МРНТИ 28.17.31

А.А. Амирбай[1], А.А. Муханова[1]

[1]Л.Н. Гумилев атындағы Еуразия ұлттық университеті,
Нұр-Сұлтан қ., Казақстан

КӘСІПОРЫННЫҢ АҚПАРАТТЫҚ РЕСУРСТАРЫН ҚОРҒАУДА ЭКСПЕРТТІК БАҒАЛАУ ӘДІСІМЕН ШЫҒЫНДАНУ ТӘУЕКЕЛДІЛІКТЕРІН ЕСЕПТЕУ

Түйіндеме. Мақалада ақпараттық қауіпсіздікті қамтамасыз етумен, сонымен қатар компьютерлік жүйеде ақпараттық ресурстарды қорғау шараларын ойдағыдай жүзеге асыру үшін қауіп-қатерді бақылау жүйесін құрумен және SIEM жүйесінің функционалдық жүйелері негізінде тәуекелдерді есептеудің толық кешенді алгоритмін іске асырумен байланысты проблемалар талқыланады. Кәсіпорын компьютерлік жүйеден және ақпараттық ресурстардан қауіп-қатерге ұшыраған жағдайларда сараптамалық бағалауды негізге ала отырып, мәліметтер базасын құру ұсынылады. Сонымен қатар, шығындарды болдырмау үшін, сондай-ақ ақпаратты сақтаудың минималды тиімді тәсілі ретінде триплет түрінде шифрлауды қолданған жөн және репозиторийлерде триплеттерді сақтау алгоритмін құру ұсынылады.
Түйінді сөздер: қатер, тәуекелдік, триплет, триплет қоймасы.

• • •

Аннотация. В статье рассматривается проблема связанная с обеспечением информационной безопасности, а также с созданием системы мониторинга угроз для успешной реализации мероприятий защиты информационных ресурсов в компьютерной системе и реализации полного комплексного алгоритма расчета рисков на основании функциональных подсистем системы SIEM. Предложено создание базы данных на основе экспертной оценки, для случаев, когда предприятие подвержено угрозам компьютерной системы и информационных ресурсов. Кроме того, для предотвращения затрат, а также как минимальный эффективный способ хранения информации, рекомендуется использовать шифрование в виде триплета и создание алгоритма хранение триплетов в репозиториях.
Ключевые слова: угроза, риск, триплет, хранилище триплетов.

• • •

Abstract. The article deals with the problem of ensuring information security, as well as creating a system for monitoring threats for the successful implementation of measures to protect information resources in a computer system and the implementation of a complete integrated algorithm for calculating risks based on functional subsystems of the SIEM system. The work proposed the creation of a database based on expert assessment, when an enterprise is exposed to threats of informa-

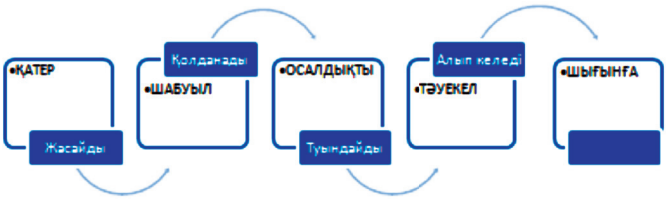
tion resources in a computer system. In addition, to prevent costs, as well as the minimum effective way to store information resources, it is recommended to use encryption in the form of a triplet and the creation of an algorithm for storing triplets in repositories.
Keywords: threat, risk, triple, triplestorage.

Кіріспе. Ақпараттық технологиялардың енуі мен қарқынды дамуы жаңа құралдардың пайда болуы мен ақпаратты өңдеу әдістерін ғана алып келген жоқ, сонымен қоса жаңа ақпараттық қауіпсіз қатер, жүйе әлсіздігі мен компьютерлік шабуылдардың жаңа түрлерінің пайда болуына да алып кеп соқты. Компьютерлік жүйеде ақпараттық ресурстарды қорғауды тиімді жүзеге асыру үшін, қауіпсіздік қауіп-қатер мониторинг жүйесін құрумен байланысқа негізделген бүтін сан қатар есебін шығару қажет. Мониторинг жүйесі ақпаратты қорғауда ағымдық амалын жүзеге асырады және құрудағы негізгі мақсаты компьютерлік жүйеде ақпараттық ресурстарға әсер еткен қатерлерден туындайтын қатерлі тәуекелдер деңгейін төмеңдету және пайда болған шығындарды азайту. Қазіргі таңда қауіп-қатер қауіпсіздік мониторинг жүйесін құрудағы ең маңызды және перпективті бағыттың бірі қауіпсіздік оқиға және ақпаратты басқаруды қамтамасыз ететін жүйе SIEM (Security Information and Event Management) болып табылады. Кез – келген SIEM – жүйесінің орталық компоненті – деректер қоймасы [1]. Деректер қоймасында SIEM – жүйесінің аналитикалық модулінен келіп түсетін сұраныстарды өңдеу мен деректерді сақтау іске асады. SIEM – жүйесі ақпараттық қауіпсіздік деңгейінің көтерілуіне әсер етеді, сонымен қоса қауіпсіздік оқиға мен программалық қақтығыстар қауіп-қатерге ұшырамай түрып басқаруды жүзеге асырады. Жұмыстың мақсаты компьютерлік жүйеде ақпараттық ресурстарды нақты уақыт режимінде қорғауды болжау және оңтайландыру мәселелерін шешу үшін жеке SIEM – жүйесінің тораптарын толтыру туралы кейбір пікірлерді ұсыну. Кәсіпорынның компьютерлік жүйесінде ақпараттық ресурстарға қарсы шабуылдаған қатерлердің жүзеге асу мүмкіндігі орын алғанда пайда болған тәуекел деңгейін эксперттік әдіс бойынша бағалау және шығының есептеу жөнінде базасын жүйеде құру. Эксперттік бағалау әдісі бойынша SQL Server 2012 жүйесінде қатерлі тәуекелдердер деңгейін сандық әрі сапалық бағалау және мүмкін болған шығындарды барлық қатерлер үшін есептеу жүргізіп, процедуралар құрылды. Сондай-ақ жұмыста күрделі шығындарды алдын-алу мақсатында, контршаралар мен АР-ды сақтаудың ең ми-

нималды, тиімді әдісі–триплеттерді пайдаланумен, жоғарыда аталған есептеудің толық кешенді алгоритмін, SIEM – жүйесінің жүйелік қосымшаларына сай келетіндей жүйеде жүзеге асыру іс-әрекеттері жүзеге асырылды. SIEM – жүйесінің жүйелік қосымшаларының қызметі негізінде жүргізілген есептеулердің толық кешенді алгоритмі компьютерлік жүйеде ақпараттық ресурстарддың нақты уақыт режимінде қорғауды болжау, тәуекелдерді бағалау мен деңгейін төмендетуге, шығындарды азайтуға мүмкіндік береді [1, 2]. Қатерлерден қорғау шаралары арасында, ақпараттық ресурстарды сақтаудың ең тиімді әдісі – триплеттерге бағытталған деректер сызбасы ұсынылды, триплеттер қоймасына арналған саралау жұмыстары жүргізілді, олардың мүмкіндіктері мен архитектурасы қарастырылды, соңымен қоса перспективалық SIEM – жүйесі үшін ең қолайлы деректерді сақтау қоймасы таңдалынды [2].

