы қосымша ақпаратты қамтиды.

Класс квалификаторлары жалпы класс туралы ақпаратты ұсынады, мысалы, класс түрі (Abstract, Dynamic, Association, булев мәндерін қабылдай алатын), класс провайдерінің аты (Provider квалификаторы), класс құру, жою, даналарды өзгерту (SupportsCreate, SupportsDelete, SupportsUpdate, булев мәндерін қабылдай алатын), UUID класс (UUID квалификаторы), даналарды жасау, жою әдістерінің атаулары (UUID), даналарды құру, жою (UUID), createby, deleteby квалификаторлары) және т. б.

Қасиеттер квалификаторлары осы сипаттың түрін (cimtype квалификаторы), оқу үшін қол жетімділікті (Read квалификаторы), жазу үшін қол жетімділікті (Write квалификаторы), сипат үшін рұқсат етілген мәндер жиынтығын (ValueMap квалификаторы) және т. б. анықтауға мүмкіндік береді.

Әдістер квалификаторлары әдіс (ValueMap квалификаторы), Privileges және т.б. шақыру үшін қажетті құқықтар (Privileges квалификаторы) және т. б. арқылы қайтарылатын көптеген мәндерді сипаттай алады. тек true мәні бар Implemented квалификаторы бар әдістерді ғана орындауға болады.

WMI ең қуатты мүмкіндіктерінің бірі-WMI оқиғалары туралы хабарламаларға жазылу, яғни белгілі бір WMI оқиғаларының жеке өңдеушілерін жасау. Оқиға мысалдары сервердегі дискілік кеңістіктің көлемін берілген мәнге дейін төмендету, оқиғалар журналында белгілі бір хабарламаның пайда болуы, белгілі бір қосымшаны және т. б. іске қосу немесе аяқтау болып табылады.

WMI оқиғалары ішкі, сыртқы және таймер оқиғаларына бөлінеді. Сыртқы оқиғалар ExtrinsicEvent классы, timerevent - таймер оқиғалары, ал ішкі оқиғалар NamespaceOperationEvent, ClassOperationEvent және

InstanceOperationEvent класстарымен ұсынылған. Оқиға орын алған кезде WMI осы оқиғаға сәйкес келетін класстың данасын автоматты түрде жасайды.

Ішкі оқиғалар WMI жеке класымен ұсынылған басқарылатын ресурстар жағдайындағы өзгерістерді, сондай-ақ CIM репозиториясының құрылымындағы өзгерістерді бақылауға мүмкіндік береді. Басқарылатын ресурстармен байланысты оқиғалар InstanceOperationEvent классынан туған класстарға сәйкес келеді. Бұл InstanceCreationEvent, InstanceModificationEvent және InstanceDeleionEvent кластары.

Ішкі оқиғалар туралы хабарламаға жазылу үшін WQL тілінде арнайы түрдегі сұраулар қолданылады.

Егер CIM-де жеке класс қарастырылмаған қандай да бір объектінің күйін бақылау қажет болса, сыртқы оқиғалар пайдаланылады. Сыртқы оқиға мысалы-тізілімдегі белгілі бір кілт мәнін өзгерту. Сыртқы оқиғаны жасау үшін бұл оқиғаны WMI провайдері қолдауы қажет.

WSH сценарийінен сыртқы оқиға туралы хабарға жазылу үшін SWbemServices класының ExecNotificationQueryAsync әдісі арқылы асинхронды WQL-арнайы түрдегі сұранымды орындау қажет. Таймер оқиғалары белгілі бір уақытта бір рет немесе белгілі бір уақыт аралығында бірнеше рет болуы мүмкін. Оқиғалар тұтынушылары уақытша және тұрақты болуы мүмкін. Уақытша оқиғалар тұтынушылары – бұл өз белсенділігі кезінде ғана оқиғалар туралы хабарлама алатын қосымшалар. Мұндай тұтынушылар WSH сценарийлері болуы мүмкін. Тұрақты оқиғалар тұтынушылары қажетті оқиғаны тікелей CIM репозиториясында тіркеуге мүмкіндік береді, содан кейін бұл оқиға туралы хабарлама CIM-ден анық жойылғанға дейін тұрақты түрде қалыптастырылатын болады. Компьютерді қайта жүктеу мұндай оқиғаны жоймайды [10].

3.2 OSSEC жұмыс істеу принципі

OSSEC-еркін және ашық бастапқы коды бар басып кіруді (HIDS) анықтау хост жүйесі. Ол жүйелік логтарды талдайды, бүтіндігін тексереді, Windows ОЖ тізілімін бақылайды, руткиттерді анықтайды, берілген уақытта және қандай да бір оқиға анықталса хабарлайды. Ол Linux, OpenBSD, FreeBSD, Mac OS X, Solaris және Windows сияқты операциялық жүйелердің көпшілігі үшін кіруді анықтау функциясын ұсынады. Оның кроссплатформлы архитектурасы бірнеше операциялық жүйелерді оңай басқаруға және бақылауға мүмкіндік береді. 2004 жылдан бастап қол жетімді.

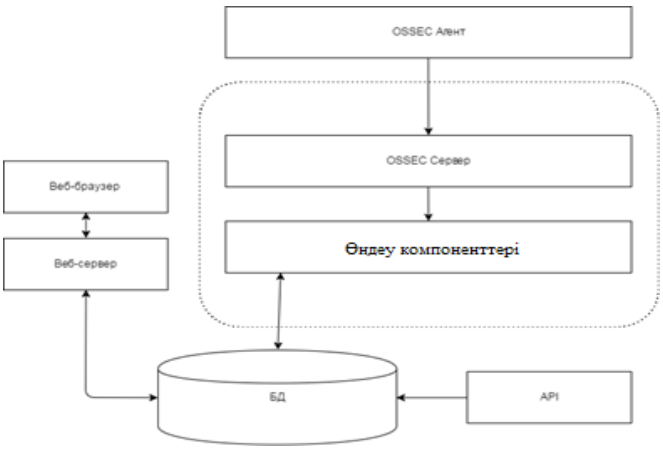
OSSEC мүмкіндіктері PCI DSS кейбір ережелерін сақтайды. 2008 жылдың маусым айында OSSEC жобасы және жоба көшбасшысы Даниэл Б. Сидке тиесілі барлық копирайттар Third Brigade компаниясы сатып алды. Компания бағдарлама әзірлеуін Open Source қауымдастығымен бірге біріктіруге және OSSEC пайдаланушыларына коммерциялық қолдау мен оқытуды ұсынуға міндеттенеді.

OSSEC логтарды өте егжей-тегжейлі талдау жүргізеді, бағдарлама бірнеше форматтағы бірнеше қосымшаларды бір мезгілде салыстыра және талдай алады. Бақылау үшін келесі қолданбаларды қолдайды:

- unix-ерекшеліктері: Unix PAM, sshd (OpenSSH), Solaris telnetd, Samba, Su, Sudo;
- FTP серверлері: ProFTPd, Pure-FTPd, vsftpd, Microsoft FTP Server, Solaris ftpd;
- пошта серверлері: Imapd and pop3d, Postfix, Sendmail, vpopmail, Microsoft Exchange Server;
- деректер базасын: PostgreSQL, MySQL;
- Web-серверлер: Apache HTTP Server (логтар мен қолжетімділік және қателер), IIS web server (NSCA және W3C кеңейтімдерін қоса алғанда), Zeus Web Server қателерінің логині;
- интернет-қосымшалар: Horde IMP, SquirrelMail, Modsecurity;
- фаерволлдар: Iptables, Solaris IPFilter, AIX ipsec / firewall, Netscreen, Windows Firewall, Cisco PIX, Cisco FWSM, Cisco ASA;
- NIDS: Cisco IOS, IDS/IPS модулі, Snort IDS (snort full, snort fast және snort syslog);
- қауіпсіздікті қамтамасыз етуге арналған утилиттер: Norton AntiVirus, Nmap, Arpwatch, Cisco VPN Concentrator;
- басқалар: Named (BIND), Squid proxy, Zeus eXtensible Traffic Manager;
- Windows оқиғаларының логтері (логин, логон, аудитке арналған ақпараттар және басқалар)Ғ
- Windows маршрутизациялау және қашықтан кіру логині;
- аутентификация құралдары unix (adduser, логиндер және басқалар).

OSSEC HIDS (3.1-сурет) агенттік құрылымда жасалған. Агент зерттелетін серверде орнатылған шағын мониторинг бағдарламасын ұсынады, ол кезең-кезеңімен талдау үшін OSSEC серверлік бөлігінің алынған деректерін жинайды және жібереді. Серверлік бөлім түрлі параметрлерді, ережелерді және файлдарды тексеру, сақтау, декодинг және тәуелділікті іздеу үшін қызмет етеді.

Жүйе мониторингі мен әкімшілендірудің тиімділігін арттыру мақсатында қазіргі уақытта OSSEC (жаңа қолдау көрсетілмейтін есептілік жүйелерін, сервистерді және т.б. іске қосу) беретіндігімен салыстырғанда өңдеу мүмкіндіктерін кеңейту үшін қосымша компоненттерді әзірлеу және веб-интерфейс және бөгде сервистер арқылы тиісті өңдеу параметрлерін баптау туралы шешім қабылданды [11].



Сурет 3.1 – OSSEC жұмыс істеу архитектурасы

3.3 Бағдарламаның техникалық сипаттамасы

Бағдарлама «PyCharm» әзірлеу ортасында жасалды. Қолданылған бағдарламалау тілі python 3.6. Бағдарламада келесі кітапханалар мен модульдер қолданылды: re, datefinder, sqlite3, logging. Деректер қорымен басқару жүйесі «Oracle Database», виртуалды орталарды қорғау шешімі қауіпсіздік коды «vGate», IDS жүйесі «NetDefendOS» негізгі лог файлдар өңдеу үшін алынған ақпарат көздері болып алынды.

Python (орыс тілінде питон атауы кең таралған) – жалпы мақсаттағы бағдарламалау тілі. Python ядросының синтаксисі өте аз. Сонымен қатар стандартты кітапхана пайдалы функциялардың үлкен көлемін қамтиды.

Python құрылымдық, объектілі-бағытталған, функционалдық, императивті және аспектілі-бағытталған бағдарламалауды қолдайды. Негізгі архитектуралық ерекшеліктер – динамикалық типизация, жадыны автоматты басқару, толық интроспекция, ерекшеліктерді өңдеу механизмі, көп ағынды есептеулерді қолдау, деректердің жоғары деңгейлі құрылымы. Өз кезегінде, пакеттерге бірігуі мүмкін модульдерге бағдарламаларды бөлу қолдайды.

Python – белсенді дамып келе жатқан бағдарламалау тілі, тілдік қасиеттерді қосу/өзгерту жаңа нұсқалары шамамен екі жарым жылда бір рет шығады. Тіл ресми стандарттауға ұшырамады, де-факто стандартының рөлін тіл авторының бақылауымен жасалған CPython орындайды.

Тұрақты өрнектер (regular expressions) – бұл Python ішінде және басқа да бағдарламалау тілдерінде пайдалануға болатын шағын тіл. Жиі "regex", "regexp" немесе жай ғана "RE", яғни "reuglar expressions" түрінде кездеседі. Perl және Ruby сияқты тілдер шын мәнінде өз тілінде тұрақты өрнектердің синтаксисін қолдайды. Python тілінде импорттау қажет кітапхана арқасында қолдайды. Тұрақты өрнектерді негізгі қызметі – жолдарды салыстыру. Тұрақты өрнектерді пайдалана отырып, жолдарды салыстыру ережелерін жасалады,содан кейін оларды қандай да бір салыстырулардың бар-жоғын көру үшін жолда қолданылады. Тұрақты өрнектердің "тілі" шын мәнінде өте қысқа, сондықтан жолдарды салыстыру кезінде барлық мұқтаждар үшін пайдалана

алуыңыз екіталай. Сонымен қатар, тұрақты сөздерді пайдаланатын міндеттермен жұмыс істей отырып, процесті айтарлықтай қиындап кетуі мүмкін, ал мұндай жағдайда багтарды емдеу өте қиын. Мұндай жағдайларда көбінесе жай ғана Python пайдалану керек. Python – оның құқықтары бойынша мәтіндерді парсинг үшін өте ыңғайлы тіл, және оны сіз тұрақты өрнектермен істеп жатқан барлық жерде қолдануға болады. Дегенмен, бұл көп код қажет болуы мүмкін және тұрақты өрнектер баяу жұмыс істейтін болады, өйткені олар C тілінде компилденген және орындалған.

SQLite – бұл транзакциялық механизмдегі серверсіз жұмыс істейтін автономды SQL деректер қоры. Python 2.5 нұсқасында sqlite3 модулін алды, бұл дегеніміз қосымша құралдарды жүктеудің қажетінсіз Python осы нұсқасында SQLite деректер базасын жасай аласыз. Mozilla SQLite деректер базасын өзінің танымал Firefox браузерінде бетбелгілерді және басқа да әр түрлі ақпаратты сақтау үшін пайдаланады. Егер деректер базасын көзбен шолып тексеру қажеттілігі туса, Firefox-те SQLite Manager плагинін пайдалануға болады, немесе командалық жолда SQLite Python командалық жолының қабығын пайдалануға болады. SQLite сұраулары MySQL немесе Postgres сияқты басқа дерекқорларда пайдаланатындарға өте ұқсас. Қарапайым SQL синтаксисін сұрауларды орындау үшін пайдаланылады, содан кейін cursor нысаны SQL орындайды.

Парсинг (Parsing) – бұл информатикада қабылданған синтаксистік талдаудың анықтамасы. Ол үшін программалау тілдерінің бірі сипатталған лексиканы формальды грамматикамен салыстырудың математикалық моделі жасалады. Компьютерге "оқу" мүмкіндігін беретін бағдарлама (скрипт) – ұсынылған сөздерді дүниежүзілік желіде бар сөздерді салыстыру парсер деп аталады. Мұндай бағдарламаларды қолдану аясы өте кең, бірақ олардың барлығы дерлік бір алгоритм бойынша жұмыс істейді.

