РУХАНИ ЖАҢҒЫРУ

20 АСТАНА

ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ

Студенттер мен жас ғалымдардың
«ҒЫЛЫМ ЖӘНЕ БІЛІМ - 2018»
XIII Халықаралық ғылыми конференциясы

СБОРНИК МАТЕРИАЛОВ

XIII Международная научная конференция
студентов и молодых ученых
«НАУКА И ОБРАЗОВАНИЕ - 2018»

The XIII International Scientific Conference
for Students and Young Scientists
«SCIENCE AND EDUCATION - 2018»

12th April 2018, Astana

ҚАЗАҚСТАН РЕСПУБЛИКАСЫ БІЛІМ ЖӘНЕ ҒЫЛЫМ МИНИСТРЛІГІ
Л.Н. ГУМИЛЕВ АТЫНДАҒЫ ЕУРАЗИЯ ҰЛТТЫҚ УНИВЕРСИТЕТІ

Студенттер мен жас ғалымдардың «Ғылым және білім - 2018» атты XIII Халықаралық ғылыми конференциясының БАЯНДАМАЛАР ЖИНАҒЫ

СБОРНИК МАТЕРИАЛОВ XIII Международной научной конференции студентов и молодых ученых «Наука и образование - 2018»

PROCEEDINGS of the XIII International Scientific Conference for students and young scholars «Science and education - 2018»

2018 жыл 12 сәуір

Астана

УДК 378

ББК 74.58
Ғ 96

Ғ 96
«Ғылым және білім – 2018» атты студенттер мен жас ғалымдардың XIII Халықаралық ғылыми конференциясы = XIII Международная научная конференция студентов и молодых ученых «Наука и образование - 2018» = The XIII International Scientific Conference for students and young scholars «Science and education - 2018». – Астана: http://www.enu.kz/ru/nauka/nauka-i-obrazovanie/, 2018. – 7513 стр. (қазақша, орысша, ағылшынша).

ISBN 978-9965-31-997-6

Жинаққа студенттердің, магистранттардың, докоранттардың және жас ғалымдардың жаратылыстану-техникалық және гуманитарлық ғылымдардың өзекті мәселелері бойынша баяндамалары енгізілген.

The proceedings are the papers of students, undergraduates, doctoral students and young researchers on topical issues of natural and technical sciences and humanities.

В сборник вошли доклады студентов, магистрантов, докторантов и молодых ученых по актуальным вопросам естественно-технических и гуманитарных наук.

УДК 378

ББК 74.58

ISBN 978-9965-31-997-6

және шетелден келген қонақтарға, ұзақ уақытқа келген туристерге қаладағы мектепке дейінгі мекеменің орналасу орнын қарастырып өзіне жақынын, ыңғайлысын таңдай алады. Таңдап қана қоймай сайтына кіріп қажетті ақпарттарға қанық бола алады.

Осы мысалдың негізінде алгоритмдік деңгейде әдістемелік ұсыныстар әзірленді:

- мектепке дейінгі мекеме жобасының құрылуы мен мақталуы;
- нақты және абстрактылық кластар құрумен;
- кластар мен слоттардың байланысы;
- іріктеу жағдайында әртүрлі салыстыру операциялары, шаблондар, логикалық операциялар, пайдаланылатын тақырыптар бойынша білім базасынан алынған әртүрлі ақпарат сұрауларды жасау;
- сұраулар кітапханасынан сақталған сұрауларды жүктеу және сақтау;
- сұрауларды жіберу.

Еліміздің туристік-рекреациялық потенциалы бай болғанына қарамастан, ішкі өнімдегі туризмнің үлесі небәрі 0,9% құрайды. Негізгі мәселе елдегі дамыған инженерлік-транспорттық және туристік инфрақұрылымның жоқтығы, т.б. Сонымен қатар елімізді танытатын, туристерге толық ақпарат беретін порталдардың жоқтығы. Цифрлік Қазақстан - 2020 мемлекеттік бағдарламасының аясында «E-Tourizm» жобасын іске асыру қарастырылған. Оның міндеттерінің бірі – елдің, аймақтың әкімшілік-туристік ақпараты, туристік маршруттар, туристік және мәдени орындар туралы визуализациясы бар интерактивті карта жасау болып табылады. «E-Tourizm» порталы соның шешімі болмақ.

