МРНТИ 50.41.17 https://doi.org/10.58805/kazutb.v.1.22-281

ДИНАМИКАЛЫҚ БАЙЕС ЖЕЛІЛЕРІН ҚОЛДАНА ОТЫРЫП ЫҚТИМАЛДЫҚ МОДЕЛЬДІ ЗЕРТТЕУ

Г.З. Зиятбекова[1*], Р.Е. Сағдатова[1], Д.К. Даркенбаев[1], А.Д. Майлыбаева[2], Д.С. Абдукадыров[3], Н.Ж. Бейсенбаев[1]

[1]әл-Фараби атындағы Қазақ ұлттық университеті, Алматы, Қазақстан,

[2]Халел Досмұхамедов атындағы Атырау университеті, Атырау, Қазақстан,

[3]«Тұран» университеті, Алматы, Қазақстан,

e-mail: ziyatbekova@mail.ru

Бұл зерттеуде басып кіруді анықтау жүйелерінің мүмкіндіктерін жақсарту үшін динамикалық Байес желілері негізінде құрылған әртүрлі ықтималдық модельдер қарастырылады. Желіге рұқсатсыз енуді көрсететін ықтималдық модель үлгілеріне баса назар аударылады. Зерттеу желілік шабуылдардың әртүрлі санаттарын анықтау үшін динамикалық Байес желілерінің әртүрлі типтерінің өнімділігін талдауды қамтиды. Алынған нәтижелер желіге енуді анықтау жүйелерінің сенімділігін арттыра отырып, ақпараттық қауіпсіздік саласына құнды үлес бола алады.

Түйін сөздер: Байес желісі, киберқауіпсіздік, желілік қауіп, шабуыл.

ИССЛЕДОВАНИЕ ВЕРОЯТНОСТНЫХ МОДЕЛЕЙ НА ОСНОВЕ ПРИМЕНЕНИЯ ДИНАМИЧЕСКИХ БАЙЕСОВСКИХ СЕТЕЙ

Г.З. Зиятбекова[1*], Р.Е.Сагдатова[1], Д.К. Даркенбаев[1], А.Д. Майлыбаева[2], Д.С. Абдукадыров[3], Н.Ж. Бейсенбаев[1]

[1]Казахский национальный университет имени аль-Фараби, Алматы, Казахстан,

[2]Атырауский университет имени Х. Досмухамедова, Атырау, Казахстан,

[3]Университет ”Туран”, Алматы, Казахстан,

e-mail: ziyatbekova@mail.ru

В рамках данного исследования рассматриваются различные вероятностные модели, базирующиеся на динамических байесовских сетях с целью улучшения способности систем обнаружения вторжений. Акцент делается на выявлении аномальных паттернов, которые могут свидетельствовать о возможных сетевых вторжениях. Исследование включает в себя анализ эффективности различных типов динамических байесовских сетей в контексте обнаружения различных категорий сетевых атак. Полученные результаты могут быть ценным вкладом в область обеспечения информационной безопасности, повышая надежность систем обнаружения сетевых вторжений.

Ключевые слова: Байесовская сеть, кибербезопасность, сетевая угроза, атака.

STUDY OF PROBABILISTIC MODELS BASED ON THE APPLICATION OF DYNAMIC BAYESIAN NETWORKS

G.Z. Ziyatbekova[1*], R.Y. Sagdatova[1], D.K. Darkenbayev[1], A.D. Mailybayeva[2], D.S. Abdukadyrov[3], N.Zh. Beisenbayev[1]

[1]Al-Farabi Kazakh National University, Almaty, Kazakhstan,

[2]Khalel Dosmukhamedov Atyrau University, Atyrau, Kazakhstan,

[3]Turan University, Almaty, Kazakhstan,

e-mail: ziyatbekova@mail.ru

This study examines various probabilistic models based on dynamic Bayesian networks to improve the ability of intrusion detection systems. The emphasis is on identifying anomalous patterns that may indicate possible network intrusions. The research involves analyzing the performance of different types of dynamic Bayesian networks in the context of detecting different categories of network attacks. The results obtained can be a valuable contribution to the field of information security, increasing the reliability of network intrusion detection systems.

Keywords: Bayesian network, cybersecurity, network threat, attack.