Ақпаратты қорғау саласындағы тәуекелдерді бағалау. Ақпараттық қауіпсіздік ақпараттың иелеріне немесе пайдаланушыларға зиян келтіруі мүмкін бір немесе бірнеше АЖ критерийлерінің (құпиялылық, қол жетімділік, тұтастық) бұзылуына байланысты кездейсоқ немесе қасақана ақпараттық ресурстарды және қолдаушы инфрақұрылымды қорғау жағдайы ретінде түсініледі [3]. Компьютерлік жүйеде ақпараттық ресурстардың бұзылуы сөзсіз шығындарға әкеп соғады: қаржылық, операциялық, тұтынушылық зиян, қызметкерлерге келтірілген зиян. Ең маңызды қауіпсіздік көрсеткіштерінің бірі - қатер.

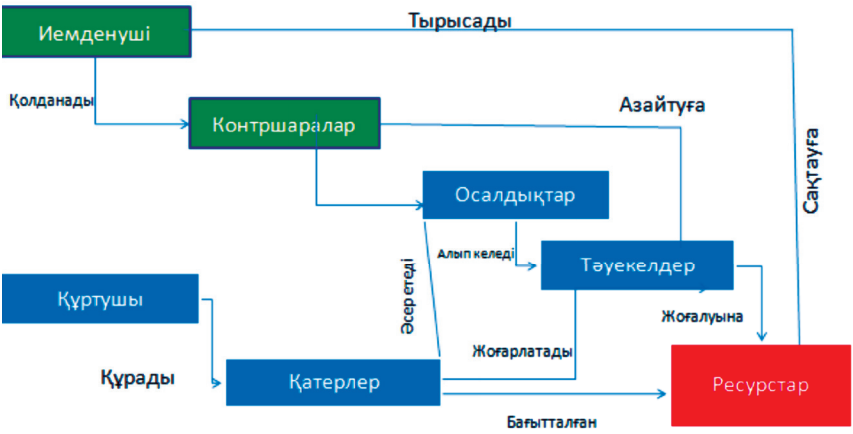
Кез-келген саладағы кәсіпорындардың қызметі белгілі бір дәрежеде тәуекелді болып табылады, бұл адам факторлары мен компания жұмыс істейтін саланың сипатына байланысты. Ақпараттық шабуылдар кәсіпорындардың ішкі және сыртқы бұзушылары және осалдықтарды пайдаланып бағдарламалық қамтамасыз ету бойынша жүзеге асырылады. Шабуылдар арқылы жүзеге асырылатын осалдықтар мен қатерлер арасындағы қарым-қатынас тәуекелдің пайда болуы алып келеді, төменде процес 1 - шы суретте көрсетілген.



1 сурет - Қауіп-қатерлердің пайда болуы мен іске асыру процесі

Ақпараттық жүйенің осалдығы(vulnerability)- кемшіліктер болып табылады, көбіне жүйені жобалау немесе кодтау кезінде жасалған қате болып табылады.

Ақпараттық технологиялар және ақпараттық қызметтер үшін дамып келе жатқан нарықтар маңызды назар аударуды және зерттеуді талап етеді, себебі құнды және маңызды ақпаратты иелену, пайдалану және беру есебінен компанияға елеулі зиян келтіруі мүмкін бірқатар тәуекелдер болуы мүмкін. Мұндағы, *тәуекел дегеніміз - кәсіпорынның кейбір ресурстарын жоғалту ықтималдығы, кіріс тапшылығы немесе бизнесті жүргізу барысында қосымша шығындардың пайда болуы.*Құқық бұзушылардың шабуылынан ықтимал шығындарды бағалауға және оны азайту жөніндегі шараларды таңдауға арналған тәуекелге негізделген тәсіл ақпараттық қауіпсіздікте кеңінен қолданылып, тәуекелдерді басқару деп аталды. Тәуекелдерді басқару тұжырымдамасын әртүрлі көздерде әр түрлі болады.Тәуекелдерді басқарудың негізгі кезеңі тәуекелдерді басқару әдістері мен құралдарын таңдау кезеңі болып табылады. Төменде 2-суретке сәйкес, модель мынадай түрде құрастырылады: бөлінген ресурстарға олардың тиісті қаржылық шығындары бойынша да, сондай-ақ ұйымның беделіне залал келтіру, оның қызметін бұзу, құпия ақпаратты жариялаудан материалдық емес зиян. Содан кейін ресурстардың өзара байланысы сипатталған, қауіпсіздік қатерлері анықталады және олардың орындалу ықтималдығы бағаланады.



2 сурет - Ақпараттық тәуекелдерді бағалау алгоритмі

Ақпараттық тәуекелдерді талдау - бұл сандық (ақша ресурстарының түрінде) және сапалы (тәуекел деңгейі: жоғары, орташа, төмен) тәуекелдік индикаторларын анықтау арқылы ақпараттық жүйені қорғау деңгейін бағалау процесі. Талдау ақпаратты қорғау процестерін қалыптастырудың әр түрлі құралдары мен әдістерін қолдану арқылы жүзеге асырылады. Тәуекелдерді талдаудың негізі – тәуекелдерді сәйкестендіру процесінде жиналған SIEM-жүйесінің репозиторийінен алынған статистикалық деректер және жүйе талдаушысының жұмысының нәтижелері SIEM жүйесіндегі тиісті түйіндерден немесе процедуралармен пайдаланылады, олар шешім қабылдайды [4]. Қазіргі кезде тәуекелдерді талдау және бағалау үлгілері тәуекелді басқаруды белгісіздік кезінде шешім қабылдау ретінде және даму барысында альтернативті немесе қосымша шешімдер қабылдау критерийлері ретінде сандық тәуекел көрсеткіштерін қарастыратын даму сатысында. Тәуекелдерді бағалау – тәуекелдерді басқарудың жалпы жүйесінің маңызды құрамдас бөлігі. Бұл тәуекел дәрежесін сандық немесе сапалы түрде анықтау үдерісі. Сапалы талдаудың негізгі міндеті, тәуекелдердің мүмкін түрлерін анықтаудан басқа, тәуекелдің осы түріне әсер ететін себептер мен факторларды анықтау және сипаттау болып табылады. Сараптамалық бағалау әдісі - белгілі бір мәселе бойынша сараптамалық қорытынды алуға бағытталған логикалық және математикалық процедуралар кешені. Бұл әдістің артықшылығы, басқару шешімдерін оңтайлы шешуге арналған құзыретті маманның тәжірибесін және түйсінуін қолдана алады, тәуекелдер сипаттамалары сарапшы құралдармен белгіленуі мүмкін.