Қорытындылай келгенде мектепке дейінгі мекемелердің білім базасын құра отырып біз уақытты тиімді пайдалана отырып, үйден немесе жұмыс орнынан шықпай ақ Қазақстандықтардың ғана емес шетелген келген Астана қаласының қонақтарының да тез әрі керек мекемесін табуына қолайлы мүмкіндіктер туатын болады.

Қолданылған әдебиеттер тізімі:

1. Муромцев, Д.И. Онтологический инжиниринг знаний в системе Protégé / Д.И. Муромцев. – СПб.: СПб ГУ ИТМО, 2007. – 63 с.
2. http://www.elib.bsu.by
3. . Anne Cregan, Malgorzata Mochol, Denny Vrandecic, Sean Bechhofer. Pushing the limits of OWL, Rules and Protégé. A simple example.
4. Муромцев Д.И. Онтологический инжиниринг знаний в системе Protégé. – СПб: СПбГУИТМО, 2007.-62с.
5. http://ru.wikipedia.org/wiki
6. Стюарт Рассел, Питер Норвиг. Искусственный интеллект: современный подход 2-е изд.: пер. с анг. –М.: Изд.дом «Вильямс», 2006. – 1408с.: ил. Парал.тит.англ.
7. http://sherdim.rsu.ru/pts/semantic_web/REC-owl-guide-20040210_ru.html OWL, язык веб-онтологий. Руководство. Рекомендация W3C 10 февр. 2004.: пер. с анг. – Д. Щербин, 2004.

УДК 519.713

АҚПАРАТТЫҚ ҚАУІПСІЗДІК (АҚ) ОҚИҒАЛАРЫН ЖИНАҚТАУ ЖҮЙЕСІ

Тілдабай Нұрғиса Еркінтайұлы
Еуразия Ұлттық Университетінің Ақпараттық жүйелер бакалавры
Ғылыми жетекші : Жузбаев Серик

SIEM жүйесінің шығу тегі. Бүгінгі таңда ақпараттық қауіпсіздік әлемі тұрақты өзгеруде. Өзінің өзектілігін қолдау мақсатында қорғау жүйелері өздері дамып және бейімделуде. Қауіпсіздіктің қазіргі сәттегі жағдайы туралы мәліметтер келетін ақпараттар көздерінің саны әр күн сайын өсіп келеді. Бірақ, сонымен қатар инфрақұрылымның өсуімен

қатар ондағы болып жатқан жалпы көрініс қадағалап отыру да қиынға соғады. Егер пайда болып жатқан қауіп - қатерлерге уақытылы жауап беріп, оның алдын ала алмаса, рұқсатсыз кіруді анықтайтын жүздеген жүйелердің пайдасының керегі де болмайды. Бұл жағдайда көмекке қауіпсіздік ақпарат және оқиғаны басқару жүйесі Security Information and Event Management (SIEM) көмекке келеді [1].

SIEM-жүйесі бір шешімнің көмегімен қауіпсіздікке төнген қауіпті анықтап, басымдылықты беріп, оны жою қызметін атқарады. Бұл жүйе қауіпсіздік тералы ақпаратты және олардың оқиғаларын басқаратын жоғары, әрі тиімді өндірмелі жүйе шабуыл, қауіп және тәуекелдер туралы деректерді біріктіре отырып, қауіп туралы қажетті ақпараттарды жинап, жанжалдарға жылдам жауап беруге, оқиғалардың барлық журналдарымен оңай жұмыс істеуге, қауіпсіздік тәуекелдерін басқару үшін қажетті контекст құруға мүмкіндік береді .