Кіріспе. Компьютерлік жүйелер үшін қорғаныс құралдарының дамуы шабуылдаушылар тарапынан жаңа ену әдістерін қолданумен және компьютерлік жүйелердегі осалдықтарды пайдаланудың жаңа түрлерінің пайда болуымен қатар дамуда. Жыл сайын шабуылдардың жаңа түрлерін жүзеге асыратын зиянды бағдарламалардың саны артып келеді. Желілік шабуылдарды анықтау әдістерін талдау желілер мен желілік жүйелерді қорғау саласындағы оңтайлы бағыт болып табылады.

Кибершабуылдарды анықтау - шабуылды азайтудың кең таралған әдісі. Бұл желіде шабуыл үлгісінің немесе бұзылымның болуы туралы хабарлау үшін аномальді қосылымға жауап беруді қамтиды. Кибершабуылдарды анықтаудың негізгі тәсілдерінің бірі интрузияны анықтау екені белгілі. Желі қорғанысына икемді болатын, яғни адаптивті интрузияны анықтау дегеніміз оның қолтаңбасын анықтау процесі немесе қосылымдардың үздіксіз ағынындағы шабуылдарды анықтаумен бірдей [1].

Ақпараттық қауіпсіздік инциденттерін анықтаудың ықтималды әдісі - Байес желісін құру. Байес желілері белгісіздік пен күрделілік мәселелерін шешу үшін ықтималдықтар теориясы мен графиктер теориясының салаларын біріктіретін машиналық оқытудың барлық түрлерінің маңызды бөлігін құрайды. Динамикалық Байес желілері желіге рұқсатсыз енуді анықтау саласында желілік трафиктің динамикасын есепке алуға және өзгеретін қауіптерге бейімделуге мүмкіндік беретін желі түрі болып табылады. Олар бір уақыттағы ықтималдықтардың таралуын ықшам түрде көрсетуге мүмкіндік беретін графикалық ықтималдық модельдердің бірі бақыланатын оқиғалардың пайда болуын қамтиды [2].

Байес желілерінің артықшылығы олардың адамдар үшін салыстырмалы интуитивтілігі, өйткені бір уақытта бірнеше оқиғалардың пайда болуының нәтижесінде орын алатын ықтималдық үлестіріміне қарағанда оқиғалар мен жергілікті ықтималдық үлестірімдері арасындағы тікелей байланыстарды түсіну оңайырақ болып табылады.

Материалдар мен әдістер. Динамикалық Байес желілеріне негізделген (DBN) желі енуін анықтау үшін құрылған ықтималдық модельдерін пайдалану қиынға соғады және барлық сценарийлер үшін әмбебап стандартты алгоритмдер жоқ. Дегенмен, зерттеушілер мен инженерлер желіге енуді анықтау үшін DBN қолданатын әртүрлі әдістер мен модельдерді әзірлеуде.

Динамикалық Байес желілерін пайдалана отырып рұқсатсыз енуді анықтау алгоритмдерінің мысалдарына тоқталайық.

1) Аномалияларды анықтауға арналған динамикалық Байес желілері:

- қалыпты жүйе әрекетін модельдеу үшін DBN пайдаланады;
- аномалиялар ағымдағы жағдайды күтілетін жағдаймен салыстыру арқылы анықталады.

2) Желі қауіпсіздігі үшін арнайы DBN үлгілері:

- желілік белсенділіктің сипаттамаларын және ену түрлерін ескеретін нақты DBN үлгілерін жасау;
- белгілі желілік қауіпсіздік сценарийлеріне үлгілерді бейімдеу.

3) Басқа машиналық оқыту әдістерімен интеграция:

- интрузияны анықтау дәлдігін жақсарту үшін DBN-ді кластерлеу немесе жіктеу әдістері сияқты машиналық оқытудың басқа алгоритмдерімен біріктіру.

4) Уақыт қатарларын пайдалану:

- желі әрекетіндегі уақыт қатарын талдау үшін DBN көмегімен оқиғалар арасындағы уақытқа тәуелділікті есепке алу.

5) Байес сүзгілері:

- желінің құрылымын өзгерту негізінде адаптивті интрузияны анықтау үшін Байес сүзгілерін қолдану.

6) Үлкен деректермен жұмыс:

- үлкен көлемдегі мәліметтерді тиімді өңдей алатын және желілік белсенділіктің динамикасына бейімделетін алгоритмдерді әзірлеу.

7) Мамандандырылған DBN архитектуралары:

- өзгермелі модельдер сияқты енуді анықтау үшін оңтайландырылған DBN архитектурасын зерттеу

және әзірлеу.