Python стандартты кітапханада logging логикалық кітапхананы ұсынады. Көптеген бағдарламашылар бағандарды емдеу үшін print операторын пайдаланады, бірақ осы мақсаттар үшін логиканы пайдалану аса ұқыптылықтың үлгісі. Логды пайдалану, сондай-ақ, барлық print операторларын жою үшін бүкіл кодты көрмеудегі таза әдіс.

Datetime модулі келесі сыныптардан тұрады:

- datetime.date;
- datetime.timedelta;
- datetime.datetime.

Осы кластардың арқасында date және datetime нысандары қажет болатын жағдайлардың көп бөлігімен жұмыс істеуге болады. Сондай-ақ, сағат белдеулерімен жұмыс істеу үшін қолданылатын tzinfo сыныбы бар (3.2-сурет).

Бағдарламаны келесі бөлімдерге бөлуге болады:

1) кітапханаларды жүктеу;

2) деректер қорын тексеру, тексеру үшін try конструкциясы қолданылады, яғни деректер қоры болмаса жаңадан жасау, болса компилятор бұл жолды өтіп кетеді;

3) циклдік тексеру жасау: for line in s,

мұндағы s – тексеріліп отырған лог мәні;

4) парсинг (3.3-сурет), бұл бағдарламаның ең үлкен бөлімі болып табылады. Жоғарыда айтылған форматтың әр бағанында өзіндік ерекшелігі бар парсер жазылған. Бірақ олардың алгоритмдері біреу. Ең бірінші берілген лог файлдан ақпарат ізделінеді. Ол re кітапханасы көмегімен іске асады:

wq = re.findall(r'\bPID=(\d{3})', line).

Ізделінген ақпарат форматтың өзіндік айнымалысына беріледі. Кейін айнымалының мәннің сәйкес келуіне тексеріледі:

if wq != 0.

Егер мән сәйкес келетін болса лог форматындағы файлға жазылады:

f.write("PID NUMBER="+str(wq)).

Басты назар аударатын жағдай ол айнымалының өз мәнін сақтап қалуында. Бұл мән деректер қорына енгізуде қолданылады.

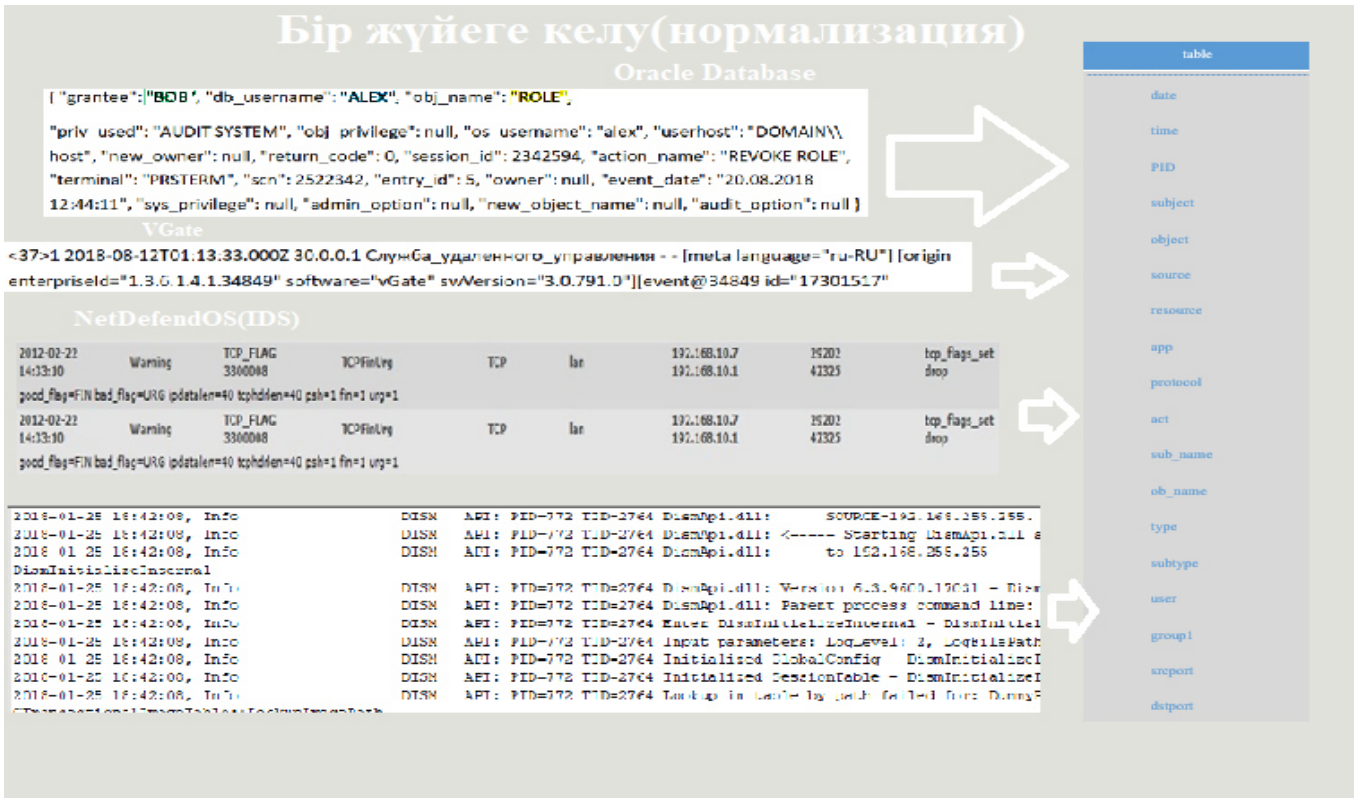
Деректер қорына енгізу процесі. Айнымалы мәндері бір массивке жинақталып деректер қоырна енеді:

firsts = [(str(date), str(time), str(subjec), str(objec), str(source), str(resource))]

cur.executemany("INSERT INTO first VALUES (?, ?, ?, ?, ?, ?)", firsts)

conn.commit().

1. Цикл біткеннен кейін деректер қоры жабылады.



Сурет 3.2 – Нормализациялау процессі

Oracle Database жүйесінен келген деректер келесі форматта көрсетілген: “grantee” – рөл беруші, “db_username” – рөл тиесілі пайдаланушы , “obj_name” – объект типі, “priv_used” – қолданылған артықшылықтары (привилегия), “obj_privilege” – объекті артықшылықтары, “os_username” - қолданушы, “userhost” – жүйенің домені, “new_owner” – жаңа иесі, “return_code” – қайтарушы код, “session_id” – сессия нөмірі, “action_name” – әрекет аты, “terminal” - терминал, “scn” – қордағы уақыт нүктесі, “entry_id” – бастауыш нөмір, “event_date” – оқиға болған күн, “time” - уақыт, “sys_privilege” – жүйелік артықшылықтар, “admin_option” – басқа пайдаланушыға беру мүмкіндігі, “new_object_name” – жаңа пайда болған объект атауы, “audit_option” – аудит кеңейтпелері.

NetDefentOs келесі форматта көрсетіледі: “date” – оқиға уақыты (күні және уақыты), “level” – оқиға деңгейоқиға деңгейі, “object_name” – объект атауы, “object_settings” – объект қосымшасы, “protocol” - хаттама, “network” - желі, “src” – ақпарат көзі IP-адресі, “resouce” – ақпарат жеткізуші IP-адресі, “src_port” - жіберуші порт нөмірі, “dst_port” – қабылдаушы порт нөмірі, “action” –әрекет.

vGate келесі форматта көрсетіледі: “date” – оқиға күні, “time” - уақыты, “meta language” - тілі, “software” – ақпарат көзі, “swVersion” - нұсқасы, “event_id” – оқиға нөмірі, “category” - санаты, “subject” – субъект IP-адресі, “subject_name” – субъект аты, “action” – әрекет, “object_name” – өзгеріс негізі (объект).

```
2018-01-25 18:42:21, Info                  DISM   DISM Package Manager: PID=1100 TID=832 Feature MSMQ-Multicast with CBS state 4(CbsInstallStateStaged) being mapped t
2018-01-25 18:42:21, Info                  DISM   DISM Package Manager: PID=1100 TID=832 Feature MSMQ-DCOMProxy with CBS state 4(CbsInstallStateStaged) being mapped t
2018-01-25 18:42:21, Info                  DISM   DISM Package Manager: PID=1100 TID=832 Feature MSMQ-RoutingServer with CBS state 4(CbsInstallStateStaged) being mapp
2018-01-25 18:42:21, Info                  DISM   DISM Package Manager: PID=1100 TID=832 Feature WCF-Services45 with CBS state 7(CbsInstallStateInstalled) being mappe
2018-01-25 18:42:21, Info                  DISM   DISM Package Manager: PID=1100 TID=832 Feature WCF-HTTP-Activation45 with CBS state 4(CbsInstallStateStaged) being m
2018-01-25 18:42:21, Info                  DISM   DISM Package Manager: PID=1100 TID=832 Feature WCF-TCP-Activation45 with CBS state 4(CbsInstallStateStaged) being ma
2018-01-25 18:42:21, Info                  DISM   DISM Package Manager: PID=1100 TID=832 Feature WCF-Pipe-Activation45 with CBS state 4(CbsInstallStateStaged) being m
2018-01-25 18:42:21, Info                  DISM   DISM Package Manager: PID=1100 TID=832 Feature WCF-MSMQ-Activation45 with CBS state 4(CbsInstallStateStaged) being m
2018-01-25 18:42:21, Info                  DISM   DISM Package Manager: PID=1100 TID=832 Feature WCF-TCP-PortSharing45 with CBS state 7(CbsInstallStateInstalled) bein
2018-01-25 18:42:21, Info                  DISM   DISM Package Manager: PID=1100 TID=832 Feature ManagementOdata with CBS state 4(CbsInstallStateStaged) being mapped
2018-01-25 18:42:21, Info                  DISM   DISM Package Manager: PID=1100 TID=832 Feature DSC-Service with CBS state 4(CbsInstallStateStaged) being mapped to d
2018-01-25 18:42:21, Info                  DISM   DISM Package Manager: PID=1100 TID=832 Feature IdentityServer-SecurityTokenService with CBS state 4(CbsInstallStateS
2018-01-25 18:42:21, Info                  DISM   DISM Package Manager: PID=1100 TID=832 Feature Application-Server with CBS state 4(CbsInstallStateStaged) being mapp
2018-01-25 18:42:21, Info                  DISM   DISM Package Manager: PID=1100 TID=832 Feature AS-NET-Framework with CBS state 4(CbsInstallStateStaged) being mapped
2018-01-25 18:42:21, Info                  DISM   DISM Package Manager: PID=1100 TID=832 Feature Application-Server-WebServer-Support with CBS state 4(CbsInstallState
2018-01-25 18:42:21, Info                  DISM   DISM Package Manager: PID=1100 TID=832 Feature AS-Ent-Services with CBS state 4(CbsInstallStateStaged) being mapped
2018-01-25 18:42:21, Info                  DISM   DISM Package Manager: PID=1100 TID=832 Feature Application-Server-TCP-Port-Sharing with CBS state 4(CbsInstallStateS
2018-01-25 18:42:21, Info                  DISM   DISM Package Manager: PID=1100 TID=832 Feature Application-Server-WAS-Support with CBS state 4(CbsInstallStateStaged
2018-01-25 18:42:21, Info                  DISM   DISM Package Manager: PID=1100 TID=832 Feature Application-Server-HTTP-Activation with CBS state 4(CbsInstallStateSt
2018-01-25 18:42:21, Info                  DISM   DISM Package Manager: PID=1100 TID=832 Feature Application-Server-MSMQ-Activation with CBS state 4(CbsInstallStateSt
2018-01-25 18:42:21, Info                  DISM   DISM Package Manager: PID=1100 TID=832 Feature Application-Server-TCP-Activation with CBS state 4(CbsInstallStateSta
2018-01-25 18:42:21, Info                  DISM   DISM Package Manager: PID=1100 TID=832 Feature Application-Server-Pipe-Activation with CBS state 4(CbsInstallStateSt
2018-01-25 18:42:21, Info                  DISM   DISM Package Manager: PID=1100 TID=832 Feature AS-Dist-Transaction with CBS state 4(CbsInstallStateStaged) being map
2018-01-25 18:42:21, Info                  DISM   DISM Package Manager: PID=1100 TID=832 Feature AS-Incoming-Trans with CBS state 4(CbsInstallStateStaged) being mappe
2018-01-25 18:42:21, Info                  DISM   DISM Package Manager: PID=1100 TID=832 Feature AS-Outgoing-Trans with CBS state 4(CbsInstallStateStaged) being mappe
2018-01-25 18:42:21, Info                  DISM   DISM Package Manager: PID=1100 TID=832 Feature AS-WS-Atomic with CBS state 4(CbsInstallStateStaged) being mapped to
2018-01-25 18:42:21, Info                  DISM   DISM Package Manager: PID=1100 TID=832 Feature ADCertificateServicesRole with CBS state 4(CbsInstallStateStaged) bei
2018-01-25 18:42:21, Info                  DISM   DISM Package Manager: PID=1100 TID=832 Feature CertificateServices with CBS state 4(CbsInstallStateStaged) being map
2018-01-25 18:42:21, Info                  DISM   DISM Package Manager: PID=1100 TID=832 Feature OnlineRevocationServices with CBS state 4(CbsInstallStateStaged) bein
2018-01-25 18:42:21, Info                  DISM   DISM Package Manager: PID=1100 TID=832 Feature WebEnrollmentServices with CBS state 4(CbsInstallStateStaged) being m
2018-01-25 18:42:21, Info                  DISM   DISM Package Manager: PID=1100 TID=832 Feature NetworkDeviceEnrollmentServices with CBS state 4(CbsInstallStateStage
```