SIEM – жүйесін құру және жұмыс істеуін бақылаудағы негізгі мақсат ақпараттық–телекоммуникациялық инфрақұрылымда ақпараттық қауіпсіздіктің деңгейін айтарлықтай көтеру, қауіпсіздік туралы ақпаратты манипуляциялау және қауіпсіз оқиға мен программалық қақтығыстарды “проактивті” басқаруын жүзеге асыру. Мұндағы “проактивті” дегеніміз “қауіп-қатерге ұшырамай түрып әрекет жасау” деген мағыльнаны береді [3, 4].

SIEM–жүйесі ақпараттық инфрақұрылысты сақтай алатындай «қосымша сервері» мен «деректер қоймасы» деп аталатын «агенттер» құрылысы бар. *Агенттер* деректердің алғашқы өңдеуі мен сүзбесін, қауіпсіз оқиғалар жинағын орындайды. Жиналған және сүзілген деректерді сақтау үшін деректер қоймасына өтеді, сосын келесі қадамды орындау мақсатында ішкі форматында сақталады.*Қосымша сервері* болса ақпарат сақтаудың негізгі қызметін атқарады. Ол кой-

мада сақталған деректерге саралау жөмыстарын жүргізіп, ақпаратты қорғау ескертулерін шығару үшін өндіріске түрлендіреді.

Бірінші деңгейде *деректерді жинау* әрқилы дереккөздердің түрлері арқасында жүзеге асады. Әрқилы дереккөздердің форматы түрліше типте болады. Олардың қатарына: файлдық серверлер, деректер қорының серверлері, Windows – серверлері, желіаралық экрандар(ЖАЭ),жұмыс станциялары,шабуылдарға қарсы жүйелер (IPS, intrusion prevention systems), вирусқа қарсы программалар және т.б. Екінші деңгейде қоймада сақталатын, қауіпсіз оқиғалар туралы басқару жүзеге асады. Қоймада сақталынған деректер *деректерді саралау* деңгейінде сұралатын сұраныс нәтижесінде алынады [5]. Бұл деңгейде тәуекелдерді сандық және сапалық бағалау сияқты көптеген операциялар жүзеге асады. Үшінші деңгейде алынатын, SIEM – жүйесіндегі деректерді саралау деңгейі блып табылады. Өңдеу нәтижесі болып алдын-ала сипатталатын ерікті түрдегі отчеттар, оперативті оқиға туралы (on-line) деректер корреляциясы, сонымен қоса on-line режимде өндірілетін ескертулер жатады.

SIEM – жүйесінің жаңа буындарының жұмыс істеу механизмі арасындағы байланыс функционалды моделдің бейнесін көрнекті түрде көрсетеді (сурет 3). Көріп тұрғанымыздай, SIEM-жүйесінде бес негізгі функционалдық жүйеліктер бар: деректерді жинақтау, деректерді өңдеу, сақтау, деректерді саралау және көрсету. Мұнда бастапқы екеуі on-line режимінде, ал қалғандары соған жақын түрде қызмет атқарады.

3 сурет - SIEM-жүйесінің функциональді моделі

Эксперттік бағалау негізінде тәуекелдерді есептеу. Қолайсыз оқиғаларды іске асырудан ақпараттық жүйелерде әдіснамалық

зиянды бағалау тәуекелдерді бағалауға байланысты. Тәуекелдер бойынша есептеулер ақпараттық жүйелерде пайда болатын жағымсыз оқиғалардың ықтималдығы негізінде есептеледі. Қолайсыз оқиғалардың пайда болуының объективті және субъективті ықтималдығы бар. Қолайсыз оқиғалардың пайда болуының объективті ықтималдығын бағалау тәуекелдерді бағалауды есептеудің алгоритміндегі маңызды міндеттердің бірі болып табылады. Қатерлер орын алғанда, қатерлердің жүзеге асу деңгейі артып, тәуекел деңгейі өседі де ықтимал шығындарды есептеуде эксперттік бағалау негізінде тәуекелдерді сандық және сапалық әдіспен есептейміз. Тәуекелдерді бағалаудың негізі - тәуекелдерді өңдеу жүйелігінде жиналған, SIEM-жүйесінің қоймасынан алынған статистикалық деректер пайдаланылады.

SIEM-жүйесінің қоймасында жиналған қатерлер тізімі, ақпараттық рессурстарды елеулі түрде бұзатын келеңсіз оқиғалардың кейбір маңызды жиындары бар. Бұл ішкі жиын келесідей белгіленеді [6]:

$$K = \{K_{i_1}, K_{i_2}, \dots, K_{i_m}\}$$

K жиынтығын құрғаннан кейін, компьютерлік жүйенің жүйелік тиімділігінің төмендеуіне әкелетін барлық қатерлердің сандық көрсеткіштеріне негізделген ішкі жиындар элементтерінің қасиеттерін талдауды жалғастырамыз. ΔT кезінде келеңсіз оқиғалардың і-ші салдарынан туындаған қатердің математикалық күтуі (мысалы, 1 ай) келесі формула арқылы ұсынылуы мүмкін:

$$v(K_i, \Delta T) = M[v(K_i) * f_i], \qquad i = 1 \dots m$$

Мұнда, $v(K_i)$ – қатерлердің жүзеге асу мүмкіндігі;
f_i – ΔT кезінде і-ші қатерлердің кездейсоқ мәні;
m – барлық қатерлердің жалпы саны.