Алгоритмді таңдау және бейімдеу желінің нақты талаптары мен сипаттамаларына, сондай-ақ, анықтағыңыз келетін ену түрлеріне байланысты екенін ескеру маңызды. DBN көмегімен басып кіруді анықтау жүйесін әзірлеу кезінде нақты жағдайыңыз үшін, ең жақсы тәсілді анықтау үшін ауқымды зерттеулер мен сынақтарды жүргізу ұсынылады [3].

Нәтижелер және талқылау. Байес желілері - бірнеше айнымалылар мен осы айнымалылардың арасындағы Байес ықтималдық тәуелділіктерін қамтитын графикалық ықтималдық моделі (кейде графикалық ықтималдық үлгісі деп те аталады). Бұл желі ықтималдықты болжау және тәуекелді бағалау мәселелерін шешу үшін пайдаланылатын тиімді математикалық қуатты құрал [4].

Байес желісін құру формуласы:

$$P(A \vee B) = \frac{P(B|A) \cdot P(A)}{P(B)} \qquad (1)$$

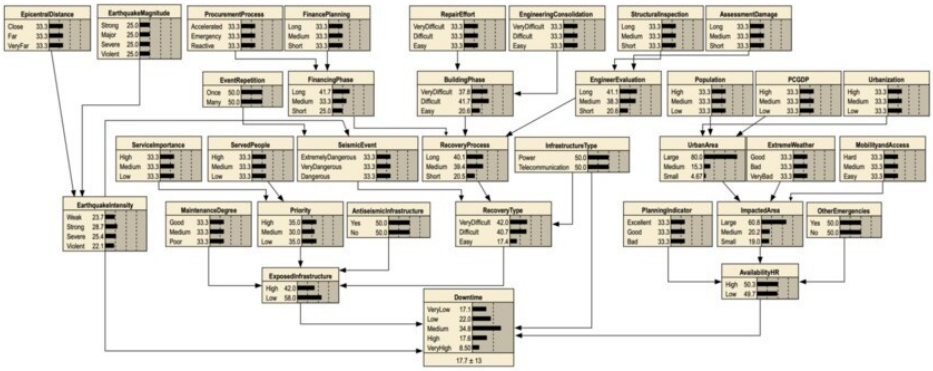
мұнда $P(A \vee B) -$ оқиғасы болған жағдайда А оқиғасының болу ықтималдығы, $P(B|A)$ —А оқиғасы болған жағдайда В оқиғасының болу ықтималдығы, ал $P(A)$ және $P(B)$- сәйкесінше А және В оқиғаларының ықтималдығы [5].

Бірлескен ықтималдық былай есептеледі:

$$P(X_1, X_2 \ldots, X_n) = \prod_{i=1}^{n} P(X_i|P\alpha(X_i) \qquad (2)$$

$X_1, X_2 \ldots, X_n$ - ағымдағы уақыттағы айнымалылар.

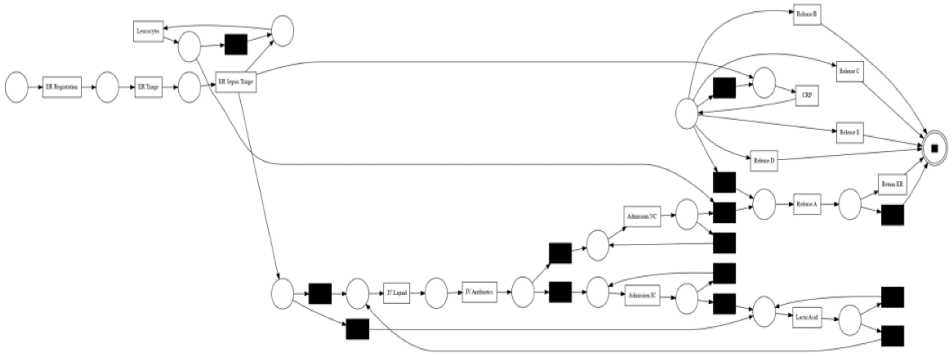
Түйіндер, қосылымдар мен (2) айнымалылар Байес желісін құрады және құрылымдық спецификация деп аталады. DBN-ды жобалау үшін Netica және Hugin редакторлары қолданылды (1-сурет).