Сурет 3.3 – Өңдеуге дейінгі ақпарат сұлбасы

ddd.log — Блокнот

Файл Правка Формат Вид Справка

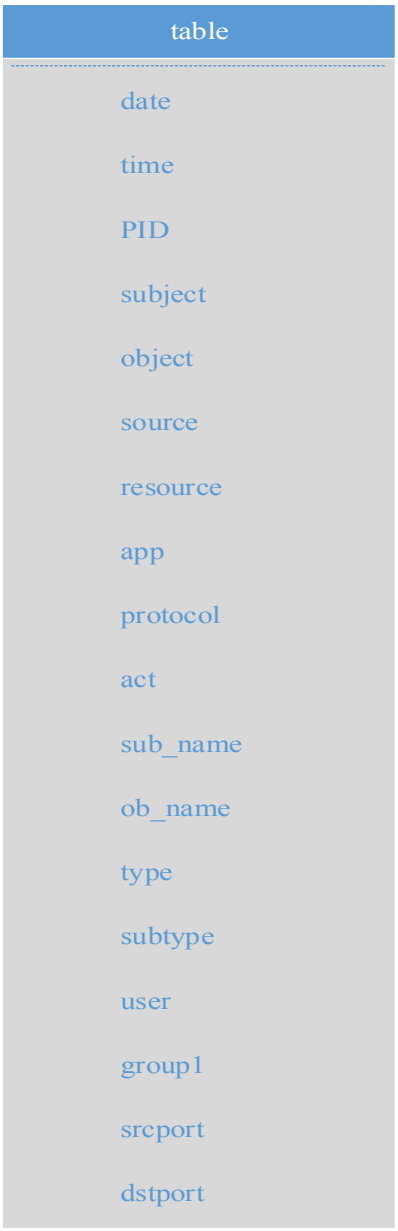
```
date=2018-01-25, time=18:42:13, PID NUMBER=['772'] type=['Info']
date=2018-01-25, time=18:42:13, PID NUMBER=['772'] type=['Info']
date=2018-01-25, time=18:42:13, PID NUMBER=['772'] type=['Info']
date=2018-01-25, time=18:42:14, PID NUMBER=['772'] type=['Info']
date=2018-01-25, time=18:42:14, PID NUMBER=['1100'] type=['Info']
date=2018-01-25, time=18:42:14, PID NUMBER=['1100'] type=['Info']
date=2018-01-25, time=18:42:14, PID NUMBER=['1100'] type=['Info']
date=2018-01-25, time=18:42:14, PID NUMBER=['1100'] type=['Info']
date=2018-01-25, time=18:42:14, PID NUMBER=['1100'] type=['Info']
date=2018-01-25, time=18:42:14, PID NUMBER=['1100'] type=['Info']
date=2018-01-25, time=18:42:14, PID NUMBER=['1100'] type=['Info']
date=2018-01-25, time=18:42:14, PID NUMBER=['1100'] type=['Info']
date=2018-01-25, time=18:42:14, PID NUMBER=['1100'] type=['Info']
date=2018-01-25, time=18:42:14, PID NUMBER=['1100'] type=['Info']
date=2018-01-25, time=18:42:14, PID NUMBER=['1100'] type=['Info']
date=2018-01-25, time=18:42:14, PID NUMBER=['1100'] type=['Info']
date=2018-01-25, time=18:42:14, PID NUMBER=['1100'] type=['Info']
date=2018-01-25, time=18:42:14, PID NUMBER=['1100'] type=['Info']
date=2018-01-25, time=18:42:14, PID NUMBER=['1100'] type=['Info']
date=2018-01-25, time=18:42:14, PID NUMBER=['1100'] type=['Warning']
date=2018-01-25, time=18:42:14, PID NUMBER=['1100'] type=['Info']
date=2018-01-25, time=18:42:14, PID NUMBER=['1100'] type=['Info']
date=2018-01-25, time=18:42:14, PID NUMBER=['1100'] type=['Info']
date=2018-01-25, time=18:42:14, PID NUMBER=['1100'] type=['Info']
date=2018-01-25, time=18:42:14, PID NUMBER=['772'] type=['Info']
date=2018-01-25, time=18:42:14, PID NUMBER=['1100'] type=['Info']
date=2018-01-25, time=18:42:14, PID NUMBER=['1100'] type=['Info']
date=2018-01-25, time=18:42:14, PID NUMBER=['772'] type=['Info']
date=2018-01-25, time=18:42:14, PID NUMBER=['772'] type=['Info']
date=2018-01-25, time=18:42:14, PID NUMBER=['772'] type=['Info']
date=2018-01-25, time=18:42:14, PID NUMBER=['772'] type=['Info']
date=2018-01-25, time=18:42:14, PID NUMBER=['772'] type=['Info']
```

Сурет 3.4 – Өңдеуден кейінгі ақпарат сұлбасы

3.4-суретте ақпарат толық берілмесе, яғни берілген форматтағы деректер табылмаса, жоқ деректердің орны бос қалдырылады. Тек қажетті ақпарат қана тіркеледі. 3.5-суретте толығырақ сипатталатын ақпарат көзінен алынғанын байқауға болады. 3.6-суретте дерек форматы көрсетілген.

```
date=2018-01-25, time=18:42:08, PID NUMBER=['772'] subject=['Beka'] protocol=['TCP'] type=['Info'] user=['Beka'] group=['amer'] SOURCE=192.168.255.255
date=2018-01-25, time=18:42:08, PID NUMBER=['772'] protocol=['TCP']type=['Info'] SOURCE=192.168.255.255
date=2018-01-25, time=18:42:08, PID NUMBER=['772'] protocol=['TCP']type=['Info'] SOURCE=192.168.255.255
date=2018-01-25, time=18:42:08, PID NUMBER=['772']  subject=['192.168.255.255'] protocol=['TCP']type=['Info'] SOURCE=192.168.255.255
date=2018-01-25, time=18:42:08, PID NUMBER=['772'] protocol=['TCP']type=['Info'] SOURCE=192.168.255.255
date=2018-01-25, time=18:42:08, PID NUMBER=['772']  subject=['Akezhan'] protocol=['TCP']type=['Info']user=['Akezhan']group=['amer'] SOURCE=192.168.255.255
date=2018-01-25, time=18:42:08, PID NUMBER=['772'] protocol=['TCP']type=['Info'] SOURCE=192.168.255.255
date=2018-01-25, time=18:42:08, PID NUMBER=['772']  subject=['Akezhan'] protocol=['TCP']type=['Info']user=['Akezhan']group=['amer'] SOURCE=192.168.255.255
date=2018-01-25, time=18:42:08, PID NUMBER=['772'] protocol=['TCP']type=['Info'] dstport=['20'] SOURCE=192.168.255.255
date=2018-01-25, time=18:42:08, PID NUMBER=['772'] protocol=['TCP']type=['Info'] dstport=['20'] SOURCE=192.168.255.255
date=2018-01-25, time=18:42:08, PID NUMBER=['772'] protocol=['TCP']type=['Info'] srcport=['88'] SOURCE=192.168.255.255
date=2018-01-25, time=18:42:08, PID NUMBER=['772'] protocol=['TCP']type=['Info'] dstport=['20'] SOURCE=192.168.255.255
date=2018-01-25, time=18:42:09, PID NUMBER=['772'] protocol=['TCP']type=['Info'] dstport=['20'] SOURCE=192.168.255.255
date=2018-01-25, time=18:42:09, PID NUMBER=['772'] protocol=['TCP']type=['Info'] dstport=['20'] SOURCE=192.168.255.255
date=2018-01-25, time=18:42:09, PID NUMBER=['772']  subject=['Akezhan'] type=['Info']user=['amer'] SOURCE=192.168.255.255
date=2018-01-25, time=18:42:09, PID NUMBER=['772'] protocol=['DNS']type=['Info'] dstport=['20'] SOURCE=192.168.255.255
date=2018-01-25, time=18:42:09, PID NUMBER=['772'] protocol=['TCP']type=['Info'] dstport=['20'] SOURCE=192.168.255.255
date=2018-01-25, time=18:42:10, PID NUMBER=['772'] protocol=['TCP']type=['Info'] dstport=['20'] SOURCE=192.168.255.255
date=2018-01-25, time=18:42:10, PID NUMBER=['772'] type=['Info'] dstport=['20'] SOURCE=192.168.255.255
date=2018-01-25, time=18:42:10, PID NUMBER=['772'] type=['Info'] dstport=['20'] SOURCE=192.168.255.255
date=2018-01-25, time=18:42:10, PID NUMBER=['772'] protocol=['TCP']type=['Info'] dstport=['20'] SOURCE=192.168.255.255
date=2018-01-25, time=18:42:10, PID NUMBER=['772'] type=['Info'] dstport=['20'] SOURCE=192.168.255.255
date=2018-01-25, time=18:42:10, PID NUMBER=['772'] protocol=['TCP']type=['Info'] dstport=['20'] SOURCE=192.168.255.255
date=2018-01-25, time=18:42:10, PID NUMBER=['772'] protocol=['TCP']type=['Info'] dstport=['20'] SOURCE=192.168.255.255
```

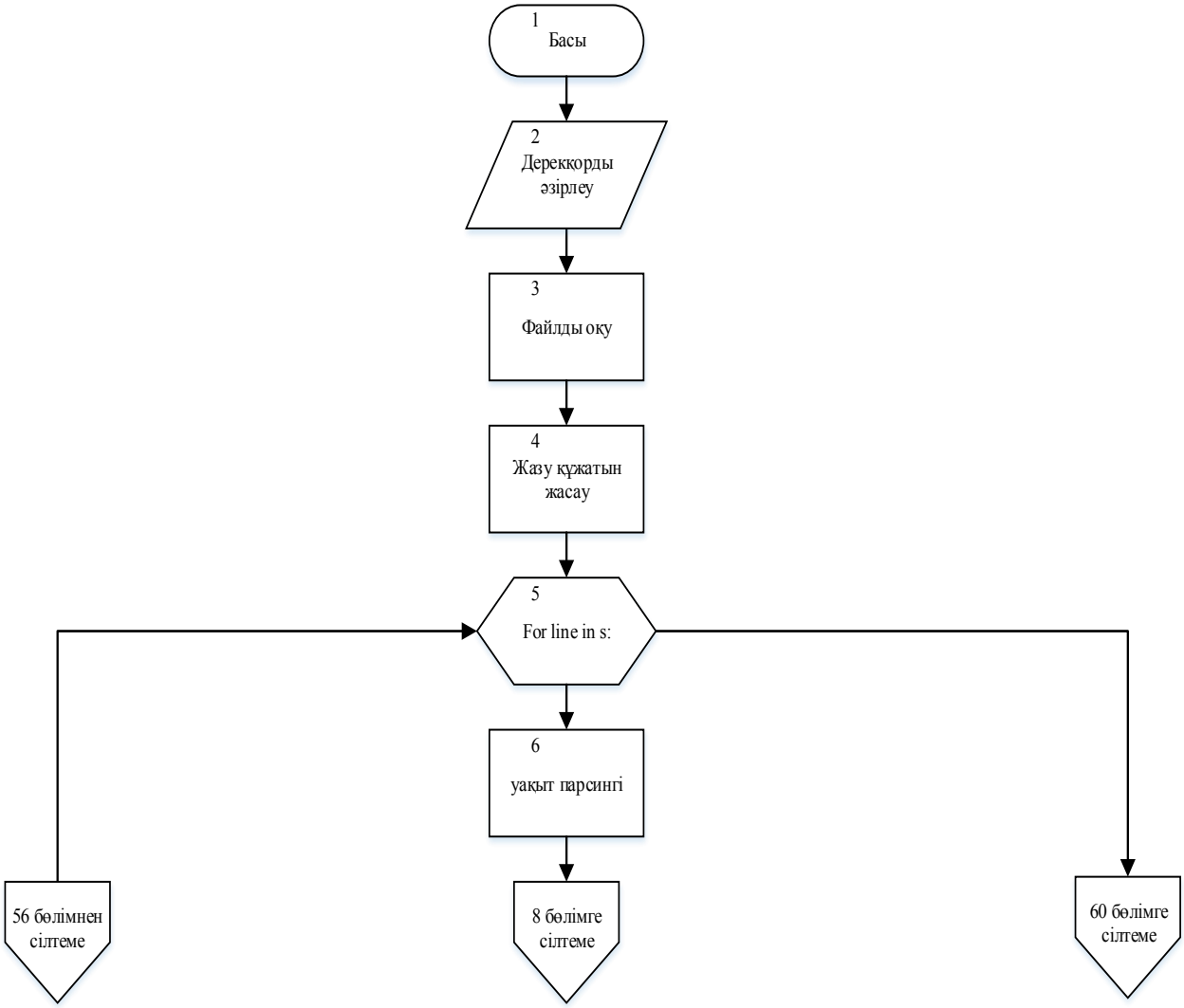
Сурет 3.5 – Екінші ақпарат көзінен алынған ақпарат сұлбасы