SIEM-жүйесі өзі шабуылдарды жоя алмайды. Егер оқиға тіркелген болса, онда ол оқиға болып қойған. DLP ақпарат алмастыруды тоқтатқан, антивирус вирусты жойған немесе қолданушы ескертуден соң ақпаратты жіберу шешімін өзгерткен және т.б. жағдайлар болса, онда оқиғаның жалғасы болмайды [13]. Дегенмен SIEM ішкі ұрыс кезінде сізге дәлелдерді ұсына алады және сіз оларды қолдана аласыз.

Жүйеге жұмыс жасау кезінде қолдау құралдары қажет болады. Олар серверді өз еркімен басқарудан бастап үлкен ұйымдардағыдай АҚ құралдарының жаңаруын және қосылуына дейін қажет болады. Сол сәтте ережелерді реттеп, жаңарту керек. Деректер қорын және басқа да қызметтік есептерді оңтайландыруды көптеген SIEM-жүйелері орындай алады.

SIEM-жүйесінің типтік құрылымы:

➢ Агенттер – ақпараттық жүйеге орнатылады және серверге жүйеден деректерді жібереді, агенттердің құрамын деректерді түрлендіру үшін модульдері қамтуы мүмкін;

➢ Сервер – коллектор – әр түрлі көздерден оқиғаларды жинайды;

➢ Сервер – коррелятор – агенттер мен коллекторлардан келген ақпаратты жинайды және өңдейді;

➢ Деректер қорының сервері – оқиғалар журналын сақтайды.

Жүйенің функциялары мен жұмыс істеу қағидасы

SIEM-жүйесінің алдына қойылатын келесі міндеттер: әр түрлі көздерден келген оқиғалардың журналын сақтау және шоғырландыру, оқиғаларды талдау мен іс-шараларды бөлу үшін құралдардың берілуі, ереже бойынша оқиғаларды өңдеу және корреляциялау, оқиға-менеджмент және автоматты түрде ақпарат беріп отыру. Жүйенің жұмыс жасауы:

1. Оқиғаларды талдау және аномалия (жүйелік қозғалыс, қолданушының күтпеген іс-әрекеттері, танылмаған құрылғылар және т.с.с.) болған жағдайда ескертулерді шығару.
2. Стандарттарға (PCI DSS, COBIT және т.б.) сай келетіндігін тексеру.
3. Өзіңіздің керектігіңізге негізделіп қолданылатын керемет есеп жасау. Мысалы, шабуылдар туралы күнделікті есеп, шабуыл жасаушылардың апта сайынғы тізімі, құрылғылардың жұмыс қабілеттілігі туралы есеп және т.б. Есептер өздерінің алушылары сияқты икемді реттеледі.
4. Маңызды жүйелер/серверлер/құрылғылардан келетін оқиғаларға мониторинг жасау, қызығушылығы бар адамдарға тиісті ескертулер құру.
5. Жеткілікті басқарушылардан АҚ жүйелеріне қаражаттарды алуға көмегін тигізу.
6. Осалдықтарды көрсететін сканер болған жағдайда, SIEM тәуекелдер тұрғысындағы проблемаларды жоюға көмектеседі.

Жүйеде қолданылатын негізгі функцияларға тоқталып өтсек:

➢ *Біріктіру (агрегация)* белгілі бір белгісі бойынша ұқсас оқиғаларды біріктіреді; деректер журналын басқару; қосымша, деректер қоры, серверлер, қауіпсіздік жүйелерінің

нүктелері, сервистер мен желілік құрылғылардың түрлі көздерінен деректерді жинайды; сыни оқиғаларды іздеу мақсатында деректерді шоғырландыруды қамтамасыз етеді.

➢ *Корреляция* белгілі бір кластерге жататын оқиғаларды байланыстырып, ортақ атрибуттарды іздеу. Бұл технология енгізілген деректерді мағыналы ақпаратқа айналдыру үшін қолданылатын әр түрлі көздердегі деректерді өңдеудің технологиялық әдістерін қолдануға мүмкіндік береді. Корреляция Security Event Management жиынының типтік функциясы болып табылады.