Егер қолайсыз оқиғалар әрбір қатерлердің зақымдануынан тәуелсіз болса, онда

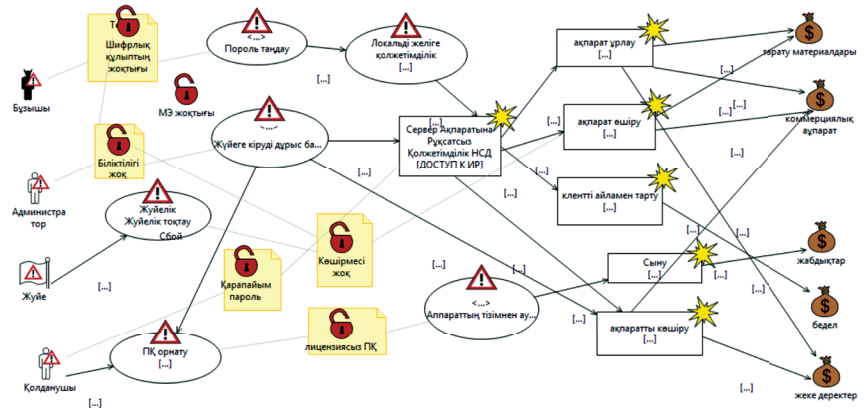
$$v(K_i, \Delta T) = M[v(K_i)] * M[f_i], \qquad i = 1 \dots m$$

және көптеген қатерлерден келтірілген шығын осы арақатынасымен анықталады:

$$V(K_i, \Delta T) = \sum_{i=1}^{m} M[v(K_i) * f_i],$$

Тәуекелдерді бағалау - кәсіпорынның немесе SIEM жүйесінің қоймасындағы, ақпараттық ресурстарға қарсы қатерлі шабуылдардың

шығындану мүмкіндігін бағалау үшін жинақталған, талданған, сақталған, өңделген статистикалық деректерге негізделген [6, 7]. Кәсіпорынның құнды дүниелері (активтер) мен олардың маңыздылығын анықтай отырып, бұлардың құрту, жою, өшіру және т.б. қолайсыз жағдайларды тудыратын қатерлерді тауып, тізімін құрдық. Қатер тудырушылардың негізгі мақсаты да осы құнды дүниелерге қол жеткізу. Құнды дүниелерге әсер етуші компьютерлік жүйенің Қатер, Осалдығы, Қатер тудырушылар, Пайда болу мүмкін Тәуекелі мен Пайда болу мүмкін шығынның анықтау қажет. Зерттеу барысында анықталған қатерлер мен оларға сәйкес осалдықтар тізімі және активтер мен шабуыл жасаушы бұзушылар тізімін визуалды 4- ші суретте бейнелейміз.



4 сурет – Активерге қарсы шабуылар

Қауіп-қатер ықтималдығын және ықтимал зақым дәрежесін бағалау негізінде тәуекелдерді бағалау жүргізіледі. 1-кестеде қатер деңгейінің матрицасы бар. Мысал ретінде кестедегі қатерді алайық (1 Кесте) :

1 Кесте - Қатер мысалы

Қатер коды	Қатерлер	Осалдықтар	Активтер	маңыздылығы [b]	Эксперттер саны
101	Басқа біреудің пайдаланушы идентификаторын тағайындау	Түпнұсқаландыру механизмдері жоқ, жеңіл құпия сөздерді пайдалануды анықтау	Жеке мәліметтер	3	m=5 m=8

Қатер жүзеге асқан сәтте мүмкін болған Тәуекелдерді және шығындарды есептеу алгоритмі:

[Қатердің жүзеге асу мүмкіндігі]= [V] = $= [\frac{N(A)}{N}]$ (1)

$$[V] = = [\frac{N(A)}{N}] = \frac{7}{25} = 0.28$$

Сапалық бағалау әдісі бойынша: *қалыпты*

Мұнда : N –қауіп-қатермен жасалған жалпы залал;

$N(A)$.– ΔT уақыт кезінде қауіптер санының кездейсоқ мәні;

[Шығын дәрежесін бағалау] =

Шығын дәрежесін шкала бойынша $=\frac{b}{m}$, (2)

Мұнда : b – активтер маңыздылығы;

m – эксперттер саны.

m = 5

Шығын дәрежесін шкала бойынша = $\frac{b}{m} = \frac{3}{5} = 0.6$

Сапалық бағалау әдісі бойынша: *критикалық*

Бұл шкала бойынша Эксперттердің тағайындаған шығындардың максимум бағасы, сандық бағалау әдісі бойынша : S = 1.200 мың теңге (2 Кесте)

2 Кесте - Тәуекел деңгейін сапалық бағалау кестесі

Қатердің жүзеге асу мүмкіндігі а / Шығын дәрежесін бағалау	**Жоғары**	**Қалыпты**	**Төмен**
Критикалық	Жоғары деңгей	Орта деңгей	Төменгі деңгей
Айтарлықтай	Орта деңгей	Орта деңгей	Төменгі деңгей
Шамалы	Төменгі деңгей	Төменгі деңгей	Қолайлы деңгей

Компьтердің осалдығы нәтижесінде, қатер шабуыл жасау арқылы тәуекел тудырды. Біз пайда болған тәуекелдерді эксперттік бағалау негізінде есептеп, сандық бағалау әдісі бойынша шкалаларын сәйкестендірдік. Келесі мәселе, сандық бағалау әдісі бойынша пайда болған шығын көлемін есептеу [8]:

[ШЫҒЫН] =[R] = [Қатердің жүзеге асу мүмкіндігі] *

[Шығын дәрежесін бағалау] = [R] = [V] * [S] (3)

[R] = [V] * [S]= 0,28 * 1.200 мың теңге = 336.000 теңге (3 Кесте)