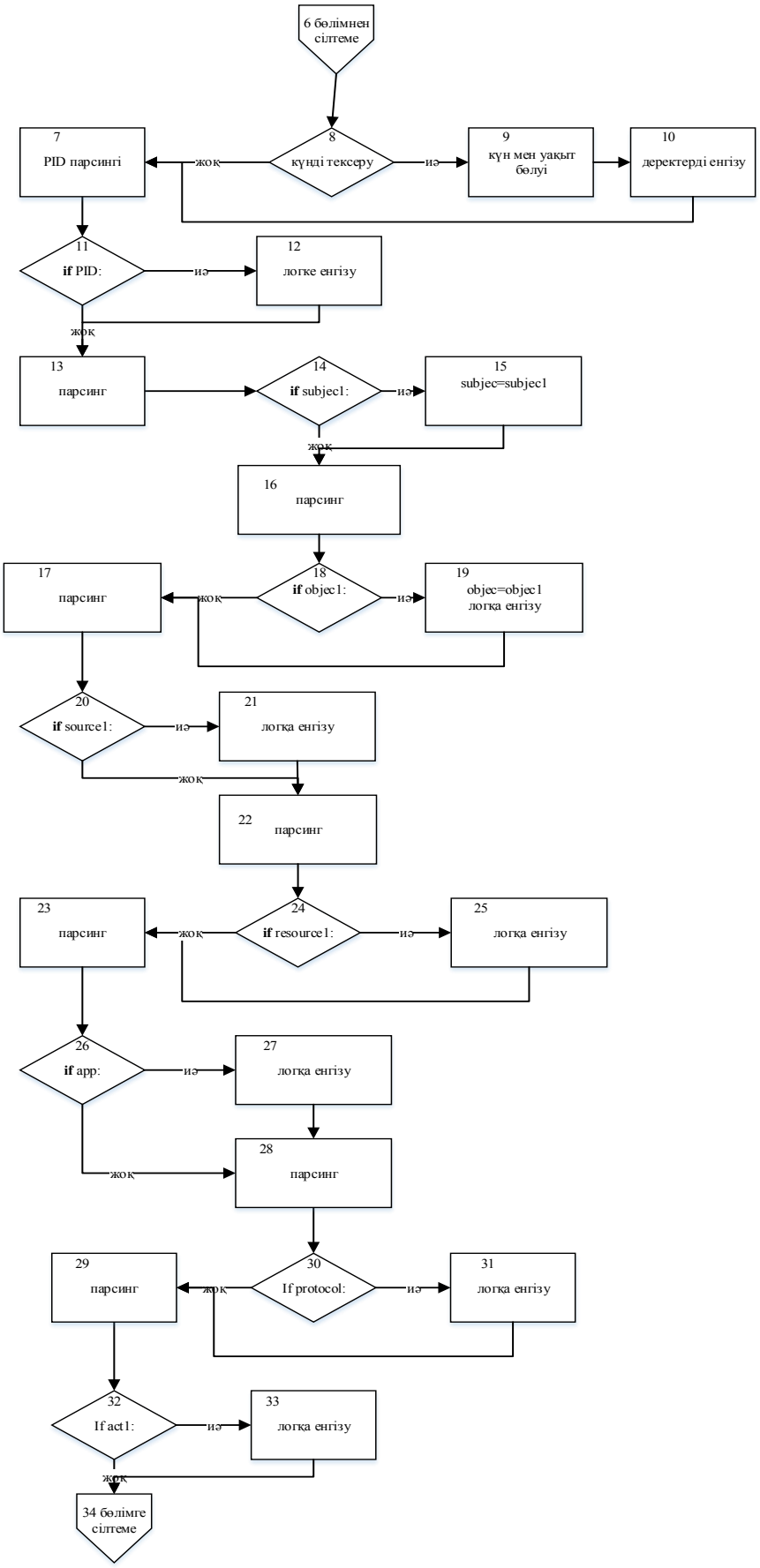
Сурет 3.6 – Дерекқорда жасалған кесте түрі

Мұндағы: date – оқиға болған күні;
time – оқиға болған уақыт;
PID – процесс идентификаторы (ағылшынша process identifier) көп қызметті операциялық жүйеде (ОЖ) процестің бірегей нөмірі (идентификатор);
subject – субъектінің IP-адресі;
object – объектінің IP-адресі ;
source – ақпарат көзінің IP-адресі ;
resource – ақпарат жеткізушінің IP-адресі;
app – қосымша (приложение) атауы;
protocol – хаттама атауы;

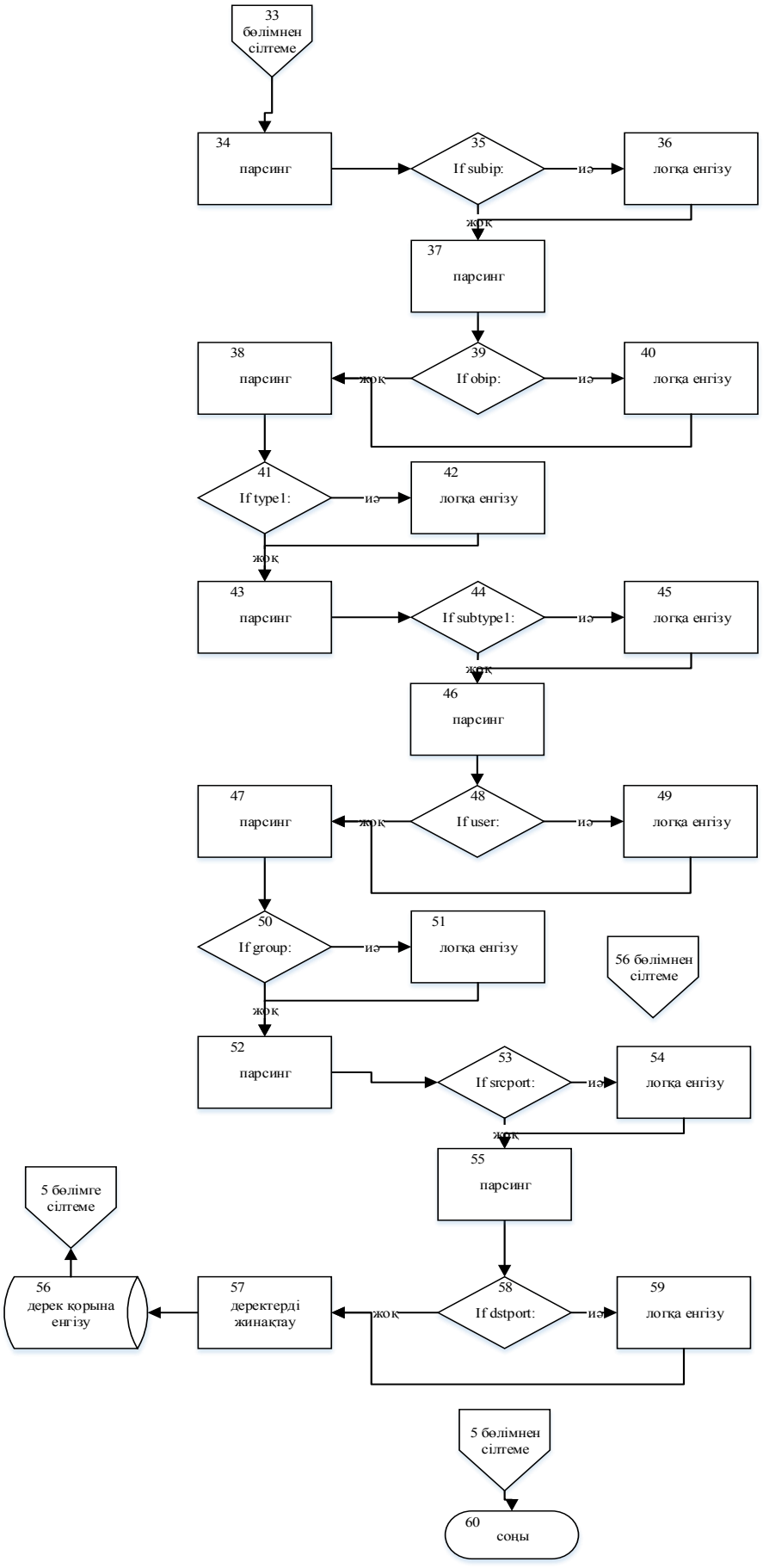
sub_name – субъектінің аты;
ob_name – объектінің аты;
type – оқиға типі;
subtype – оқиға деңгейі;
user – пайдаланушы аты;
group1 – пайдаланушы бөлімі;
srcport – ақпарат көзінің порты;
dstport – қабылдаушының порты.



Сурет 3.7 – Құрылған бағдарламаның блок-сызбасы



Сурет 3.8 – Құрылған бағдарламаның блок-сызбасы



Сурет 3.9 – Құрылған бағдарламаның блок-сызбасы

4 Өмір тіршілік қауіпсіздігі

4.1 Электрмагниттік өрісінің қауіпі және зиянды факторлары

Электромагниттік радиация магниттік энергиядан және электромагниттік толқындар арқылы пайда болады. Барлық электромагниттік энергия электромагниттік спектрге түседі, олар өте төменгі радиацияның жиілігінен ренгендік және гамма-сәулелеріне дейін өзгереді.

Иондаушы емес электромагниттік сәулелену мен өрістерге оптикалық және радиожиілікті диапазонындағы электромагниттік сәулеленулерді, сонымен қатар шартты-статикалық электрлік және тұрақты магниттік өрістерді жатқызу қабылданған.

Электромагниттік сәулеленулер (ЭМС) толқын ұзындығымен – λ (м), тербеліс жиілігімен – f (Гц) және таралу жылдамдығымен – V (м/с) сипатталатын элктромагниттік толқындар түрінде таралады. Бос кеңістікте ЭМС таралу жылдамдығы жарық жылдамдығына тең $C = 3 \cdot 10^8$ м/с.

Табиғи иондаушы емес сәулеленулер мен өрістер салыстырмалы түрде жақын арада зерттеле бастады және соңғы он жылдықтарда жерде тіршілік пайда болуында, одан әрі дамуы мен реттелуінде олардың маңызды ролі дәлелденді. Табиғи электромагниттік өрістердің спектрін шартты түрде бірнеше құрам бөліктеріне бөлуге болады. Олар жердің тұрақты магниттік өрісі, немесе геомагнитті өріс (ГМӨ), және 10^{-3}-нен 1012 Гц дейінгі жиілік диапазонындағы электростатикалық өріс пен айнымалы электромагниттік өрістер [12].

Табиғи электромагниттік өрістер, оның ішінде геомагнитті өріс ағзаға әр түрлі әсер етуі мүмкін. Бір жағынан, геомагниттік ауытқулар экологиялық қауіп-қатер факторы ретінде қарастырылады – биологиялық ырғақтардың, мидың функционалдық жағдайы модуляциясының синхрондылығын бұзады, клиникалық тұрғыдан ауыр медициналық патологиялар (миокард инфарктысын, инсульттерді, жол-көлік жағдайлары мен апаттарын, соның ішінде әуе апаттарының) санының өсуіне себеп болады. Басқа жағынан, ГМӨ-нің кезеңдік емес түрінің циркадтық, инфрадтық және циркосептадтық биологиялық ырғақтармен және олардың ара қатынастарымен байланысы анықталған.

Ағзаға тек магниттік толқу (буря) ғана қолайсыз әсер етіп қоймайды, сонымен қатар, адамның әлсіз электромагниттік өріс жағдайында ұзақ уақыт болуы факторы да, оның ішінде, жұмысы экрандалған бөлмелер мен құрылыстарда істелетін бірқатар өндірістерде де қолайсыз әсер етуі мүмкін. Мұндай жағдайда жұмыс істеушілер жиі көңіл-күйінің және денсаулығының нашарлағанына шағымданады, бұл-геомагниттік өрістің әсерін зерттейтін гигиенаның жаңа бағытының пайда болуына негіз болды. Геомагниттік өрістің төмен деңгейі тек экрандалған құрылыстарда ғана емес, сонымен қатар метрополитеннің жерасты құрылыстарында (2-5 есе), темір-бетонды конструкциялардан салынған ғимараттарда (1,3-2,3 есе), тез жүретін лифт

кабинасында (15-19 есе), бұрғылау қондырғылары мен эксковаторлардың кабиналарында, жеңіл автокөліктердің салонында (1,5-3 есе) және басқаларда да байқалады [12].

Радиожиілікті диапазонындағы электромагниттік сәулеленулерге (ЭМС) жиілігі 3-тен $3 \cdot 10^{12}$ Гц дейінгі (100000км-ден 0,1 мм дейінгі толқын ұзындығы сәйкес келетін) электромагниттік өрістер (ЭМӨ) жатады. Халықаралық регламентке сәйкес жиілігіне және толқын ұзындығына байланысты, 12 кіші диапазондарға бөлінеді.

Электромагниттік тербелістердің ең жиі кездесетін екі түрін ажыратады – үйлесімді және өзгертілген.

Үйлесімді тербелістерде электрлік (Е) және магниттік (Н) құрамдастар синус немесе косинус заңы бойынша өзгереді. Өзгертілген тербелістер кезінде амплитудасы мен жиілігі белгілі бір заң бойынша өзгереді.

Радиожиілікті диапазонындағы электромагниттік сәулеленудің көздері халық шаруашылығының әр түрлі салаларында қолданылады: қашықтан ақпараттарды беру үшін (радиохабарлар, радиотелефонды байланыс, теледидар, радиолокация және басқаларда). Өнеркәсіптерде радиотолқынды диапазондағы электромагниттік сәулеленулер материалдарды индукциялық және диэлектрлік қыздыру үшін қолданылады. Ғылыми зерттеулерде электромагниттік сәулеленулер радиоспектроскопияда, радиоастрономияда, медицинада– физиотерапияда, сондай-ақ хирургтар мен онкологтар практикасында қолданылады. Электрлік берілістің әуе желісінің, трансформаторлық кішістанциялардың, электрқұралдарының, оның ішінде тұрмыстық құралдардың маңайында электрмагниттік сәулелену жанама қолданылмайтын фактор ретінде түзіледі. Қоршаған ортада радиожиілікті электромагниттік өрістердің пайда болатын негізгі көздеріне радио және телерадиостанциялардың, радиолокациялық станциялардың антена жүйелері, сондай-ақ ұялы радиобайланыс жүйелері мен электр берілістерінің әуе желілері жатады.