1-сурет - Байес желісінің мысалы

Егер шыңдар айнымалылар тізбегінен құралса, онда Байес желісі динамикалық деп аталады. Динамикалық Байес желісі - уақыт бойынша айнымалылар арасындағы ықтималдық қатынастарды модельдеу үшін қолданылатын статистикалық модель [6].

Динамикалық Байес желілерін (DBN) пайдаланып желілік шабуылдарды анықтауға арналған желі құрылымы арнайы талаптарға, желі әрекетінің сипатына және анықтағыңыз келетін ену түрлеріне байланысты болады. Интрузияны анықтаудың стандартты әдістері қазіргі уақытта деректерге және модельге бағытталған тәсілдерге бөлінеді. Біріншісі сандық айырмашылықтарды талдау арқылы деректерді анықтауға бағытталған [7]. Интрузияны анықтау алгоритмін ұсыну үшін динамикалық ықтималды Байес желісіне Петри графикалық моделін (2-сурет) қосу арқылы Байес-Петри ықтималды желісін қолданамыз. Байес желісі мен Петри желісі жүйелерді сипаттау әрі талдау үшін қолданылатын екі түрлі модель екені белгілі. Олардың мақсаты мен қолданбалары әртүрлі, бірақ жүйелердегі интрузияны анықтау сияқты күрделі мәселелерді шешу үшін біріктірілуі мүмкін. Оларды пайдалану аномалияны анықтаудың жан-жақты және тиімді әдісін қамтамасыз ете алады.



2-сурет - Петри моделі

Динамикалық Байес желісі мен Петри желісі арасындағы өзара әрекеттесуді ескере отырып келесі формуланы қолданамыз [8]:

$$\Pr\left\{\begin{array}{l} Ds \int Sp(\pi)\left\{\begin{array}{l} V_a: \\ S^0,\ \ldots,\ S^0,\ O^0,\ \ldots,\ O^T \\ Dc: \\ \left\{\begin{array}{l} P(S^0 \ldots\ S^t O^0 \ldots\ O^T|\pi) \\ = P\left(S^0 O^0\right) * \prod_{t=1}^{T}\left[P\left(S^t\middle|S^{t-1}\right) * P(O^t|S^t)\right] \end{array}\right. \\ F: \end{array}\right. \\ \qquad F_0: \\ \qquad Qu\ :\left\{\begin{array}{r} P(S^{t+k}|O^0 \ldots\ O^t) \\ (k=0 \equiv Filtering) \\ (k>0 \equiv Prediction) \\ (k<0 \equiv Smoothing) \end{array}\right. : \end{array}\right.$$

Динамикалық модель және алдыңғы сәттегі күйді бағалау арқылы фазалық күйді болжауға болады:

$$\sum_{S^{t-1}}\left[P\left(S^t\middle|S^{t-1}\right) * P(S^{t-1}|O^0\ \ldots\ O^{t-1})\right]$$

Динамикалық Байес желісін Петри желісімен біріктіру екі модельдің өзара әрекеттесуін мұқият қарастыруды және жүйенің дұрыс жұмыс істеуін, сондай-ақ, оларды талдауды қамтамасыз ету үшін сәйкес интеграция әзірлеуді талап етеді [9]. Бұл үлгіні жасау үшін *pgmpy* және *PetriNet* кітапханалары бар Python сияқты Bayesian және Petri желілерімен жұмыс істеуге арналған арнайы құралдарды пайдаланамыз:

1) Динамикалық Байес желісін құру алгоритмі:

```
from pgmpy.models import DynamicBayesianNetwork as DBN
from pgmpy.factors.discrete import TabularCPD

# DBN үiілгсн жасау
dbn = DBN()

# Айнымалылар мен қоларды әiiітуелдлктерн қанытау
dbn.add_edges_from([
    ('Connection', 'DataTransfer'),
    ('DataTransfer', 'AnomalyDetection')
])
# Айнымалылар үішн ққытималды ікестелерн қанытау
cpd_connection = TabularCPD(variable='Connection', variable_card=2,
    values=[[0.8], [0.2]])
```

```
cpd_data_transfer = TabularCPD(variable='DataTransfer', variable_card=2,
                               values=[[0.9, 0.6], [0.1, 0.4]],
                               evidence=['Connection'], evidence_card=[2])
cpd_anomaly_detection = TabularCPD(variable='AnomalyDetection', variable_card=2,
                                   values=[[0.95, 0.8], [0.05, 0.2]],
                                   evidence=['DataTransfer'], evidence_card=[2])

# DBN үіілгсне құытималды ікестелерн қосу
dbn.add_cpds(cpd_connection, cpd_data_transfer, cpd_anomaly_detection)
```