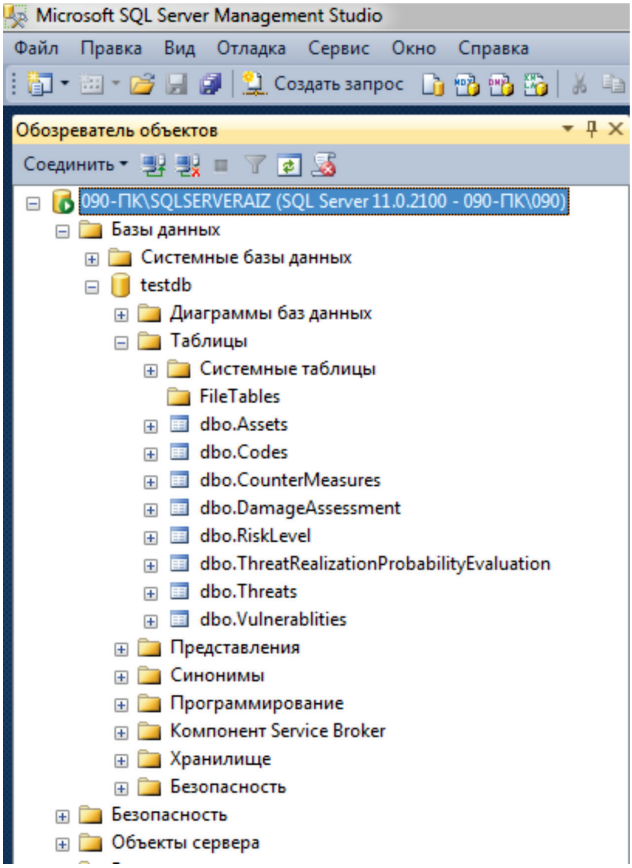
3 Кесте - Шығын есептеу мысал кестесі

№	N	N(K)	V	Қатердің жүзеге асу мүмкіндігі	Шығын дәрежесі	Актив маңыздылығы, b	Шығын дәрежесі шкала бойынша	S, мың	R, тг
1	25	7	0,28 (m=5)	қалыпты	критикалық	3	0.6	1.200	336000
2	25	7	0,28 (m=8)	қалыпты	маңызды	3	0.375	680	190400
3	64	58	0,9 (m=5)	жоғары	критикалық	3	0.6	1.200	1087500
4	48	6	0.125 (m=5)	төмен	критикалық	3	0.6	1.200	150000
5	48	6	0.125 (m=8)	төмен	маңызды	3	0.375	680	85000

Тәуекел деңгейлері қауіп-қатерлердің жіктелуіне сәйкес белгіленеді. Шығынды бағалаудың дұрыстығы тәуекел деңгейінің таразысына сәйкес тексеріледі. Тәуекел деңгейі – **Орта деңгей.** Жоғарыда көрсетілген әдіспен кәсіпорынның мүмкін болатын Тәуекелдерін есептеу компьтерлік жүйенің көмегінсіз тиімді болып табылмайды, әрі көп уақытты қажет етеді. Сол себепті, SIEM – жүйесінің *деректерді жинау жүйелігінде* сүзгіден өткен, әрі қалыптандырылған деректер *деректерді сақтау* жүйелігінде, яғни қоймада сақталады. Сол деректер қоймасы ретінде, жоғарыдағы есептерді жүзеге асыру мақсатында SQL Server 2012 программалық жүйесі таңдалып алынды. Microsoft SQL Server 2012 - бұл ең жаңа және ең қуатты деректер базасын басқару жүйесі [9]. ДҚБЖ үшін стандартты мүмкіндіктерден басқа, SQL Server 2012 деректерді талдау қызметтерінің біріктірілген жиынтығын қамтиды. Яғни, Қауіп-қатер орын алған сәтте, шабуылдар мен компьтерлік осалдықтарды талдап, тәуекелдерді бағалау және деректерді талдаудың сандық және сапалық бағаларын есептеп көрсетеді. Бұл SIEM – жүйесінің *Талдау жүйелігінің* негізгі қызметтеріне тікелей сайкес келгендігін көрсеткендіктен, Microsoft SQL Server 2012 жүйесі таңдалынды. Жүйеде жаңа дерекқор құрып, қажетте деректерді енгізу үшін Кестелер құрамыз, ол үшін кестелерінің тінтуірдің оң жағын басамыз және әр қажетті кестелер үшін тиісті параметрлердің көрсеткішін белгілейміз. Біз келесідей кестелерді жүйеде құрамыз:

Кодттар кестесі, Қатерлер кестесі, Осалдықтар кестесі, Бағалы дүниелер кестесі, Қатердің жүзеге асу мүмкіндігі кестесі, Шығын дәрежесін бағалау кестесі, Тәуекел деңгей кестесі және Контршаралар кестесі. Соңында курсорды Id бағанына орнатып, бағдарлама құралдар тақтасындағы алтын кілтін нұқу керек. Осы-

дан кейін идентификатор өрісінің алдында алтын кілт пайда болуы керек. Бұл кілт id бағаны бастапқы кілт ретінде әрекет ететінін көрсетеді [10].



5 сурет – Дерекқордағы құрылған кестелер

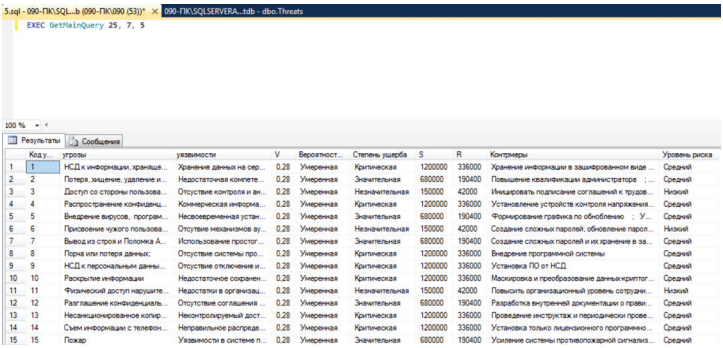
Келесі, Деректер қорында құрған кестелерімізге деректерді енгіземіз. “Қатерлер” кестесінде, 5- суреттегідей Қатерлер аты, типі, Бұзушылар және Құпиялығы, Бүтінділігі, Қолжетімділік критерийлері бойынша бағалау жасалынды. Кестелер байланысы деректерге сұраныс жасау операцияларын жүзеге асыру мақсатында жасалынды. Онымен сұраныс жасап, сақтап, жүктеп, өңдей аламыз. Сонымен қа-

тар, кез-келген серверге қосылмай, сұраулар бойынша жұмыс істей аламыз. Сұрау өңдегіші тақтасын ашу үшін, SQL Server Management Studio құралдар тақтасында Жаңа Сұрау түймешігін басамыз: Кәсіпорынның АР-на Қатерлердің жүзеге асуы мен осалдығы салдарынан мүмкін болатын Тәуекелдерді есептеу алгоритмі:

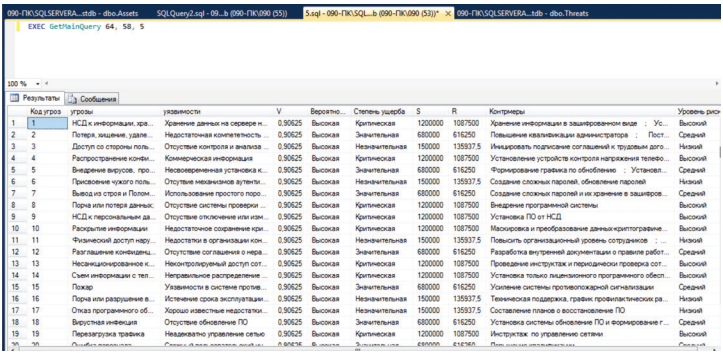
```
---------------------------------------------------------------------------
USE [testdb]
GO
SET ANSI_NULLS ON
GO
SET QUOTED_IDENTIFIER ON
GO
ALTER procedure [dbo].[GetMainQuery]
(
@TotalDamage float,
@RandomDamage float,
@NumberOfExperts float
)
as
begin
SELECT
    t.CodeId AS ‘Кодугроз’,
    t.ThreatNameRu AS ‘угрозы’,
    v.VulnerablityNameRu AS ‘уязвимости’,
    (@RandomDamage/@TotalDamage) AS ‘V’,
    (SELECT TOP 1 ThreatRealizationProbability
            FROM ThreatRealizationProbabilityEvaluation WHERE
QualityOnScaleFrom <= (@RandomDamage/@TotalDamage)
            AND QualityOnScaleTo >= (@RandomDamage/@
TotalDamage) ) AS ‘Вероятность реализации Угроз’,
    (SELECT TOP 1 DegreeOfDamage FROM DamageAssessment
WHERE QualityOnScaleFrom <=
            ((SELECT TOP 1 Significance FROM Assets WHERE
CodeId = t.CodeId)/@NumberOfExperts)
            AND QualityOnScaleTo >= ((SELECT TOP 1 Significance
FROM Assets WHERE CodeId = t.CodeId)/@NumberOfExperts)) AS
‘Степеньущерба’,
    (SELECT TOP 1 ExpertAssessment FROM DamageAssessment
```

```
WHERE QualityOnScaleFrom <=
        ((SELECT TOP 1 Significance FROM Assets WHERE
CodeId = t.CodeId)/@NumberOfExperts)
        AND QualityOnScaleTo >= ((SELECT TOP 1 Significance
FROM Assets WHERE CodeId = t.CodeId)/@NumberOfExperts)) AS 'S',
    ((@RandomDamage/@TotalDamage) * (SELECT TOP 1
ExpertAssessment FROM DamageAssessment
        WHERE QualityOnScaleFrom <= ((SELECT TOP
1 Significance FROM Assets WHERE CodeId = t.CodeId)/@
NumberOfExperts)
        AND QualityOnScaleTo >= ((SELECT TOP 1 Significance
FROM Assets WHERE CodeId = t.CodeId)/@NumberOfExperts))) AS 'R',
    (SELECT TOP 1 CounterMeasure FROM CounterMeasures
WHERE CodeId = t.CodeId) AS 'Контрмеры',
    (SELECT TOP 1 RiskLevelRu FROM RiskLevel WHERE
        RiskLevelFrom <= ((@RandomDamage/@TotalDamage)
* (SELECT TOP 1 ExpertAssessment FROM DamageAssessment
        WHERE QualityOnScaleFrom <= ((SELECT TOP
1 Significance FROM Assets WHERE CodeId = t.CodeId)/@
NumberOfExperts)
        AND QualityOnScaleTo >= ((SELECT TOP 1 Significance
FROM Assets WHERE CodeId = t.CodeId)/@NumberOfExperts)))
        AND RiskLevelTo >= ((@RandomDamage/@
TotalDamage) * (SELECT TOP 1 ExpertAssessment FROM
DamageAssessment
        WHERE QualityOnScaleFrom <= ((SELECT TOP
1 Significance FROM Assets WHERE CodeId = t.CodeId)/@
NumberOfExperts)
        AND QualityOnScaleTo >= ((SELECT TOP 1 Significance
FROM Assets WHERE CodeId = t.CodeId)/@NumberOfExperts)))) AS
'Уровеньриска'
    FROM Threats t
    INNER JOIN Vulnerablities v ON t.CodeId = v.CodeId;
    end
    ---------------------------------------------------------------------------
```

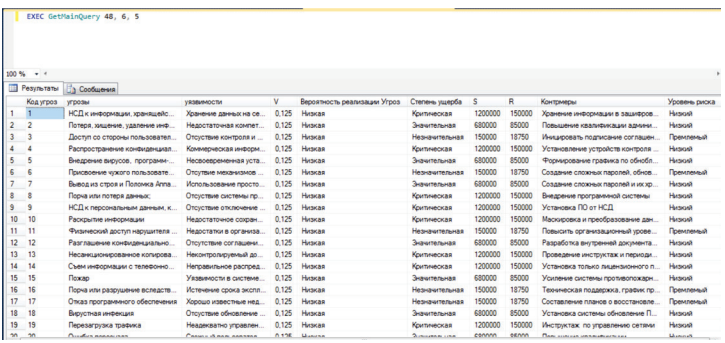
Процедураны Sql Server Management Studio ортасында барлық қатерлер үшін, Тәуекелдердің бағалауын есептеп, нәтижесін төменде әрбір қатер үшін 6-8 суреттерден көре аласыздар:



6 сурет - Қатерлердің жүзеге асуы қалыпты деңгейде тәуекелдерді эксперттік бағалау сұранысының нәтижесі



7 сурет - Қатерлердің жүзеге асуы жоғары деңгейде тәуекелдерді эксперттік бағалау сұранысының нәтижесі



8 сурет - Қатерлердің жүзеге асуы төмен деңгейде тәуекелдерді эксперттік бағалау сұранысының нәтижесі

Қауіпсіздікті бақылау топтары. Ақпараттың құпиялылығын қамтамасыз ету үшін оны электронды түрде беру кезінде шифрлаудың әртүрлі түрлері пайдаланылады. Шифрлау жіберілген ақпараттың шынайылығын растауға, оны ашық медиада сақтау кезінде қорғауға, компанияның бағдарламалық жасақтамасын және басқа ақпараттық ресурстарын рұқсатсыз көшіруден және пайдаланудан қорғауға мүмкіндік береді. Соның ішінде ақпаратты сақтаудың тиімді әдістердің бірін ұсынғым келеді, яғни ақпараттарды (деректерді) шифрлауда - Триплет түрде шифрлау әдісін ұсынамын. Триплет дегеніміз [11] - ақпаратты сақтаудың ең минималды өлшемі болып табылады. Триплет түсінігі «субъект - предикат - объект» түріндегі қарапайым логикалық пікір ретінде түсіндіріледі.Түсінікті болу үшін келесі мысалды келтіріп көрейік: «компьютер Windows7 ОЖ-сі бар». Мұнда субъект - бұл «компьютер», предикат – бұл «ОЖ-сі бар», объект – бұл «Windows 7». Яғни, «субъект – предикат – объект» түріндегі қарапайым ресурс жөніндегі пікір триплет деп аталады. Қарапайым сөйлем түрінде берілген пікірді жүзеге асырамыз.