Адам ағзасы радиожиілікті электрмагниттік өріс әсеріне аса сезімтал болып келеді. Аса сезімтал мүшелер мен жүйелерге ОЖЖ, көз, гонадалар, ал кейбір авторлардың пікірі бойынша қан түзуші жүйелер де жатады. Бұл сәулеленулердің биологиялық әсері толқын ұзындығына (немесе сәулелену жиілігіне), түзілу режиміне (үзіліссіз, импульсті) және ағзаға әсер ету жағдайына (тұрақты, үзілісті, жалпы, жергілікті), әсер ету қарқындылығы мен ұзақтығына байланысты болады.

Биологиялық белсендігі толқын ұзындығы өскен сайын (немесе сәулелену жиілігі төмендеген сайын) азая береді. Радиотолқындардың санти- және дециметрлік диапазондары ең белсенділері болып табылады. Радиожиілікті электромагниттік сәулеленулер тудыратын зақымданулар жедел немесе созылмалы болуы мүмкін. Жедел зақымданулар қарқынды лығы үлкен, айқын жылулық әсері бар сәулеленулер әсер еткен кезде дамиды. Олар өте сирек кездеседі – радиолокациялық станцияларда апаттар болғанда немесе

қауіпсіздік техникасы өрескел бұзылған кезде орын алады. Электромагниттік сәулелену көздерімен жұмыс істейтіндерге, әдетте, ЭМС микротолқынды диапазонындағы көздерімен бірнеше жылдар жұмыс істегеннен кейін анықталатын созылмалы кәсіби зақымданулар көбірек тән. Оның клиникалық көріністерінде үш негізгі синдромды ажыратады: астениялық (бас ауруы, жоғары дәрежеде қажығыштық, ашушаңдық, жүрек тұсында кезеңді түрде пайда болатын ауыру сезімі), астеновегетативтік (гипотония, брадикардия, гипертония түріндегі нейро-циркуляторлы дистония) және гипоталамустық (ұстамалы жыпылық аритмия ұстамалары, қарыншалық электросистолалар, кейіннен ерте пайда болатын атеросклероз, жүректің ишемия аурулары, гипертония ауруы дамиды) Нормативтік құжаттарда электрлік (Е) және магниттік (Н) өрістерге арналған энергетикалық экспозиция (ЭЭ), сондай-ақ, жұмыс күніндегі энергия ағынының тығыздығы (ЭАТ) нормаланады.

Радиожиілікті диапазонының облысында жұмыс істейтін аппараттарға жеке адамдық компьютерлердің терминалдары бейнедисплейлері, сондай-ақ ұялы телефондар жатады.

Өнеркәсіптік жиіліктегі электрмагниттік өрістердің (ӨЖ ЭМӨ) ішінен жиілігі 50 Гц электрмагниттік өрістер өз алдында жеке диапазонға бөлінген. Олардың негізгі көздеріне айнымалы токтың өндірістік және тұрмыстық электржабдықтарының әр түрлі түрлері, сондай-ақ аса жоғары кернеулі (АЖК) электр берілісінің әуе желілері мен подстанциялары жатады. Өнеркәсіптік жиіліктегі электрмагниттік өрістерді гигиеналық бағалау электрлік және магниттік өрістері бойынша жеке-жеке жүргізіледі.

Магнит өрісі нерв жүйесіне тежегіштік әсер етеді. Ал қан айналым жүйесінде, қан тамырларының кеңеюін байқауға болады. Өте күшті магнит өрісінің әсерінен микроорганизмдер өсу жылдамдығы және оның өсу сипаты өзгеріске ұшырайды.

Магнит өрісінің организмге тигізетін әсері мен тірі организм туғызатын магнит өрісін зерттейтін биофизиканың бір саласын магниттік биология деп атайды. Магнит өрісінің адам организміне әсері өте ерте заманнан-ақ зерттелген. Магнит өрісі нерв жүйесіне жақсы әсер ететінін орыс ғалымы С.П.Боткин ашқан. Тіпті магнит өрісімен кез-келген ауруды емдеп жазуға болады деп ғылымда дәлелденген. Жиіліктер келесі топқа бөлінеді:

- төменгі жиілікті: 0-20Гц;
- ультрадыбысты жиілік:20кГц-200кГц;
- ультражоғары жиілікті: 30МГц-300МГц;
- аса жоғары жиілікті:300МГц.

Электромагниттік толқындардың әсерінен әртүрлі аурулар туындайды:

- анкологиялық аурулар;
- Альцгеймер ауруы;
- Паркинсон ауруы.

4.2 Электрмагниттік өрісінің адамға әсері және олардан қорғану шаралары

Электромагнитік өрістің әсері – электр заряды не магниттік моменті бар бөлшектер арасындағы электромагнитік өріс арқылы берілетін белгілі. Адам өмірге келгеннен бастап, электромагнит сәулесінің әсерінде болады. Адамға, жануарларға, өсімдіктерге, микроорганизмдерге жер қыртысынан бөлінетін гамма сәулелер және ғарыш сәулелері сырттан,организмде болатын радиоактивті элементтер сәуелері іштен әсер етеді. Егер бұл сәулелер тірі организмге артық мөлшерде өтсе, клеткалардың, органдардың тіршілігіне қауіпті ауру жабысады.

Радиожиілікті қондырғылар шығаратын электромагниттік сәулелерді мөлшерден көп қабылдаған жағдайда ол адамда мамандық ауруға әкеліп соғады. Нәтижесінде нерв жүйесі жүрек қан тамырлары эндокриналды жүйе және де басқа да ағзаларға әсер етуі мумкін. Электромагниттік өріс әсерінде ұзақ уакыт болған жағдайда адамдар тез шаршайды, ұйқышылдық пайда болады, жиі-жиі басы ауырады, нерв жүйесі бұзылады және тағы да басқа ауруларға тап болады. Системетикалық сәулелену болған жағдайда психикалық ауру, қан қысымының өзгеруі, жүрек соғысының баяулауы және шашының түсуі байқалады.

Электромагинттік өрістен қорғану әдістері:

1) сәуле шығару көзіндегі сәулеленуді азайту;

2) өте жоғары жиілікті және ультра жиілікті қондырғыларды дұрыс орнату;

3) экрандалған бөлмелердегі қондырғыны алыстан бақылау;

4) жұмыс істеу орнын және сәуленің шығу көзін экрандау немесе мыстан жасалатын жоғары өткізгіштік қасиеті бар тор металдар шағылдырғыш жерлету;

5) экран ретінде пайдалану шаралар «электромагниттік сәулеленуді дозиметр көмегімен кемінде айына бір рет тексеру;

6) жылына медициналық тексеруден бір рет өткізу.

Ағзаға әсер ететін факторлардың тобына:

- табиғи иондаушы емес электромагниттік сәулеленулер мен өрістер;
- статикалық электрлік өрістер;
- тұрақты магниттік өрістер;
- электромагниттік сәулелену мен өнеркәсіптік жиіліктегі және радиожиілікті диапазонындағы өрістер;
- лазерлік сәулелену жатады.

Өндіріс жағдайында адамға аталған өрістер мен сәулеленулердің соңғы төрт түрі әсер етеді [13].

Өнеркәсіптік жиіліктегі электрмагниттік өрістердің әсеріне өндіріс жағдайында ұшыраған жұмысшылардың денсаулық жағдайында өзгерістер байқалады. Олар негізінен ағзаның неврологиялық статусындағы өзгерістерді (бас ауруы, жоғары ашушаңдық , тез қажығыштық, салғырлық, ұйқышылдық),

сонымен қатар жүрек-тамыр қызметінің бұзылыстарын (тахикардия және брадикардия, артериалық гипертензия немесе гипотония, тамыр тұрақсыздығы, гипергидроз) және асқазан-ішек жолдарындағы өзгерістерді білдіретін шағымдар түрінде болады. Шеткі қан құрамында өзгерістер-орташа дәрежеде тромбоцитопения, нейтрофильді лейкоцитоз, моноцитоз, ретикулопенияға бетбұрыс болуы мүмкін.

Өнеркәсіптік жиіліктегі электрлік өрістердің ШРЕД-і толық жұмыс күні үшін 5 кВ/м деңгейінде орнатылады, ал 10 минуттан аспайтын әсеріне арналған максималды ШРЕД-і 25 кВ/м құрайды, қарқындылығы 5-20 кВ/м аралығындағы рұқсат етілген болу уақыты келесі өрнек бойынша анықталады:

$$T = E /50 - 2 \qquad (4.1)$$

мұндағы Т – электрлік өрістің әсерінде болатын рұқсат етілген уақыты, сағатпен[12].

Е – кВ/м берілген бақыланатын зонадағы электрлік өрістің әсер ететін кернеулілігі.

Магниттік өрістердің шектік рұқсат етілген деңгейлері жалпы (барлық денеге) және жергілікті (аяқ-қолға) әсер ету жағдайлары үшін жұмысшының болу уақытына байланысты өрістің кернеулілігі (Н) немесе магнитті индукция (В) бойынша орнатылады.

4.3 Операторлық бөлменің желдету жүйесін есептеу

Желдету – әртүрлі жүйелер мен құрылғылар көмегімен жүзеге асырылатын үй-жай жағдайындағы ауа алмасу.

Адам бөлмеде тұрғанда, ауа сапасы нашарлайды. Экзальді көміртегі диоксидімен қатар басқа метаболизм өнімдері, шаң, зиянды өндірістік заттар ауада жиналады. Сонымен қатар, температура мен ылғалдылық артады. Сондықтан ауа алмасуды қамтамасыз ететін бөлмені желдету, ластанған ауаны кетіру және оны таза ауамен ауыстыру қажеттілігі туындайды.

Ауа алмасу терезе мен транскастер арқылы табиғи жолмен жүзеге асырылуы мүмкін.

Ауа алмасудың ең жақсы тәсілі жасанды желдету болып табылады, онда ауаны тазарту және ластанған ауаны жою механикалық түрде желдеткіштер мен басқа құрылғылардың көмегімен жүзеге асырылады.

Жасанды желдетудің ең озық нысаны - ауаны баптау. Технологиялық процестерді, жабдықтарды және құралдарды қамтамасыз ету, мәдени және көркемдік құндылықтарды сақтау үшін ең қолайлы (ыңғайлы) техникалық құралдарды пайдалану арқылы ғимарат пен көлік құрастыру ауасын баптайды.

Кондиционер ауа ортасының оңтайлы параметрлерін, оның температурасын, салыстырмалы ылғалдылығын, газ құрамын, қозғалыс жылдамдығын және ауа қысымын құру арқылы қол жеткізіледі.

Кондициялау қондырғылары шаңнан ауаны тазарту, жылыту, салқындату, ылғалдандыру және ылғалдандыруға арналған құрылғылармен,

сондай-ақ автоматты басқару, бақылау және басқару үшін жабдықталған. Кейбір жағдайларда ауаны көмірқышқыл газын, оттекті байытуды және ауаны бактериологиялық тазартуды жоюды (ауаны хош иісті заттармен қанықтыру), дезодорацияны (жағымсыз иістерді бейтараптандыру), ион құрамын реттеуді (иондалуды), әуедегі инфекциямен ауыратындар) ауаны кондициялау жүйелері арқылы жүйеге асады.

Әдетте, барлық құрылымдарда және жергілікті бөлмелерде орталық бөлмеде қызмет көрсететін орталықтандырылған кондиционер бар.

Кондиционерлеу әртүрлі типтегі кондиционерлермен жүзеге асырылады, олардың дизайны мен құрылысы олардың мақсатына байланысты. Ауа баптау үшін әртүрлі жабдықтар пайдаланылады: желдеткіштер, ылғалдандырғыштар, ауа ионизаторлары. Үй ішіндегі оңтайлы температура қысқы ауа температурасы + 19-дан +21 С дейін, жазда - +22-ден +25-ке дейін салыстырмалы ылғалдылықта 60-дан 40% -ға дейін, ал әуе жылдамдығы 30 см/с-тан аспайды.

Ауа алмасуын есептеу келесі жағдайларда жүргізіледі: артық ыстықты кетіруді есептеу, ластанудан тазалау және басқалар. Бірақ олар тек кәсіби деңгейде жинақталады және міндетті емес, тұрмыстық желдету үшін барлығы қарапайым:

- едендік кеңістік;
- көпше;
- санитарлық-гигиеналық нормалар.

Желдету - бұл үй-жайдан зиянды газдар мен шаңмен ластанған ауаны кетіруді қамтамасыз ететін ұйымдастырылған және реттелетін ауа алмасу, сондай-ақ өндірістік үй-жайларда микроклиматтық жағдайларды жақсарту.

Желдетуді келесідей жіктеуге болады:

1) ауа алмасуды ұйымдастыру әдісіне сәйкес - жалпы алмасу, ауаның ауысуы үй-жайдың толық көлемінде жүзеге асырылған кезде; жергілікті алмасу, онда бөлмедегі белгілі бір жерде әуе беріледі немесе жойылады.

2) қозғалыс күштерінің табиғаты бойынша - табиғи, табиғи күштердің арқасында ауа қозғалысы болғанда; жасанды (механикалық), ауа желдеткіштің көмегімен қозғалғанда.

3) әрекет принципі бойынша – сырттан ауа үрлеу (ауаны беру) немесе ішкі ауаны шығару (ауаны кетіру).

Табиғи желдету ол сыртқы ауаның салмағы және бөлмедегі ауа салмағының айырмашылығы есебінен (гравитациялық қысым), сондай-ақ жел күші (желдің қысымы) әсерінен туындаған ауа алмасу.