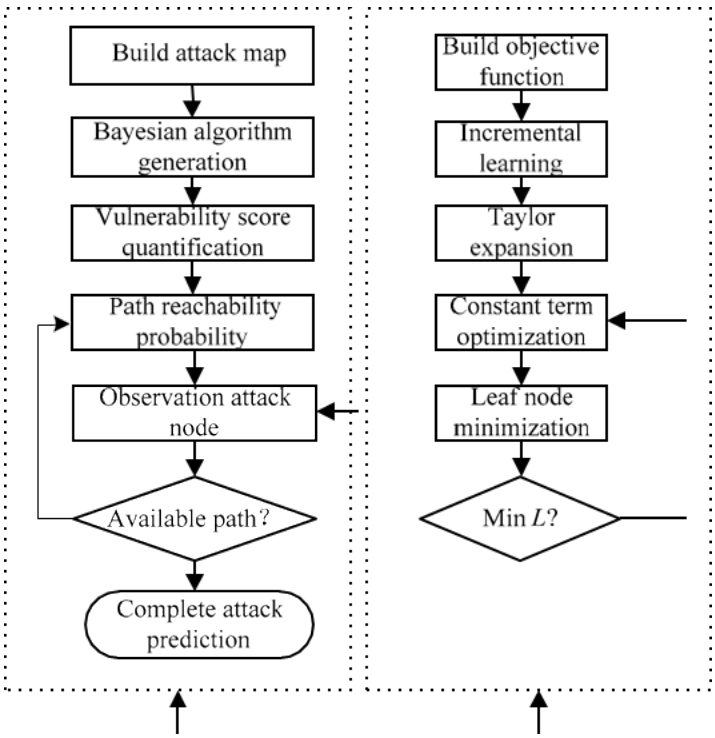
2) Петри торлы (SP) моделін құру алгоритмі:

```
from PetriNet import PetriNet
sp = PetriNet()
# Орындар мен ауысуларды қанытау
sp.add_place('NormalState')
sp.add_place('AnomalyState')
sp.add_transition('DetectAnomaly')

# Өітпел матрицаны қанытау
transition_matrix = {
    'DetectAnomaly': {'NormalState': 1, 'AnomalyState': 1}
}
sp.add_transition_matrix(transition_matrix)
```

3) Интеграция:

```
# Интеграция мысалы: SP ііішндег ауысуларды іске қосу үішн DBN ііішндег үкй
    қапаратын пайдалану
from pgmpy.inference import DBNInference

# DBN-ден айнымалы үікйлерд алу (олар құездейсо әмндер болса)
evidence = {'Connection': 1, 'DataTransfer': 1}

# DBN-ге қорытынды жасау үішн DBNInference нысанын алу
dbn_inference = DBNInference(dbn)

# үКй құытималдытарын алу үішн қорытынды жасау
query_variables = ['Connection', 'DataTransfer', 'AnomalyDetection']
result = dbn_inference.query(evidence=evidence, variables=query_variables)

# әіНтижен SP-де ауысуларды ібелсендру үішн пайдалану
if result['AnomalyDetection'][1] > 0.5:
#Егер аномалияны қанытау қытималдыы ішект әмннен ғжоары болса
sp.fire_transition('DetectAnomaly')
```