Триплеттер W3C (World Wide Web Consortium) консорциум ұсынған Resource Description Framework (RDF) [12] деректерді көрсету модели құрылым негізінде, машиналық өңдеуге жарайтын әркелкі ресурстар туралы пікір жазуды көрсету үшін арналған ақпарат сақтаудың ең минималды өлшемі. RDF бұл деректерді көрсету үшін арналған Бүкілəлемдік жүйе консорциумы негізінде құрылған модель болып табылады. RDF ресурсы болып кез-келген болмыс бола алады – ақпараттық та (мысалы, веб-парақша не бейне) және ақпараттық емес те(мысалы, адам не қала). RDF – деректерді өңдеу үшін түрлі программалық сұраныс тілдер қолданылады.Соның ішінде, W3C ұсынған тиімді сұраныс тілі *SPARQL Protocol* and RDF Query Language (SPARQL) [13] болып табылды. Көптеген RDF – пікірлер бағытталған граф құрады, ондығы төбесі - субъект және объект, ал бүйірі предикаттармен айқындалған.

Мысалы:URIs:<http://example.com/resource> or prefix:name

Triple:prefix:subject other_prefix:predicate «object».

Шаблонды триплеттер түрінде жазамыз, мысалы Aizat есімді адамды іздеу туралы сұраныс жасайық:

```
---------------------------------------
select? x
where {? x: типі: адам.
? x: аты «Aizat»
}
---------------------------------------
```

Мұнда, «select» блогы сұраныс нәтижесін енгізетін айнымалылар тізімінен тұрады.

«?x» — табылған объект үшін іздестіру кезінде URI сілтемесін иеленетін айнымалы. «where» блогы сұраныс шаблонын құрайтын триплеттер жинағынан тұрады. Іздеу нәтижесінде шаблонды қанағаттандыратындай, 9 – суретте сызба жасалады.

9-сурет– Триплет сызбасы

? x: типі: адам

Триплеттермен жұмысқа бағытталған сақтау жүйесі «триплеттер қоймасы» (triplestores) деп аталды. Триплеттер қоймасы қазіргі таңда деректер қоймасы аумағында жаңа әрі қарқынды дамып келе жатқан бағыт болып табылады. Триплеттер қоймалардың функционалды мүмкіндіктеріне салыстырма анализ жүргізіп, бағалау жұмыстарын жасадық. Бағалау бойынша, Virtuoso өндірімділігі сұраныс орындау барысында RDF– деректерді таңдау көлемі басқаларына қарағанда 100М триплетке жоғары болып шықты,яғни 1,5–2,5 есе көп (7352 сұраныс/сағ). Сол себепті,өзінің өндірімділігі бойынша Virtuoso жүйесі жеткілікті түрде оңтайлы болып табылады. Virtuoso жуйесі OpenLink компаниясы өнімдерінің ақысыз нұсқасы екенің ескере отырып, перспективалық SIEM– жүйелері үшін деректерді сақтауда ең тиімді таңдау болып шешілді [14]. Осылайша, ақпаратты қорғау жүйесі мен деректерді сақтау қоймасын құруда жаңа әдіс қолдану, соңымен қоса ақпараттық қауіпсіздікті қамтамасыз ететін ескерту мен шешім шығаратын жедел басқаруды жүзеге асыру мен деректердің сараптама сапасы мен өңдеу жылдамдығына әсер ететін, жалпы жұмыстың тиімділігін айтарлықтай жоғарлататын деректерді көрсету мен сақтау үшін ең мықты, бәсекеге сай SIEM – жүйелерін қолдануды ұсынамыз. Қолданушылар үшін триплет түрінде көрсетілген деректерді сақтау жолдары мен өңдеудің жаңа әдістерімен таңыстырып, деректерді басқару мен программалық әлсіздікті шығару және компьютерлік шабуылдардан қорғайтын жуйені қамтамасыз етуді жүзеге асыру қажет.

Қорытынды. Жұмысты орындау нәтижесі бойынша кәсіпорынның компьютерлік жүйедегі ақпараттық ресурстарға шабуылдаған қатерлердің жүзеге асу мүмкіндігі орын алғанда пайда болған тәуе-

кел деңгейін эксперттік әдіс бойынша бағалау және шығының есептеу базасы SQL Server 2012 жүйесінде құрылып, SIEM-жүйесінің жүйелік қосымшаларына сай келетіндей программалық орталарда есептеу нәтижелері көрсетілді. Сондай-ақ, тәуекелдердің жүзеге асу деңгейін, шығындарды алдын-алу мақсатында, ақпараттық ресурстарды сақтаудың ең минималды, тиімді әдісі ретінде –триплеттерге бағытталған деректер сызбасы ұсынылды, триплеттер қоймасына арналған саралау жұмыстары жүргізілді, олардың мүмкіндіктері мен архитектурасы қарастырылды, соңымен қоса перспективалық SIEM – жүйесі үшін ең қолайлы деректерді сақтау қоймасы таңдалынды.

SIEM-жүйесінің жүйелік қосымшаларының қызметі негізінде жүргізілген есептеулердегі ақпараттық ресурстардыдың қатерлері мен осалдықтары анықталып, өңделді. Ақпараттық ресурстардыдың қатерлері мен осалдықтарын саралау, бір түрге жинақтауды визуалды турде бейнелеп көрсеттік. Жиналып, өңделген және саралау жұмыстары жүргізілген қатерлер SQL Server 2012 жүйесінде сақталып, жоғарыда аталған есептердің толық кешенді алгоритмі орындалып, нәтижесі алынды. Тәуекелдеді бағалау негізінен статистикалық деректерге негізделеді: кәсіпорынның ақпараттық жүйесінде немесе SIEM - жүйесінің деректер қоймасындағы ақпараттық ресурстарға қатысты бұзушылықтардың шабуылы мен пайдаланушылардың қателіктерінен туындаған шығынды бағалау үшін жазылады, жинақталады, талданып, сақталады және шығынды төмендету шаралары таңдалынады. Атап айтқанда, қолайсыз оқиғалардың туындау мүмкіндігінде объективті ықтималдылықты бағалау, кәсіпорын ақпараттық жүйелеріндегі ақпараттық ресурстардың қауіпсіздігінің бұзылуынан келтірілген зиянның объективті құнын бағалау және зиянды болжау туралы бағалауды алуға мүмкіндік беретін әдіснамалар ұсынылды.