Газ көлемі 1° С температура көбейгенде 1/273 есе артады. Демек, ауа температурасы оның массасының азаюына әкеледі. Жылы және суық ауаның көлемдік массасындағы айырмашылық қысымның өзгеруін тудырады. Салқын ауа құрылыстық материалдардың тесіктері арқылы және бөлме ішіндегі кездейсоқ саңылауларға (инфильтрация) еніп, үстіңгі жақта орналасқан (жылу қысымына) қарағанда жеңіл, жылы ауа алмастырады. Әрине, термиялық

қысым артқан сайын бөлмедегі және одан тыс жерлердегі температураның айырмашылығы артады, және же кіріс және шығыс тесіктері арасындағы биіктігі де артады. Жел өз жолындағы кедергілерге қысым жасайды (жел қысымы). Желдің қысымы желдің жылдамдығымен көтеріледі. Ғимараттың қабырғаларында тесіктер мен кездейсоқ саңылаулар арқылы, жел жағындағы терезе тесіктері арқылы жел қысымымен бөлме ішіне ауа кіреді, ал жел ығында тұрған қысымы төмен жақтан ауа шығады.

Табиғи желдету кезінде жылу мен жел қысымдары бір мезгілде әсер етеді. Өндірістік ғимараттардың табиғи желдетудің ең тиімді және тиімді ұйымдастырылған желдету түрі - аэрация, желдету ғимарат қабырғаларында және төбесінде арнайы саңылаулар арқылы жүзеге асырылады; сыртқы температура, бағыт, жел жылдамдығы және т.б. факторларды ескере отырып, осы саңылауларды қолдануға болады.

Аэрация заманауи өндірістік кәсіпорындардың ірі өндірістік үй-жайларында қарқынды ауа алмасуды (20-40 есе) қамтамасыз етеді. Аэрацияны реттеу – оны дұрыс пайдаланудың маңызды шарттарының бірі. Бұл желдің күші мен бағытына, ауа температурасына және т.б. байланысты.

Жазда сыртқы ауа ғимараттың төменгі тесіктеріне шығуы керек. Желдің көлденең жағында орналасқан жел өткелі жабық болуы керек.

Қыста суық ауаны жұмыс аймағына кіргізбеуі үшін, ауа еденнен 4,5 метрден төмен емес орналасқан саңылаулар арқылы ағып кетуі керек.

Табиғи күштерге байланысты зиянды заттардың пайда болу орнынан ауаны кетіретін қолшатырлар, арнайы шахталарды ұйымдастыру арқылы жоюға болады.

Аэрация, әдетте, шаң мен зиянды заттардың концентрациясы тиімділіктің 30% -нан аспайтын шеберханаларда қолданылады.

Жел қысымын пайдалану үшін, пайдаланылған шахталар дефлекторометрлермен жабдықталады, бұл бөлмедегі ауаны соруға үлес қосады, себебі желдің беткі жағындағы дефлекторға вакуум пайда болады.

Механикалық желдету, әдетте, табиғи желдеткіштің гигиеналық талаптарға сай көрсеткіштерге жете алмаған кезде қолданылады.

Механикалық желдету жүзеге асыру жағынан күрделі болып табылады, табиғи желдетуге қарағанда бірқатар маңызды артықшылықтарға ие:

а) ауа температурасын, салыстырмалы ылғалдылықты қамтамасыз ету мүмкіндігі;

ә) климаттық жағдайларға тәуелсіз, талап етілетін көлемде жыл бойына біркелкі пайдалану мүмкіндігі;

б) бөлменің кез келген нүктесінде ауаны жеткізу және ауа ағымынан бөлеу мүмкіндігі;

в) құрылғының жергілікті сору қабілеті;

г) бөлмеден алынатын желдетілетін ауаны тазарту мүмкіндігі.

Арнайы бағыттау желдетуі кезінде желдету аумағы берілген аумақтан көлемдірек болуы мүмкін.

Төмендегі құрылғылар таза ауаны желдетудің элементтері болып табылады: қабылдау құрылғысы, жылу, ауаны ылғалдандыру, ауа қозғалысының күшейткіші, шеберханаға ауа беру үшін ауа өткізгіш жүйе. Сыртқы ауа қабылдайтын орын ғимараттың сыртқы қабырғасындағы тесік, ауа сорғыш білігі және т.б.

Формулаларға ауыстырудың барлық қажетті желдету стандарттары арнайы СНиП, ГОСТ және басқа нормативтік құжаттарда келтірілген.

Бөлменің аумағына негізделген желдету жүйесін есептеу

Бір сағат ішінде қанша рет бөлменің көлемі толығымен таза ауамен толтырылғанын және пайдаланылғандардан тазартылғандығын сипаттайтын мән, көпше деп аталады. Бөлмедегі ауаның айырбас бағамы, анықтамасынан анық болғандай, осы бөлме көлеміне байланысты. Яғни, егер бізде бір сағат ішінде үйдің бір бөлігінің таза ауасы болса, онда бұл жағдайда бірнеше есе көп, бұл іс жүзінде іс жүзінде үй жағдайында жүз пайызға тең.

Көптеген бөлмелерде желдетуді есептеу

Бұл есептеу үшін тек екі цифрды ескеру керек: нормалар 1 $м^2$ бөлме үшін 3 $м^3$ / сағ таза ауаны жеткізуді орнатады. Сонымен қатар, бөлмедегі адамдардың саны мүлдем маңызды емес. Бөлменің ұзындығын, биіктігі мен енін біле отырып, желдетудің өнімділігін есептейміз.

Көптеген бөлмелерде желдетуді есептеу

Әр бөлме көлемін санау - біз осы бөлмелердің биіктігін, ұзындығын және енін көбейтеміз немесе үйді немесе пәтерді қабырғасы жоқ бөлме ретінде қараймыз - бұл жағдайда біз үйдің немесе пәтердің жалпы көлемін ғана қарастырамыз;

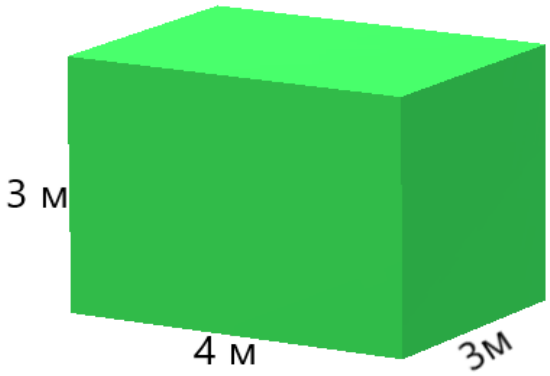
Формулаға сәйкес әрбір бөлме үшін қажетті ауа көлемін есептеу:

$$L = n \cdot V \qquad (4.2)$$

(мұнда L - талап етілетін ауа көлемі, n - ауа алмасу жылдамдығы (SNiP анықталады), V - бөлменің көлемі) [12].

Жеткізу және шығатын ауаның көлемі есептеу кезінде бірдей болуы керек екенін есте ұстаған жөн. Егер бірінші шамасы екіншіден асып кетсе, онда ол ең аз мөлшерде қабылданған бөлмелері үшін шығатын ауаның мәндерін ұлғайту қажет.

Санитарлық-гигиеналық нормаларды есептеу, бұл есепте қайтадан екі суретті есте сақтау қажет: бір адамға 60 $м^3$ / сағ, ауада уақытша тұрып жатқан адамға 20 $м^3$ / сағ. Бұл сандар тұрғын үйлер мен әкімшілік орындардың санитарлық нормаларын белгілейді. Яғни, бір адам тұрақты және біреуі уақытша тұрып жатқан бөлмеде сағатына ауа көлемі 80 $м^3$ құрайды.



Сурет 4.1 – Бөлме сұлбасы

Операторлық бөлме көлемі [12]:

$$V=4*3*3=36 \text{ м}^3 \quad (4.3)$$

Әкімшілік бөлме үшін адам 1 адамға керекті ауа алмасу жылдамдығы 20 $м^3$/сағ.

2.1-формулаға сәйкес:

$$n=20 \text{ м}^3/\text{сағ},$$

$$V=4*3*3=36 \text{ м}^3,$$

$$L=n*V=20*36=720.$$

Ауаның кіру жылдамдығы 20 $м^3$/сағ, шығу жылдамдығы 20 $м^3$/сағ болуы тиіс.

5 Техникалық-экономикалық негіздеме

Бұл дипломдық жобаның мақсаты SIEM жүйесі көздерінен деректерді жинайтын және деректерді бастапқы өңдеуді жүргізетін бағдарламалық қамтамасыз етуді әзірлеу болып табылады.

Пассивті қорғау арқылы ақпаратты қорғауға мүмкіндік беретін ақпаратты қорғаудың көптеген жүйелері бар. Бұл БҚ деректерді тек операциялық жүйелерден ғана емес, сонымен қатар ақпаратты қорғаудың басқа жүйелерімен де өзара қатынас жасайды, бұл деректерді жинауды айтарлықтай жақсартады, осылайша ақпаратты қорғауды нығайтады.

Бағдарламалық қамтамасыз етуді техникалық жетекші, бағдарламашы-әзірлеуші кіретін мамандар тобы әзірлейді. Техникалық басшы бағдарламалық қамтамасыз етуді әзірлеу барысын қадағалауы, жобаны оңтайландыруға бағыт беруі тиіс. Бағдарламашы-әзірлеуші міндетіне бағдарламалық қамтамасыз етуді әзірлеу, тестілеу, сүйемелдеу және техникалық сипаттама әзірлеу кіреді.

Техникалық-экономикалық негіздеме мынадай тармақтардан тұрады:

- БҚ әзірлеу күрделілігін анықтау;
- БҚ әзірлеуге арналған шығындарды есептеу;
- негізгі қорлардың амортизациясын және өзге де шығындарды есептеу;
- ықтимал (шарттық) бағаны айқындау;
- БҚ жұмыс нәтижелерін бағалау.

5.1 Әзірлеу күрделілігін анықтау

Бағдарламалық жасақтаманы әзірлеудің күрделілігін дәл анықтау үшін барлық тапсырманы қарапайым кезеңдерге бөлу қажет. Бұл күрделі міндетті неғұрлым қарапайым тапсырыстарға бөлу есебінен бағдарламалық қамтамасызтандыруды әзірлеу прогресін тиімді бақылауға мүмкіндік береді. Менің көзқарасым бойынша мұндай тәсіл неғұрлым тиімді болып саналады және нәтижелі, тез табыс табуға мүмкіндік береді. Моделі бөлу күрделілігі әзірлеу және игеру сатысындағы 5.1-кестеде көрсетілген.

5.1-кесте – Бағдарламалық қамтамассыздандырудың әзірлеу кезеңдері

Әзірлеу кезеңдері	Жұмыс түрі	Еңбек сыйымдылығы, адам сағ..
Кезең 1	Тапсырмалар қою	5
Кезең 2	БҚ әзірлеуге ТТ әзірлеу және бекіту	10
Кезең 3	Мұндай бағдарламаларды іздеу және зерттеу	25
Кезең 4	Ілеспе әдебиеттерді іздеу және зерттеу	20
Кезең 5	БҚ бойынша талдау кестелерін құру	5

5.1-кесте жалғасы:

Кезең 6	Дипломдық жұмыстың теориялық бөлімін рәсімдеу	15
Кезең 7	Дипломдық жобаның тәжірибелік бөлігін әзірлеу	25
Кезең 8	Жобаны іске асыру	50
Кезең 9	Ақауларды жөндеу және жою	20
Кезең 10	Есепті және жұмыс нәтижелерін ұйымдастыру	10
Кезең 11	Тестілеу	10
Кезең 12	БҚ әзірлеу бойынша қорытынды шығару	5
Кезең 13	Енгізу	20
Барлығы: жобаны орындаудың еңбек сыйымдылығы		215

Жұмыс күнінің ұзақтығы 8 сағатқа тең. Нәтижесінде бағдарламалық қамтамасыздандыруды іске асыру үшін 27 жұмыс күні қажет.

5.2 Бағдарламаны әзірлеу бойынша шығындарды есептеу

Бағдарламалық қамтамасыз етуді әзірлеу үшін қажетті шығындарды анықтау қолда бар смета негізінде жүргізіледі, ол мынадай элементтерді қамтиды:

- материалдық шығындар;
- еңбекақы төлеу шығындары;
- әлеуметтік салық;
- негізгі қорлардың амортизациясы;
- өзге де шығындар.

Материалдық шығындар негізгі және қосалқы шығындарға, материалдарға, энергияға және БҚ әзірлеу үшін қажетті басқа да шығындарға бөлінеді. Материалдық шығындарды есептеу 5.2-кестеде берілген нысан бойынша жүргізіледі.

5.2 кесте-Материалдық ресурстарға шығындар

Материал аты	Маркасы	Өлшем бірлігі	Саны	Бір дана үшін бағасы	Сомасы, теңге
Кеңсе қағазы	International Paper	Қорап	3	1 000	3 000
Дәптер (96 бет)	Маяк Канц	Дана	2	190	380
Блокнот	КТС-ПРО	Дана	1	400	400
Қаламдар	Parker Jotter	Дана	2	90	180

5.2-кесте жалғасы:

Компьютерлік тышқан	TECH	Дана	1	2 000	2 000
USB flash 32 Gb	Transcend	Дана	1	2600	2600
Барлығы:					8 560

Бағдарламалық қамтамасыз етуді әзірлеу үшін Acer Aspire S5-371-7270 NX ноутбук қолданылады. GCHER.012, ноутбук қуаты қойылған міндеттерді орындау үшін жеткілікті. Себебі ноутбукта 4 ядро, микропроцессор CoreI7-8200M және құрамында белгіленген операциялық жүйесі Windows 10 x64 және үшін қажетті бағдарламалық қамтамасыз етуді әзірлеу және өндіруге қосымша шығындар қажеттілігі жоқ ОС бар.

Материалдық құралдарға ($З_м$) қажетті жалпы соманы мынадай формула бойынша есептеуге болады:

$$З_м = \sum P_i * Ц_i, \quad (5.1)$$

мұнда P_i - материалдық ресурстың і түрінің шығысы, заттай бірліктер;

$Ц_i$ - материалдық ресурстың і түрінің бірлігінің бағасы, тг;

і - материалдық Ресурстың түрі;

n - материалдық ресурстар түрлерінің саны [13].