➢ *Хабарлама* қазіргі уақыттағы проблемалар туралы хабарларды (ескертулер) генерациялау және корреляцияланатын оқиғаларды автоматты түрде талдау. Хабарламалар қосымшаның өзінің тақтасында көрсетілуі мүмкін және басқа да үшінші тарапқа бағытталуы да мүмкін: электрондық пошта (e-mail), GSM-шлюз және т.б.

➢ *Бейнелеу құралы (ақпараттық тақталар)* стандарт тәртіптен айырмашылығы бар паттерндерді анықтауға көмегін тигізетін диаграммаларды көрсету.

➢ *Үйлесімділік* (*transformability)* автоматты түрде деректерді жинауға, ақпараттық қауіпсіздік пен аудиттті басқаруы бар процесстердегі деректерді біріктіріп бейімдеу есептерін әзірлеуге қосымшаны пайдалану.

➢ *Деректерді сақтау* үйлесімділікті қамтамасыз ету және уақыт бойынша деректердің корреляциялануы үшін тарихи реттегі деректерді сақтау қорын ұзақ уақыт қолдану. Деректерді ұзақ уақытты деректер сақтау компьтерлі-техникалық сараптама жүргізуге сыни болып келеді, себебі желілік шабуылды зерттеу шабуыл болып жатқан кезде жүрмеуі мүмкін.

➢ *Сараптамалық талдау:* түрлі тораптардан көптеген уранлдарды іздеу мүмкіндігі; бағдарламалы-техникалық сараптама аясында орындалуы мүмкін.

➢ *Қалыпқа келтіру (нормализация)* әр түрлі көздерден бірыңғай ішкі форматқа жиналған журнал жазбаларын сақтау мен келесі өңдеуде қолданылатын форматтарды келтіруді білдіреді.

➢ *Басымдылығын анықтау (приоритезация)* жүйеде анықталған және ережелерге негізделген қауіпсіздік оқиғалардың маңыздылығы мен сыншылдығын анықтайды.

➢ *Ақпараттарды визуализациялау* қауіпсіздік оқиғаларын талдау нәтижелері және қорғалып тұрған инфрақұрылым мен оның элементтерінің жағдайын сипаттайтын деректерді графикалық түрде ұсынады.

➢ *Шешімдерді қабылдау* инфрақұрылымдардың қауіпсіздігін қалпына келтіру немесе шабуылдардың алдын алу мақсатында қорғау құралдарын қайта баптаудың шараларын өндіруді айқындайды.

SIEM-жүйесінің жұмыс істеу қағидасы . Теорияда барлығы қарапайым: жүйе ақпараттарды жинап, оларға талдау жасайды және алдын алатын хабарламалар жасайды, деректер қорына енгізеді, алдында болған шабуылдарға бақылау жасау негізінде талдайды да хабарламаларды шығарады. Практикада бұл тізбек белгілі бір компоненттердің көмегімен жүзеге асады: агенттер (түрлі көздерден деректерді жинау), сервер-коллектор (агенттерден келетін ақпараттарды анықтау), деректер қорының сервері (ақпараттарды сақтау), сервер-корреляция (ақпараттарды талдау).

SIEM жүйесінің ақпаратты алу көздері. Деректер көзінің көп мөлшері дегеніміз кәсіпорынның АТ-инфрақұрылымында тіркелетін барлық оқиғаларды толық және мұқият қамту болып табылады. Өзінің алдына қойған мақсаттарды орындау үшін SIEM жүйесі келесі ақпарат көздерін қолданады :

Access Control, Authentication. Артықшылықтарды қолдану және ақпараттық жүйелер қатынасын басқаруға талдау жасау үшін қолданылады.

DLP-жүйелері. Қатынас құқықшылығын бұзу, инсайдерлік шығң әрекеттері туралы ақпарат.

IDS/IPS-жүйелері. Желілік шабуылдар, конфигурацияларды өзгерту және құрылғыларға қолжетімділік туралы мәліметтерді енгізеді.

Антивирустік бағдарламалар. Шабуылды кодтар, конфигурациялардың өзгеруі, деректер қорының және бағдарламалық қамсыздандырудың (БҚ) жұмыс істеу қабілеттілігі туралы оқиғаларды жинақтайды.