Әдебиеттер

1 *Котенко И.В., Степашкин М.В.* Метрики безопасности для оценки уровня защищенности компьютерных сетей на основе построения графов атак // Защита информации. Инсайд, - 2009.- № 3. - С.36–45. [Kotenko I.V., Stepashkin M.V. Metriki bezopasnosti dlya otsenki urovnya zashhishhennosti komp'yuternykh setej na osnove postroeniya grafov atak // Zashhita informatsii. Insajd, - 2009.- № 3. - S.36–45.]

2 *A. Fedotov. A. Muhanova.* Vulnerability Classification of Information Security in Corporate Systems. International Journal of INFORMATION (Indexed by Scopus, JDream, Mathematical Reviews, Zentralblatt MATH, ProQuest, Swets, EBSCO). – 2014. - Vol.17, No.1.- pp.219-228.

3 *Дойникова Е.В., Котенко И.В.* Расширение методики оценки информационныхрисков за счет использования графов зависимостей сервисов // Санкт-Петербург. Издательство Политехнического университета. - 2011. - С.71-72 [Dojnikova E.V., Kotenko I.V. Rasshirenie metodiki otsenki informatsionnykhriskov za schet ispol'zovaniya grafov zavisimostej servisov // Sankt-Peterburg. Izdatel'stvo Politekhnicheskogo universiteta. - 2011. - C.71-72]

4 *Федотов. А.М., Ревнивых А.В.А.А. Муханова.* Классификация угроз и уязвимостей информационной безопасности в корпоративных системах.Вестник. Серия информационных технологий.– Новосибирск: НГУ, - 2013. - Т.11. В. 2. – С.55-72. [Fedotov. A.M., Revnivykh A.V.A.A. Mukhanova. Klassifikatsiya ugroz i uyazvimostej informatsionnoj bezopasnosti v korporativnykh sistemakh. Vestnik. Seriya informatsionnykh tekhnologij.– Novosibirsk: NGU, - 2013. - T.11 V. 2. – S.55-72.]

5 *Киреенко А. Е.* Современные проблемы в области информационной безопасности: классические угрозы, методы и средства их предотвращения // Молодой ученый. – 2012. №3. – С. 215-237. [Kireenko A. E. Sovremennye problemy v oblasti informatsionnoj bezopasnosti: klassicheskie ugrozy, metody i sredstva ikh predotvrashheniya // Molodoj uchenyj. – 2012. - №3. – S. 215-237.]

6 *Котенко И.В., Воронцов В.В.,* Проактивные механизмы защиты от сетевых червей: подход, реализация и результаты экспериментов. № 1, - 2009. - С.37–42. [Kotenko I.V., Vorontsov V.V., Proaktivnye mekhanizmy zashhity ot setevykh chervej: podkhod, realizatsiya i rezul'taty ehksperimentov. № 1, - 2009. - C.37–42.]

7 *Муханова А.А., Амирбай А.А.* Расчет рисков на основе объективных оценок для уязвимостиинформации в компьютерной системе предприятия // XVII Международная научно-практическая конференция «Российская наука в современном мире».-Москва: МГУ, 2018. – С.140-142 [Mukhanova A.A., Amirbaj A.A. Raschet riskov na osnove ob»ektivnykh otsenok dlya uyazvimostiinformatsii v komp'yuternoj sisteme predpriyatiya // XVII Mezhdunarodnaya nauchno-prakticheskaya konferentsiya «Rossijskaya nauka v sovremennom mire».-Moskva: MGU, 2018. – S.140-142]

8 *Miller D.R., Harris Sh., Harper A.A., VanDyke S., Black Ch.* Security Information and Event Management (SIEM) Implementation. McGraw–Hill Companies. 2011. - 430 p.

9 *Деревянко А.В.* Построение эмпирических моделей для управления сложными технологическими процессами. 2009. – Вып.12, № 863. – С. 101-110. [Derevyanko A.V. Postroenie ehmpiricheskikh modelej dlya upravleniya slozhnymi tekhnologicheskimi protsessami. 2009. – Vyp.12, № 863. – S. 101-110.]

10 *Чечулин А.А., Котенко И.В.* Анализ происходящих в реальной сети событий наоснове использования системы моделирования сетевых атак // VII Санкт-Петербургская межрегиональная конференция «Информационная безопасность регионов России (ИБРР–2011). 26–28 октября 2011 г. - С.97–98. [CHechulin A.A., Kotenko I.V. Analiz proiskhodyashhikh v real'noj seti sobytij naosnove ispol'zovaniya sistemy modelirovaniya setevykh atak //

VII Sankt-Peterburgskaya mezhregional'naya konferentsiya «Informatsionnaya bezopasnost' regionov Rossii (IBRR–2011). 26–28 oktyabrya 2011 g. - S.97–98.]

11 *Абденов А.Ж., Абденова Г.А., Амирбай А.А., Кулбаев Д.Р.* Маркетинговые информационные услуги в SIEM-системах // Вестник ЕНУ. Серия естественно-технических наук. - Астана: ЕНУ, 2017. -№4(119). – С.24-35. [Abdenov A.ZH., Abdenova G.A., Amirbaj A.A., Kulbaev D.R. Marketingovye informatsionnye uslugi v SIEM-sistemakh // Vestnik ENU. Seriya estestvenno-tekhnicheskikh nauk. - Astana: ENU, 2017. -№4(119). – S.24-35.]

12 *Дойникова Е.В., Чечулин А.А., Котенко И.В., Котенко Д.И.* Расширение методикиоценки информационных рисков для учета атак нулевого дня . 2011. - С.52-60. [Dojnikova E.V., CHechulin A.A., Kotenko I.V., Kotenko D.I. Rasshirenie metodikiotsenki informatsionnykh riskov dlya ucheta atak nulevogo dnya . 2011. - S.52-60.]

13 *Котенко И.В., Коновалов А.М., Шоров А.В.* Агентно-ориентированное моделирование бот-сетей и механизмов защиты от них // Вопросы защиты информации, - № 3, - 2011. - С.24–29. [Kotenko I.V., Konovalov A.M., SHorov A.V. Agentno-orientirovannoe modelirovanie bot-setej i mekhanizmov zashhity ot nikh // Voprosy zashhity informatsii, - № 3, - 2011. - S.24–29]

14 *Цирлов В.Л.* Основы информационной безопасности автоматизированных систем: краткий курс. - М.: Феникс, 2008. – 304 с. [TSirlov V.L. Osnovy informatsionnoj bezopasnosti avtomatizirovannykh sistem: kratkij kurs. - M.: Feniks, 2008. – 304 s]

Муханова А.А. - и.о. доцента, e-mail: ayagoz198302@mail.ru.
Амирбай А.А. - магистрант, e-mail: a_i_z_a_t_@mail.ru