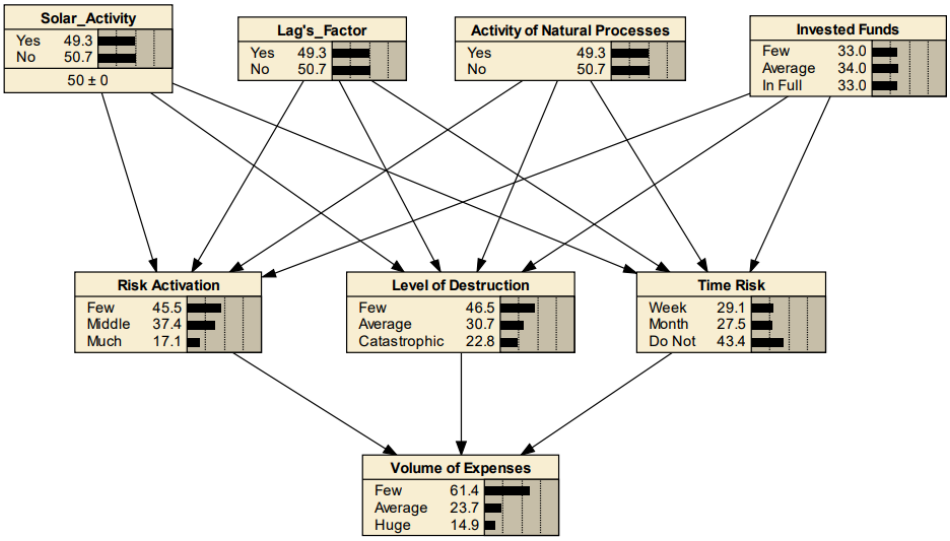
Байес-Петри моделін толық құрған соң, интрузияны анықтау диаграммасын енгіземіз (3-сурет).



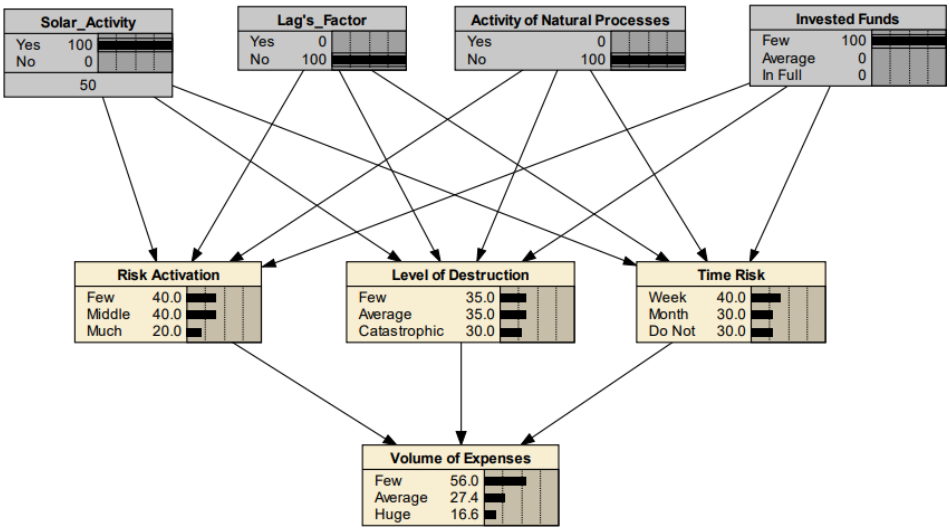
Байестік шабуыл диаграммасы Петри желісін қолдану алгоритмі

3-сурет -Интрузияны анықтау жүйесі

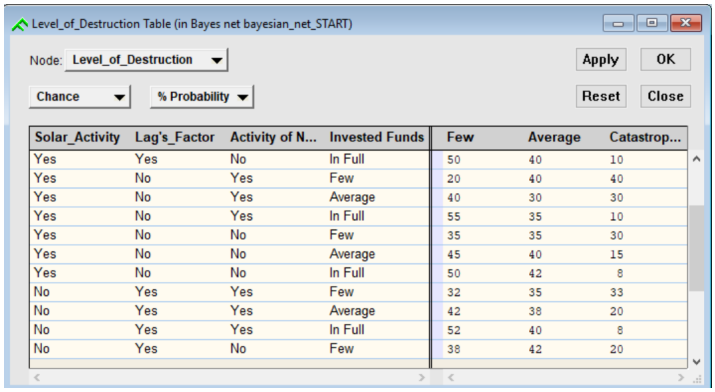
Келесі 4-6-суреттерде интрузияны анықтау мәндері Netice бағдарламасының нәтижелері жүйесі түрінде ұсынылған:



4-сурет - Модельдеу және болжау



5-сурет - Сенімді оқыту желісін әзірлеу



Solar_Activity	Lag's_Factor	Activity of N...	Invested Funds	Few	Average	Catastrop...
Yes	Yes	No	In Full	50	40	10
Yes	No	Yes	Few	20	40	40
Yes	No	Yes	Average	40	30	30
Yes	No	Yes	In Full	55	35	10
Yes	No	No	Few	35	35	30
Yes	No	No	Average	45	40	15
Yes	No	No	In Full	50	42	8
No	Yes	Yes	Few	32	35	33
No	Yes	Yes	Average	42	38	20
No	Yes	Yes	In Full	52	40	8
No	Yes	No	Few	38	42	20

6-сурет - Алғашқы өңдеу қорытындылары

Осылайша, интрузияны анықтауға арналған ықтималды динамикалық Байес негізіндегі Петри торлы желісі интрузияларды анықтау және жүйе қауіпсіздігі саласындағы әртүрлі мәселелерге сәтті қолданылуы мүмкін оңтайлы тәсіл екені анықталды.