Жұмыс станциялары мен серверлердің оқиға журналдары. Қолжетімділікті басқару, үзіліссіздікті қамсыздандыру, ақпараттық қауіпсіздіктің саясатын сақтауда қолданылады.

Желіаралық экрандар. Шабуылдар, зиянды бағдарламалық қамсыздандырулар (БҚ) және т.б. туралы ақпараттар.

Желілік белсенді құрылғы. Қолжетімділікті басқару мен желілік трафикті тіркеуге қолданылады.

Осалдылық сканерлері. Активтер, сервистер, бағдарламалық қамсыздандыру, осалдықтарды түгендеу және сол туралы деректерді жеткізу мен топологиялық құрылым туралы мәліметтерді жеткізеді.

*Түгендеу жүйелері және asset-management.*Инфрақұрылымда активтерді бақылау және жаңа активтерді табу туралы мәліметтерді жеткізеді.

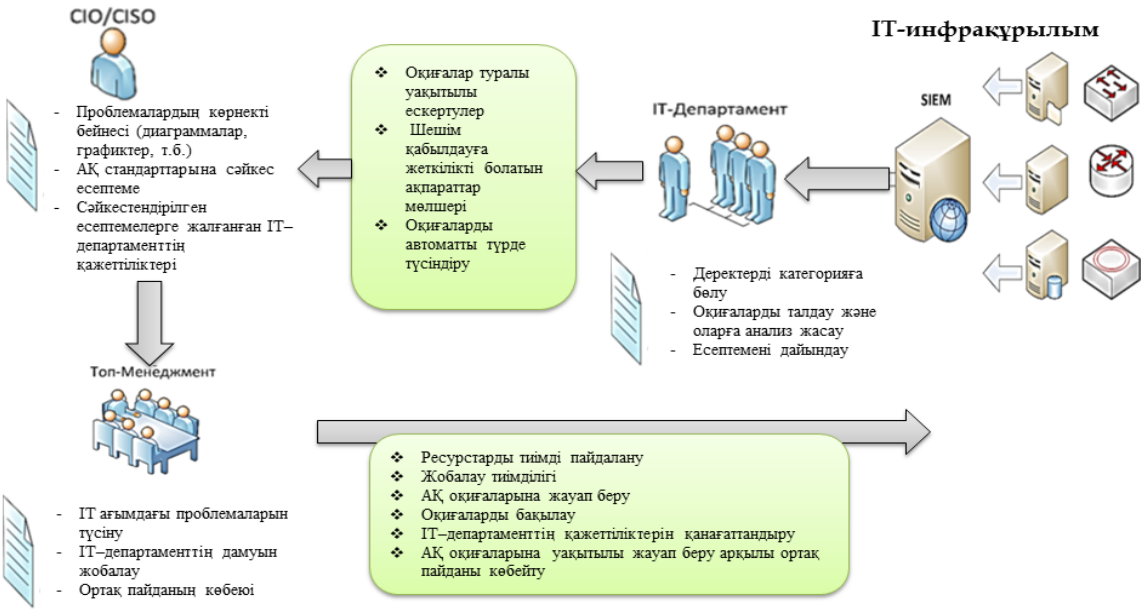
Веб-фильтрация жүйелері. Қызметкерлердің күдікті және тыйым салынған веб-сайттарға кіргендігі туралы ақпараттарды береді.

Сурет 1.1 SIEM жүйесі қолданатын ақпарат көздері

SIEM жүйесінде ақпараттарды жинау үшін бірнеше түрлі компонеттер қолданылады. Олардың арасында тексеріліп отқан ақпараттық жүйеге орнатылатын агенттер, белгілі бір оқиға журналын немесе жүйені түсінуге арналған агенттердгі коллекторлер, көптеген көздерден келген оқиғаларды алдын ала жинайтын сервер-коллекторлер, оқиғалар журналының сақталуына жауап беретін деректер қорының сервері бар.