Қажетті жабдықтар мен бағдарламалық қамтамасыз ету шығындарын есептеу 5.3-кестеде келтірілген нысан бойынша жүргізіледі.

Кесте 5.3 – Жоба үшін қажетті жабдық пен БҚ шығындарын есептеу

Материалдың атауы	Маркасы	Өлшем бірлігі	Саны	Бір дана үшін бағасы	Сомасы, теңге
Ноутбук	Acer E5-576G NX.GU2ER.011	Дана	1	280 000	280 000
Принтер	HP LaserJet Pro M15a	Дана	1	36 200	36 200
Бағдарламалық қамтамассыздандыру	PyCharm	Дана	1	-	-
Модем	ID Net	Дана	1	4600	4600
ОЖ	Windows 10	Дана	1	-	-
Барлығы:					320 800

$З_м$ = 8 560 + 320 800 = 329 360 (тг)

Бағдарламалық қамтамасыз етуді іске асыру үшін 329 360 теңге сомаға материалдар қажет.

5.3 Электр энергиясына шығындарды есептеу

Электр энергиясын тұтынбай бағдарламалық қамтамасыз етуді әзірлеу мүмкін емес болғандықтан электр энергиясына жұмсалатын шығындарды есептеу қажет.

5.1 кестеге сүйене отырып, бағдарламалық қамтамасыз етуді әзірлеу үшін шамамен 215 сағат қажет, енді 215 сағат ішінде жұмсалатын электр энергиясының құнын есептеу қажет. Принтер үшін есептеу 24 сағат кезеңі үшін жүргізіледі, себебі принтерді үнемі пайдалану қажет емес.

$$Э = Ш_{эл.эн.құрал.} + Ш_{қос.шығ.}, \quad (5.2)$$

мұндағы $Ш_{эл.эн.құрал.}$ - жабдықтың электр энергиясына арналған шығындар [13];

$Ш_{қос.шығ.}$ - қосымша мұқтаждықтарға электр энергиясының шығындары.

Жабдық үшін қажетті электр энергиясын есептеу мынадай формула бойынша анықталады:

$$Ш_{эл.эн.құрал.} = \sum W * К_{исц} * S * T, \quad (5.3)$$

мұндағы W-тұтынылатын қуат, Вт;

$К_{исц}$ - пайдалану коэффициенті ($К_{исц}$ = 0,7..0,9);

Т-жұмыс уақыты;

S-тариф (1кВт / сағ = 23,85 тг) [13].

Электр энергиясының құнын есептеу бойынша қорытынды 5.4-кестеде көрсетілген.

5.4 кесте - Электр энергиясына шығындар

Құрал атауы	Төлқұжат қуаты, кВт	Қуаттылық коэффициенті	Құрал жұмыс істеу уақыты, сағ	Баға ЭЭ тг/кВтч	Сома, тг.
Ноутбук	0,6	0,7	215	23,85	2 153,65
Модем	0,08	0,9	215	23,85	369,20
Принтер	0,5	0,9	24	23,85	257,58
Кондиционер	0,8	0,9	180	23,85	3 090,96
Жарықтандыру	0,3	0,7	215	23,85	1 076,83
Барлығы:					6 948,22

$$Ш_{эл.эн.құрал.} = 6\,948{,}22 \text{ (теңге)}$$

Қосымша қажеттіліктерге шығыстар электр энергиясына арналған шығыстардың 5% көлемінде жоғары көрсеткіш негізінде есептеледі:

$$Ш_{қос.шығ.} = 5\% * Ш_{эл.эн.құрал.}, \quad (5.4)$$

Формулаға (5.4) сәйкес қосымша қажеттіліктерге жұмсалатын шығындарды анықтаймыз:

$$Ш_{қос.шығ.} = 0.05 * 6948,22 = 347,41 \text{ (теңге)}$$

Барлық есептеулерге сүйене отырып, электр энергиясына толық шығындар құрайды:

$$Э = 347,41 + 6948,22 = 7295,63 \text{ (теңге)}$$

5.4 Еңбекақы төлеу шығындарын есептеу

Бағдарламалық қамтамасыз етуді әзірлеу үшін бұрын көрсетілгендей, екі қызметкер қажет:

- жоба жетекшісі – жұмыс уақытын басқару, жұмыс процестерін түзету, үйлестіру, пәндік облысты зерттеу;
- әзірлеуші – БҚ әзірлеу, тестілеу және сүйемелдеу.

Еңбекақы төлеу шығындарының сомасын келесі формула бойынша есептеуге болады:

$$З_{тр} = \sum СМ_i * T_i \quad (5.5)$$

мұндағы $СМ_i$ - і қызметкердің сағаттық мөлшерлемесі, тг;

T_i - модельді әзірлеудің еңбек сыйымдылығы, адам*сағ; і-қызметкердің санаты;

n – бағдарламалық продукт әзірлеумен айналысатын қызметкерлердің саны [14].

Жұмыс уақыты әр түрлі, сондықтан әрбір қызметкердің сағаттық ставкасын және жалпы жалақы көлемін белгілеу қажет.

Қызметкердің сағаттық мөлщерін келесі формула бойынша есептеуге болады:

$$СМ_i = \frac{Ж_i}{ЖУҚ_i} \quad (5.6)$$

мұндағы $Ж_i$ - і-ші қызметкердің айлық жалақысы, тг;

$ЖУҚ_i$ - і жұмыс уақытының айлық қоры, сағат.

Жетекшінің айлық жалақысы 200 000 теңгеге тең және әзірлеушінің айлық жалақысы 135 000 теңгеге тең. Әр қызметкердің сағаттық мөлшерін (5.6) формулаға сәйкес есептейміз:

$$СМ_{жетекші} = \frac{200\,000}{22 * 8} = 1\,136{,}37\ тг/сағ$$

$$СМ_{әзірлеуші} = \frac{135\,000}{22 * 8} = 767\ тг/сағ$$

Жетекшінің сағаттық мөлшері 1 136,37 (тг/сағ) құрайды, еңбек сыйымдылығы 100 сағатқа тең. Әзірлеушінің сағаттық мөлшерлемесі 757 (тг/сағ), әзірлеудің еңбек сыйымдылығы 215 сағатқа тең. (5.5) формулаға сәйкес қызметкерлердің еңбекақысына арналған шығын сомасын есептейтін болсақ:

$$З_{тр} = 1136{,}37 * 100 + 767 * 215 = 113\,637 + 164\,905 = 278\,542$$

Еңбек ақы төлеу бойынша шығындарды есептеу (5.5) кестеде көрсетілген.

5.5-кесте. – Жалақыны есептеу

Қызметкердің санаты	Квалификация	Еңбек сыйымдылығы БП, сағ.	Сағатты қ мөлшер, тг/сағ	Сома, тг.
Жетекші	Проект жетекшісі	100	1 136,37	113 637
Әзірлеуші	Бағдарламашы	215	767	164 905
Итого:				278 542

5.5 Әлеуметтік салық бойынша шығындарды есептеу

Қазақстан Республикасының Салық Кодексіне сәйкес әлеуметтік салық еңбекақы төлеу қорының 9,5% - ын құрайды. Әлеуметтік салықты келесі формула бойынша есептеуге болады:

$$Ә_с = (ЕТҚ - ЗА) * 0{,}095 \qquad (5.7)$$

мұндағы ЗА – зейнетақы қорына аударымдар ЕТҚ-ның 10% құрайды;
ЕТҚ – еңбекақы төлеу қоры.

$$ЗА = 278\,542 * 0{,}1 = 27\,854{,}2\ теңге$$

$$Ә_с = (278\,542 - 27\,854{,}2) * 0{,}095 = 23\,815{,}3\ теңге$$

Есептеу нәтижелері кестеде берілген (5.6):

Кесте 5.6 - Әлеуметтік салықты есептеу

Қызметкер санаты	Адам саны	Айлық мөлшері, тг	Зейнетақы аударымы, тг	Әлеуметтік салық, тг
Жетекші	1	113 637	11 364	9 716
Әзірлеуші	1	164 905	16 490	14 099,3
Барлығы:				23 815,3

5.6 Негізгі қорлардың амортизациясы және өзге де шығындар

Амортизация нормаларын НҚ салық кодексіне сәйкес анықтау қажет. НҚ амортизациясын келесі формула бойынша анықтауға болады:

$$A_{\text{г}} = \frac{\text{Ж}_{\text{құны}} * \text{Н}_{\text{а}}}{100} \quad (5.8)$$

мұндағы, С_об – жабдықтың құны;

$\text{Н}_{\text{а}}$ – амортизация нормасы (амортизация нормасы = 25);

Формула (5.8) ноутбук үшін бір жыл ішінде амортизациялық аударымдар үшін қажетті соманы есептеуге мүмкіндік береді:

$$A_{\text{г}} = \frac{280\,000 * 25}{100} = 70\,000 \text{ теңге}$$

Енді әзірлеу кезеңі үшін амортизация нормасын есептеу қажет:

$$A_{\text{г}} = \frac{70\,000 * 27}{365} = 5\,178{,}08 \text{ теңге}$$

Осылайша, барлық жабдық үшін амортизация нормасын есептеу қажет. Есептеу нәтижелері кестеде келтірілген (5.7).

5.7 кесте – НҚ амортизациясы

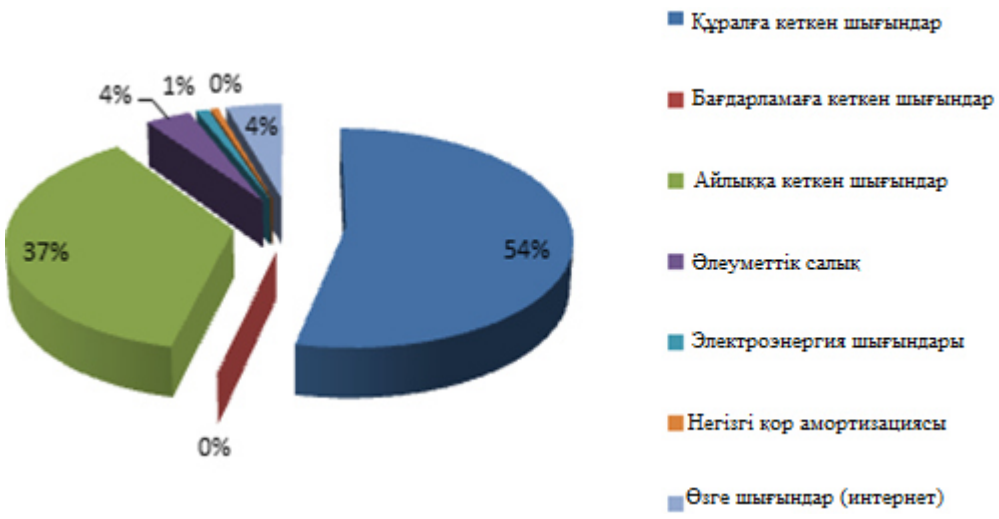
Жабдық атауы және БҚ	Жабдықтармен БҚ құны, тг	Жылдық амортизациясы, %	Жылдық амортизациясы сомасы, тг	Әзірлеу кезіндегі амортизация сомасы, тг
Ноутбук	280 000	25	70 000	5 178,08
Принтер	36 200	25	9 050	669,45
Модем	4600	20	920	68,05
Барлығы:			79 970	5916

БҚ әзірлеуге арналған шығыстар сметасы.

Барлық берілген есеп-қисаптардың негізінде (5.8) кестеде келтірілген нысан бойынша әзірлеуге арналған шығыстар сметасын ресімдеу қажет. Суретте (12) жұмыс шығыстарының диаграммасы көрсетілген.

5.8 кесте – БҚ әзірлеуге арналған шығындар сметасы

Шығындар	Сома, тг
Құралға кеткен шығындар	320 800,00
Айлыққа кеткен шығындар	278 542,00
Әлеуметтік салық	23 815,30
Электроэнергия шығындары	7295,63
Негізгі қор амортизациясы	5916
Смета бойынша жиыны:	630 452,93



5.1 сурет – Шығындар диаграммасы

5.7 Ықтимал (шарттық) бағаны айқындау

Бағдарламалық қамтамасыз етудің құны әзірленген өнімнің сапасы, оны әзірлеу мерзімі және өнімнің өнімділігі негізінде анықталады. Бағдарламалық қамтамасыз ету үшін $Б_{ш}$ құнын мына формула бойынша есептеуге болады:

$$Б_{ш} = Ш_{толық}\left(1 + \frac{P}{100}\right) \quad (5.9)$$

мұндағы $Ш_{толық}$ - бағдарламалық қамтамасыз етуді әзірлеуге арналған шығындар, nu;

Р – БҚ рентабельділігінің орташа деңгейі, (%). Бұл параметр 25% тең [14].

$$Б_{пайда} = 630\,452{,}93 * \frac{25}{100} = 157\,613{,}23 \text{ теңге}$$

$$Б_{ш} = 630\,452{,}93 + 157\,613{,}23 = 788\,066{,}16 \text{ теңге}$$

Бұдан әрі ҚҚС есебімен сату құнын анықтау қажет, ҚҚС мөлшері ҚР заңнамасымен белгіленеді. 2019 жылға ҚҚС мөлшері 12% құрады. Іске асыру құны ҚҚС-ты ескере отырып есептеуге болады мынадай формула бойынша:

$$Б_р = Б_ш + Б_ш * ҚҚС \quad (5.10)$$

$$Б_р = 788\,066{,}16 + 788\,066{,}16 * 0{,}12 = 882\,634{,}10 \text{ теңге}$$

Бұл бағаны 882 650 теңгеге дейін жуықтауға болады. Яғни, бағдарламалық өнімді әзірлеуге кететін шығындар (өзіндік құн) 630 452,93 теңгені құрады, ал пайда (рентабельділік) 157 613,23 теңгеге тең. Осыған байланысты шарттық баға 788 066,16 теңгеге тең. ҚҚС-ты есепке ала отырып сату құны 882,634,10 теңгені құрады. Бұл сома 882 650 теңгеге дейін жуықтатылды. Таңдалған баға экономикалық тиімділік тұрғысынан тиімді.