Қорытынды. Бұл мақалада Байес жүйелерінің сипаттамалары талданды. Динамикалық Байес желілерін қолдану негізінде желілік интрузияларды анықтауда қолданылатын ықтималдық модельдерді қолдану қажеттіліктері мен ерекшеліктері атап өтілді. Зерттеудің теориялық талдауы, әсіресе динамикалы өзгеретін желілік орталарда желіге енуді анықтау контекстінде динамикалық Байес желілерінің ықтимал артықшылықтарын ашады. Дегенмен, мәліметтерді қорытындылау тек теориялық аспектілерді талдауға негізделгенін және практикалық сынақтарды өткізу осы зерттеуді дамытудың келесі қадамы екенін атап өткен жөн.

Қорытындылай келе, теориялық зерттеуде динамикалық Байес желісі киберқауіпсіздік саласындағы рұқсатсыз енуді анықтаудың оңтайлы құралы ретінде қарастыруға мүмкіндік береді. Дегенмен, зерттеушілер мен инженерлер желіге енуді анықтау үшін DBN қолданатын әртүрлі әдістер мен модельдерді әзірлеуде. Қарастырылған модельдер киберқауіпсіздік жүйелерінде енуді анықтау және ықтимал қауіптерді азайту қабілетін көрсетеді.

Жұмыс әл-Фараби атындағы ҚазҰУ жанындағы Математика және механика ҒЗИ қаражаты және AP19678157 жобасы бойынша 2023-2025 жылдарға арналған ғылыми зерттеулерді гранттық қаржыландыру есебінен орындалды.

Литература

1.L.Buczak, E.Guven. A survey of data mining and machine learning methods for cyber security intrusion detection, IEEE Communications Surveys & Tutorials, 2016. - Vol. 18, -No. 2.- pp.1153-1176.

2.М.М.Путято,А.С.Макарян.Кибербезопасность как неотъемлемый атрибут многоуровневого защищенного киберпространства / М.М. Путято, А.С. Макарян // Прикаспийский журнал: управление и высокие технологии, 2020. -№ 3(51).- стр. 94-102.

3.H.Shapoorifard, P. Shamsinejad. A Novel Cluster-based Intrusion Detection Approach Integrating Multiple Learning Techniques. International Journal of Computer Applications, 2017.-Vol. 166.-No.3.- pp. 13-16.

4.Трухан С.В., Бидюк П.И. Применение сетей Байеса к построени. моделей оценки риска актуарные процессов. ScienceRise, 2016.-Т.8.- № 2(25).-стр.6-14. DOI: 10.15587/2313-8416.2016.74962

5.З.Гахрамани. Изучение динамических байесовских сетей. Конспект лекций по информатике, 2017.- стр.168-197. CiteSeerX 10.1.1.56.7874.doi:10.1007/ BFb0053999. ISBN 978-3-540-64341-8 .

6. Thomas Dean, Keiji Kanazawa. A model of causal reasoning and robustness. Computational Intelligence, 2019. -Vol. 5.- pp. 142-150.

7.N.Friedman, K. Murphy, S. Russell. Learning the structure of dynamic probabilistic networks. UAI'98, 2018. - pp.139-147. CiteSeerX 10.1.1.1.75.2969

8.G.Tandon, P. Chan. Learning useful system call attributes for anomaly detection. In The Florida Artificial Intelligence Research Society Conference, 2015. - pp. 405-410.

9.D.Yeung, Y. Ding. User profiling for intrusion detection using dynamic and static behavioral models. Advances in Knowledge Discovery and Data Mining, 2017.- pp. 494-505.

References

1.L.Buczak, E.Guven. A survey of data mining and machine learning methods for cyber security intrusion detection, IEEE Communications Surveys & Tutorials, 2016. - Vol. 18, -No. 2.- pp.1153-1176. [in Eng.].