SIEM жүйесі бізге ақпараттарды жинау және талдау үшін қажет. Ақпарат әр түрлі көздерден келеді: DLP-жүйелері, IDS, маршрутизаторлар, желіаралық экрандар, АРМ қолданушылар және серверлер . Үлкен сандқ көлемді көздерден әрқайсысынан жеке қарап, тексеру қиынға соғады. Сондай-ақ түрлі көздерден алынған сыртынан қауіп төндірмей тұрған оқиғалар шабуыл жасайтын жағдайлар да кездеседі. Егер де ұйым ішіндегі белгілі бір қолданушы сезімді хатты өзінің қарапайым жіберіп жүрген адрестеріне емес, басқа белгісіз бір адреске жіберетін болса, бұл жағдайды DLP-жүйесі анықтау алмайды, ал SIEM жүйесі жиналған статистиканы қолдана отырып, қауіпті оқиғанын болғанын анықтай алады. Шабулы болған соң, оны жасаған пайдаланушы өз шабуылын мойындамаса, бұл жүйе қажетті дәлелдерді шығарып, көрсетіп бере алады. Айта келетін болсақ, бұл жағдай жүйенің негізгі мақсаты болып табылады. Шабуыл пайда болар сәтте оған қатысты адамдардың барлығы көрсетіледі.

Белгілі бір стандарттарға сай периодты түрде аудиттер жүргізу керек болса, SIEM жүйесін қолдануға болады. Қосымша мүмкіндіктеріне қарай АҚ қаражаттарын да реттеп отыра алады. SIEM жүйесі қандай жағдайларда пайдалы екендігі төменде көрсетілген. Егер SIEM жүйесі болмаған жағдайды сурет 1.3-тен байқауға болады.



Сурет 1.2 Ұйымда SIEM жүйесі болған жағдай

Бұл суреттерде SIEM жүйесінің не үшін қажет болатындығын анықтап, көсетеді. Бұл жүйе қазіргі таңда дамыған және де әлі де дамып келе жатқан өнім болып табылады. Оның фунциялары күннен күнге ұлғайып өсуде.

SIEM тек қана ақпараттық қауіпсіздіктің құралы ғана емес, барлық ақпараттық технологияның құралы екенін түсінген жөн. Күшті корреляциялық механизмдердің негізінде IT-сервистердің тоқтаусыз жұмысын тиімді қамтамасыз етуге, ақпараттық пен операциялық жүйелер және құралдық қамсыздандырудағы қателіктерді анықтауға болады. Сондай-ақ бұл жүйе автоматтандыру құралы болып табылады. Қарапайым көптеген ұйымдарда өзекті мысал келтірсек, IP-адрестердің қақтығысы. Бұл проблеманы қарапайым RBR ережесін қолдана отырып, қолданушының қоңырауының алдында анықтауға болады. Сонымен қатар, қателікті жою шығындары азаяды, яғни бизнестегі мүмкін болатын финанстық қиындықтар да азаяды.

Практикада SIEM-жүйесін қолдана отырып, шынайы қолданысты талдайтын болсақ, әр түрлі ақпарат көздерінен келетін оқиғалар журналдарын шоғырландыруға арналғандығын байқасақ болады. Шындығында келгенде, тек қана SIM функционалы ғана қолданылады. Берілген корреляция ережелері бар болса да, олар толықтырылмайды.

Қорытынды. Ағымдағы проблемалар туралы хабардандырудың жасалуын, жинақталған есептерінің жасалуын, сондай-ақ Интернеттен ақпараттық ресурстарға желілік деңгейде қолжетімділігін бұғаттау қажет болған кездегі, (оның ішінде, байланысатын) оқиғаларын автоматты түрде талдау үшін SIEM жүйесі енгізілді.

Жаңа ұрпақтың SIEM-жүйесі үлкен сандық мөлшердегі ақпарат көздерінен деректерді жинай алады. Сонымен қатар, оқиғалар туралы деректер ақпарат көздеріне орнатылған агенттердің көмегімен ғана жиналмайды, протоколдар бойынша байланыс арқылы қашықтан жиналады.