Қорытынды

Бұл дипломдық жұмыста SIEM (Security information and event management) жүйесінің ақпаратты жинау және алғашқы өңдеу жұмысы туралы мәліметтер жинақталды.

SIEM-жүйесіне қойылатын талаптарды іске асыруға мүмкіндік беретін қауіпсіздік оқиғалары туралы ақпаратты ұсыну, жинау, сақтау және өңдеу саласындағы әдістер мен модельдерді әзірлеу маңызды ғылыми міндет болып табылады, үлкен мемлекеттік және халық шаруашылық маңызы бар және ақпараттық қауіпсіздік саласындағы ғылыми зерттеулердің жаңа бағыттарын айқындайтын өзекті ғылыми міндет болып табылады. Бұл жүйе бүгінде өте өзекті мәселелердің бірі және Қазақстанда әлі де толық шешімі табылмаған мәселе болып табылады.

Жұмыс барысында ақпаратты өңдеудегі қалыпқа келтіру функциясына бағдарламалық шешім ұсынылды. Бағдарламалау тілі негізі ретінде «python 3.6» тілі қолданылды. Бағдарламалық бөлімде лог-файлдерді өңдеуге дейін 4 топқа жинақтау, бөлінген топқа байланысты бір форматқа келтіру және оларды келесі өңдеуге процесіне деректор қоры ретінде тапсыру қарастырылған. Бағдарламаның жұмыс істеу уақытын азайту үшін серверсіз деректор қоры SQLite пайдаланылды.

Өмір тіршілік қауіпсіздігі бөлімінде электрмагниттік өрісінің қауіпі және зиянды факторлары қарастырылып, электрмагниттік өрісінің адамға әсері және олардан қорғану шаралар айқындалды, операторлық бөлменің желдету жүйесіне есептеулер жүргізілді.

Экономикалық бөлімінде капиталды шығындарға, базалық және жобаланған нұсқа бойынша қолдану шығындарына есеп жүргізілген, сонымен қатар жобаның экономикалық тиімділігімен ағымдағы таза құны есептелген.

Қысқартулар тізімі

DLP (Data Loss Prevention) - ақпаратты ішкі қауіп-қатерден қорғау технологиясы.

ESM (Enterprise Security Manager) – кәсіпорын қауіпсіздігін басқару.

IDS (Intrusion Detection System) – басып кіруді анықтау жүйесі.

IP (Internet Protocol) – интернет протоколы.

IPS (ntrusion Prevention System) – басып кіруді болдырмау жүйесі.

PID (ағылшынша process identifier) – процесс идентификаторы.

SIEM (Security information and event management) – оқиғаларды жинау және корреляциялау жүйесі.

SOC (Security Operation Center) - қауіпсіздікті басқару орталығы.

URL (Uniform Resource Locator) – ресурстың біріздендірілген көрсеткіші.

АЖК – аса жоғары кернеулі.

АЖО – автоматтандырылған жұмыс орны.

АҚ – ақпараттық қауіпсіздік.

АТ – ақпараттық технология.

БҚ – бағдарламалық қамтамассыздандыру.

ДҚ – деректер қоры.

ЗА – зейнетақы қорына аударымдар.

ҚҚС – қосылған құн салығы.

ҚТ – қаіпсіздік технологиясы.

НҚ – негізгі қор.

ОЖ – операциялық жүйе.

ӨЖ ЭМӨ – өнеркәсіптік жиіліктегі электрмагниттік өріс.

ЭАТ – энергия ағынының тығыздығы.

ЭЭ – энергетикалық экспозиция.

Әдебиеттер тізімі

1. Котенко И.В., Федорченко А.В., Саенко И.Б., Кушнеревич А.Г. Технологии больших данных для корреляции событий безопасности на основе учета типов связей // –М: изд. Кибер, 2017. № 5 (24). С. 2-16.

2. D.R. Miller, S. Harris, A.A. Harper, S. VanDyke, C. Blask. Security Information and Event Management (SIEM) Implementation. - N.Y.: McGraw-Hill 2016, 430 p.

3. Федорченко А.В., Левшун Д.С., Чечулин А.А., Котенко И.В. Анализ методов корреляции событий безопасности в SIEM-системах. Часть 2 // Труды СПИИРАН. –СПб.: изд. Петр, 2016. Вып. 49. С. 208-225.

4. VM Cotenescu. SIEM (Security Information and Event Management Solutions) Implementations in Private or Public Clouds. J. Lee, Y.S. Kim, J.H. Kim, I.K. Kim. Toward the SIEM architecture for cloud-based security services //–Berlin: Naval Academy Scientific Bulletin. 2016. Volume XIX. Issue 2.

5. Марков А.С., Цирлов В.Л. Структурное содержание требований информационной безопасности // Мониторинг правоприменения. Ташкент: ТТУ, 2017. № 1 (22). С. 53-61.

6. J. Lee, Y.S. Kim, J.H. Kim, I.K. Kim. Toward the SIEM architecture for cloud-based security services // Communications and Network Security IEEE Conference, 2017.

7. K. Kent, M. Souppaya. Guide to Computer Security Log Management // NIST Special Publication 800-92, N.Y.: McGraw-Hill, 2006. 72 p.

8. Ершов А.Л., Карасёв С.В., Поляков С.А., Рыболовлев Д.А. Подход к формированию модели данных события информационной безопасности // Информационные системы и технологии. -Воронеж: изд. Сара, 2017. № 6 (104). С. 124-129.

9. Карасёв С.В., Рыболовлев Д.А. Применение методов выявления зависимостей между событиями при построении систем управления инцидентами безопасности // Информатика: проблемы, методология, технологии. –Воронеж: изд. Свет, 2016. Секция №3. С. 154-156.

10. Сулеев Д.К., Исаханова А.Б., Суйесинова Г.И., Болатбаева Т., Утепова А.Б. Электромагнитные поля в учебных аудиториях. –Алматы: Вестник КазНТУ, 2007. -№ 1/1 (58).-С.22-27.

11. Суйесинова Г.И., Болатбаева Г,А., Тусупова А.А.,Уразбахова А., Мединский А.И. Исследование характеристик электромагнитных полей компьютеров //- Алматы: Вестник КазНТУ, 2009.-№3(73).

12. Утепов Е.Б., Исаханова А.Б., Суйесинова Г.И., Мединский А.И., Батыркулов Н.Т. Снижение уровней электромагнитного поля на производстве. Монография.–Алматы: КазНТУ, 2010.-144 с.

13. Суйесинова Г.И. Электрмагниттік сәулелерге ұшырайтын жұмысшылардың еңбек жағдайын жақсарту. // «Тіршілік қауіпсіздігі саласындағы жаналықтар» атты он бірінші ғылыми-техникалық конференция. 3 т. –Алматы: КазНТУ, 2009.-С.109-111.

14. Суйесинова Г.И. Электромагниттік сәулелердің жұмысшы ағзасына әсерін бәсеңдету бойынша іс-шараларды жасау. // «Тіршілік қауіпсіздігі саласындағы жаналықтар» атты XI Халықаралық ғылыми-техникалық конференция. 3 т. –Алматы: КазНТУ, 2009.-С.111-112.

А қосымшасы

```
import datetime
import logging
import re
import datefinder
import adodbapi
import sqlite3
import dateutil.parser
# add filemode="w" to overwrite
logging.basicConfig(filename="ddd.log", level=logging.INFO)
# log = logging.getLogger("ex")
#with open('sample.log','wr') as f:
f = open('ddd.log','a+')
print(f.read())

database = "db1.mdb"
conn = sqlite3.connect("mydatabase.db")
tablename = "dannye"
s = open('dism.log')
cur=conn.cursor()
# Создание таблицы
try:
   cur.execute("""CREATE TABLE first
                (date1 DATE, time1 TIME, PID text, subject text, object  text, source text,
                resource text, app text, protocol text, act text, sub_name text,
                 ob_name text, type text, subtype text, user text, group1 text, srcport text, dstport text)
             """)
except:
   conn.commit()
conn.commit()
for line in s:
   indicator=0
   #dateutil.parser.parse(line, fuzzy=True)
# установка времени
   matches = list(datefinder.find_dates(line))
   if len(matches) > 0:
      # date returned will be a datetime.datetime object. here we are only using the first match.
      date = matches[0]
      date1=re.split(r' ', str(date))
      date=date1[0]
      time=date1[1]
#       print (date)
      f.write("date="+str(date1[0])+", ")
      f.write("time="+str(date1[1])+", ")
   else:
      print('No dates found')

   PID = 0
   PID = re.findall(r'\bPID.(\d+)', line)
   if PID != 0:
```

```
            f.write("PID NUMBER="+str(PID)+" ")
        subjec1 = re.findall(r'SOURCE.(\d+[.]\d+[.]\d+[.]\d+)', line)
        if subjec1:
            subjec=subjec1
            f.write(" subject=" + str(subjec))
            indicator += 1
        subjec1 = re.findall(r'src.(\d+[.]\d+[.]\d+[.]\d+)', line)
        if subjec1:
            subjec = subjec1
            f.write(" subject=" + str(subjec))
            indicator += 1
        subjec1 = re.findall(r'from.(\d+[.]\d+[.]\d+[.]\d+)', line)
        if subjec1:
            subjec=subjec1
            f.write(" subject=" + str(subjec))
            indicator += 1
        subjec1 = re.findall(r'db_username.(\w+)', line)
        if subjec1:
            subjec=subjec1
            f.write(" subject=" + str(subjec))
            indicator += 1
    #парсинг объекта
        objec=''
        objec1 = re.findall(r'dst.(\d+[.]\d+[.]\d+[.]\d+)', line)
        if objec1:
            objec=objec1
            f.write(" object=" + str(objec))
            indicator += 1
        objec1 = re.findall(r'to (\d+[.]\d+[.]\d+[.]\d+)', line)
        if objec1:
            objec=objec1
            f.write(" object=" + str(objec))
            indicator += 1
        objec1 = re.findall(r'grantee.(\w+)', line)
        if objec1:
            objec=objec1
            f.write(" object=" + str(objec))
            indicator += 1

    #парсинг источника
        source = ''
        source1 = re.findall(r'dvc.(\d+[.]\d+[.]\d+[.]\d+)', line)
        if source1:
            source=source1
            f.write(" source=" + str(source))
            indicator += 1
        source1 = re.findall(r'device.(\w+)', line)
        if source1:
            source=source1
            f.write(" source=" + str(source))
            indicator += 1
```

```
#парсинг ресурса
    resource = ''
    resource1 = re.findall(r'obj_name.(\w+)', line)
    if resource1:
        resource=resource1
        f.write(" resource=" + str(resource))
        print(resource)
    if indicator == 0:
        subjec = re.findall(r'\d+[.]\d+[.]\d+[.]\d+', line)
        if subjec:
            f.write(" subject=" + str(subjec))
    app = ''
    app = re.findall(r'app.(\w+)', line)
    if app:
        f.write("app="+str(app))
    protocol = ''
    protocol = re.findall(r'Framed-Protocol.(\w+)', line)
    if protocol:
        f.write("protocol=" + str(protocol))
    protocol = re.findall(r'protocol.(\w+)', line)
    if protocol:
        f.write("protocol=" + str(protocol))
    act = ''
    act1 = re.findall(r'Action.(\w+)', line)
    if act1:
        act = act1
        f.write("act=" + str(act))
    act1 = re.findall(r'Actual action.(\w+)', line)
    if act1:
        act = act1
        f.write("act=" + str(act))
    subip=''
    subip=re.findall(r'subject_ip.(\w*)', line)
    if subip:
        f.write("subip="+str(subip))
    obip = ''
    obip = re.findall(r'object_ip.(\w+)', line)
    if obip:
        f.write("obip=" + str(obip))
    type = ''
    type1 = re.findall(r'status.(\w+)', line)
    if type1:
        type = type1
        f.write("type=" + str(type))
    type1 = re.findall(r'type.(\w+)', line)
    if type1:
        type = type1
        f.write("type=" + str(type))
    subtype = ''
    subtype1 = re.findall(r'subtype.(\w+)', line)
    if subtype1:
```

```
        subtype = subtype1
        f.write("subtype=" + str(subtype))
    user = ''
    user = re.findall(r'user.(\w+)', line)
    if user:
        f.write("user=" + str(user))
    group = ''
    group = re.findall(r'group.(\w+)', line)
    if group:
        f.write("group=" + str(user))
    srcport = ''
    srcport1 = re.findall(r'srcport.(\d+)', line)
    if srcport1:
        srcport=srcport1
        f.write("srcport=" + str(srcport))
    srcport1 = re.findall(r'NAS-port.(\d+)', line)
    if srcport1:
        srcport=srcport1
        f.write("srcport=" + str(srcport))
    dstport = ''
    dstport = re.findall(r'dstport.(\d+)', line)
    if dstport:
        f.write("dstport=" + str(dstport))
    f.write("\n")
    firsts = [(str(date), str(time), str(PID), str(subjec), str(objec), str(source), str(resource), str(app),
            str(protocol), str(act), str(subip), str(obip), str(type), str(subtype), str(user),
            str(group), str(srcport), str(dstport))]

#    cur.executemany("INSERT INTO first VALUES (date, time, subject, object, source,
resource)", firsts)
    cur.executemany("INSERT INTO first VALUES (?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?, ?)",
firsts)
    conn.commit()
f.close()
```