2.M.M.Putjato,A.S.Makarjan.Kiberbezopasnost' kak neotemlemyj atribut mnogourovnevogo zashhishhennogo kiberprostranstva / M.M. Putjato, A.S. Makarjan // Prikaspijskij zhurnal: upravlenie i vysokie tehnologii, 2020. -№ 3(51).- str. 94-102. [in Russian].

3.H.Shapoorifard, P. Shamsinejad. A Novel Cluster-based Intrusion Detection Approach Integrating Multiple Learning Techniques. International Journal of Computer Applications, 2017.-Vol. 166.-No.3.- pp. 13-16 (.) [in Eng.].

4.Truhan S.V., Bidjuk P.I. Primenenie setej Bajesa k postroeni. modelej ocenki riska aktuarnye processov. ScienceRise, 2016.-T.8.- № 2(25).-str.6-14. DOI: 10.15587/2313-8416.2016.74962 [in Russian].

5.Z.Gahramani. Izuchenie dinamicheskih bajesovskih setej. Konspekt lekcij po informatike, 2017.- str.168-197. CiteSeerX 10.1.1.56.7874.doi:10.1007/ BFb0053999. ISBN 978-3-540-64341-8 [in Russian].

6.Thomas Dean, Keiji Kanazawa. A model of causal reasoning and robustness. Computational Intelligence, 2019. -Vol. 5.- pp. 142-150. [in Eng.].

6.Tomas Din, Kejdzhi Kanadzava. Model' rassuzhdenij o prichinno-sledstvennyh svjazjah i ustojchivosti. Computational Intelligence, 2019. -Vol. 5.- pp. 142-150. [in Eng.].

7.N.Friedman, K. Murphy, S. Russell. Learning the structure of dynamic probabilistic networks. UAI'98, 2018. - pp.139-147. CiteSeerX 10.1.1.1.75.2969. (in Eng.)

8.G.Tandon, P. Chan. Learning useful system call attributes for anomaly detection. In The Florida Artificial Intelligence Research Society Conference, 2015. - pp. 405-410. [in Eng.].

9.D.Yeung, Y. Ding. User profiling for intrusion detection using dynamic and static behavioral models. Advances in Knowledge Discovery and Data Mining, 2017.- pp. 494-505.[in Eng.].

Авторлар туралы мәліметтер

Зиятбекова Г.З. - PhD, әл-Фараби атындағы Қазақ ұлттық университетінің доцент м.а., Алматы, Қазақстан, e-mail: ziyatbekova@mail.ru;

Сағдатова Р.Е. - әл-Фараби атындағы Қазақ ұлттық университетінің магистранты, Алматы, Қазақстан, e-mail: rsagdatova@gmail.com;

Даркенбаев Д.К. - PhD, әл-Фараби атындағы Қазақ ұлттық университеті, Алматы, Қазақстан,

e-mail: dauren.kadyrovich@gmail.com;

Майлыбаева А.Д. - физика математика ғылымдарының кандидаты, Халел Досмұхамедов атындағы Атырау университеті Информатика кафедрасының қауымдастырылған профессоры, Атырау, Қазақстан, e-mail: mjkka@mail.ru;

Абдукадыров Д.С. - «Тұран» университетінің магистранты, Алматы, Қазақстан, e-mail:22231307@turan-edu.kz;

Бейсенбаев Н.Ж. - әл-Фараби атындағы Қазақ ұлттық университетінің магистранты; Алматы, Қазақстан, e-mail: beisenbayeff.nursultan@gmail.com

Information about the authors

Ziyatbekova G.Z.- PhD, Acting Associate Professor Al-Farabi Kazakh National University; e-mail: ziyatbekova@mail.ru;

Sagdatova R.E. - graduate student at Al-Farabi Kazakh National University; e-mail: rsagdatova@gmail.com;

Darkenbayev D.K.- PhD, Al-Farabi Kazakh National University, e-mail: dauren.kadyrovich@gmail.com;

Mailybayeva A.D.-Candidate of Physical and Mathematical Sciences; Associate Professor of the Department of Informatics of the Atyrau University named after Kh. Dosmukhamedov, e-mail: mjkka@mail.ru;

Abdukadyrov D.C. - graduate student at Turan University; 22231307@turan-edu.kz;

Beisenbayev N.Zh.- graduate student at Al-Farabi Kazakh National University,e-mail: beisenbayeff.nursultan@gmail.com