SIEM-жүйесінің көмегі арқылы жасай алатын жұмыстардың тізімін қарастырайық: журналдар, ағындар және әлсіздіктерін корреляциялау; желілік қауіпсіздік құралдарының конфигурациясына мониторинг жасау; әлсіздіктердің басымдылығын анықтау; желілерді талдау; симуляция мен залалдарды модельдеуді болжау; тәртіптің аномалияларды табу; толық талдау мен зерттеулер жүргізу үшін контентті алу және т.б.

Әрине, жүйенің тиімді ақпарат көздері көп болса, залалдың пайда болу кезеңін ертерек табу ықтималдығы да көбейеді. Жүйені немесе осалдық сканерін жеке қолдануға

болады. Бірақ сипатталған байланыс тәуекелдердің мөлшерін азайтады. Яғни, сканер мен жүйе екеуін бірге қолданған дұрыс болып табылады.

Қорытындылай келе, бұл жүйенің көмегімен көптеген жұмыстарды жасай алатынымызды білдік. Осы жүйені елімізге толығымен енгізіп, әрбір ұйымның немесе кәсіпорынның ақпараттарын ғана емес, мемлекеттегі маңызды жасырын құпия ақпараттарды қорғауға мүмкіндік алу. Жүйе тек қана қауіп төндіріп тұрғаны туралы ақпарат беретін болғандықтан, оны ары қарай дамытып, сол қауіптерді жоя алатындай жаңа бір жүйе ойлап табу қажет.

Пайдаланылған әдебиеттер тізім:

1. Котенко И. В., И. Б. Саенко, О. В. Полубелова. Перспективные системы хранения данных для мониторинга и управления безопасностью информации, Тр. СПИИРАН. 2013. № 25. С. 113-134.

2. Karlzen H. An Analysis of Security Information and Event Management: The Use of SIEMs for Log Collection, Management and Analysis. Department of Computer Science and Engineering, University of Gothenburg. 2009.

3. Kotenko I.V., Chechulin A.A. A Cyber Attack Modeling and Impact Assessment Framework // Proceedings of 5th International Conference on Cyber Conflict 2013 (CyCon 2013). 2013. pp. 119–142.

4. Файзуллин Р. Р., Васильев В. И. Метод оценки защищенности сети передачи данных в системе мониторинга и управления событиями информационной

УДК 519.713

АВТОМАТЫ БЕЗ ВЫХОДА В КРИПТОГРАФИИ

Шахметова Гульмира Балтабаевна
Евразийский национальный университет им. Л.Н.Гумилева, Астана, Казахстан
Научный руководитель – Шарипбай А.А.

Еще с древних времен человечество интересовало обеспечение секретности передаваемой информации. Создавались различные виды кодирования информации, изобретались новые устройства для создания стойких шифров и легкого шифрования сообщений. Долгое время криптографические методы шифрования были засекречены, и применялась только с целью обеспечения секретности военных и государственных тайн. Ситуация кардинально поменялась в XX веке с появлением персональных компьютеров, тогда возникла естественная потребность в защите персональных данных. С развитием информационных технологий, на замену старых шифров приходили усовершенствованные и более стойкие алгоритмы шифрования/дешифрования, и как следствие интерес к такой науке, как криптография стремительно возрос. Основная цель криптографии – это обеспечить целостность, конфиденциальность, аутентификацию данных и неотказуемость авторства [1]. Достигаются эти задачи путем преобразования (шифрование) пересылаемого открытого текста в непонятный зашифрованный текст, а затем дешифрования этого сообщения обратно в его первоначальную форму.

Первое время широкую известность имела симметричная криптография, а позже и асимметричная. Симметричная криптография включает в себя криптографический алгоритм с использованием одного секретного ключа, в то время как асимметричное шифрование представляет собой криптосистему с двумя ключами: открытым и закрытым. В симметричной криптосистеме при шифровании и дешифровании пересылаемого сообщения используется один ключ, известный как отправителю, так и получателю и передаваемому по засекреченному каналу. В асимметричной криптосистеме передаваемое сообщение шифруется с помощью открытого общедоступного ключа, а для дешифрования данных