УДК 004.04
МРНТИ 81.93.29
https://doi.org/10.47533/2024.1606-146X.25

Н. БАЙШОЛАН*, Қ. С. БАЙШОЛАНОВА

Әл-Фараби атындағы Қазақ ұлттық университеті, Алматы, Қазақстан
*e-mail: *baisholan@gmail.com, baisholanova.k@gmail.com*

ФРОДПЕН КҮРЕСУДЕ ЖАСЫРЫН МАРКОВ МОДЕЛІН ҚОЛДАНУ

Мақалада қаржы саласындағы алаяқтықтың алдын алуда фродқа қарсы күресуде жасырын Марков моделін қолдану арқылы машиналық оқыту әдісінің тәуекелділікті төмендететіні туралы талдау ұсынылады. Себебі Бүкіләлемдік экономикалық форумның жылдық жаһандық тәуекелдер туралы есеп берулерінде киберосалдық пен киберқауіпсіздік шараларына аса назар аудару өзекті мәселелердің бірі екені қарастырлып, алдағы уақыттарда оның алдын алу, болжау қажеттігі туындады. Транзакциялық ортадағы аномалияларды анықтағанда машиналық оқыту арқылы тәуекелдерді дәл анықтау және талдау арқылы алаяқтық әрекеттердің ықтималдылығы бағаланады. Антифрод жүйесі үшін болатын тосын ауытқулардың ықтималдылығы мен жүйе күйлерінің сипаттарын Марков тізбегінің талаптарына сәйкес стохастикалық модель немесе процесс ретінде қарастыруға болады. Сондықтан ақауларды немесе біздің жағдайымызда алаяқтықты анықтауда қадамдар арасындағы уақыт тұрақты емес және жаңа күйге көшу тек соңғы күйге ғана байланысты екені ескерледі.

Машиналық оқыту арқылы фродқа қатысты әрекеттерді болжауда жасырын Марков моделін қолдана отырып, hmmlearn бағдарламалық жабдығымен қажетті деректер тізбегін модельдеуге болатыны және апостериорлық ықтималдылықты пайдаланып, болжанған тұжырымды жаңартуға да болатыны қарастырылған. Нәтижесінде қаржылық алаяқтыққа байланысты тәуекелділікті айқындап және оны азайтуда статистикалық тәсілдер мен ережелерді қолданудың тиімділігі үлкен көлемді деректерді дұрыс талдауға байланысты екені байқалады. Дегенмен, фрод үшін жасырын Марков моделін қолдануда құпия қаржылық деректерге қол жеткізудің қиындығы мен оны жүзеге асырудың күрделілігі, бастапқы күйлердің өту матрицасының айқын сипаттамалуына қойылатын жоғары талаптар секілді шараларды ескеру қажеттілігі баяндалады.

Түйін сөздер: *антифрод, фрод, ықтималдық, жасырын Марков моделі, машиналық оқыту, темпоральді мәліметтер, мәліметтер ағынын талдау.*

Н. БАЙШОЛАН*[1], К. С. БАЙШОЛАНОВА[1]

[1]КазНУ имени аль-Фараби, Алматы, Казахстан
*e-mail: *baisholan@gmail.com, baisholanova.k@gmail.com*

ПРИМЕНЕНИЕ СКРЫТОЙ МАРКОВСКОЙ МОДЕЛИ ПРОТИВ ФРОДА

В статье представлен анализ того, как метод машинного обучения снижает риск за счет использования скрытой марковской модели в борьбе с фродом в предотвращении мошенничества в финансовой сфере. Это связано с тем, что в ежегодных отчетах Всемирного экономического форума о глобальных рисках особое внимание уделялось мерам кибероуязвимости и кибербезопасности, возникла необходимость их предотвращения, прогнозирования. При обнаружении аномалий в транзакционной среде с помощью машинного обучения точно выявляются риски, а с помощью анализа оценивается вероятность мошеннических действий. Вероятности неожиданных отклонений, происходящих для антифродовой системы, и свойства состояний системы можно

рассматривать как стохастическую модель или процесс в соответствии с требованиями цепи Маркова. Поэтому при обнаружении неисправностей или в нашем случае мошенничества учитывается, что время между шагами не является постоянным, и переход в новое состояние зависит только от конечного состояния.

Предполагается, что можно смоделировать требуемую последовательность данных с помощью программного обеспечения hmmlearn, используя СММ для прогнозирования действий, связанных с фродом, с помощью машинного обучения, а также можно обновить предсказанное утверждение, используя апостериорную вероятность. В результате заметно, что эффективность применения статистических подходов и правил в выявлении и снижении риска, связанного с финансовым мошенничеством, зависит от правильного анализа больших объемов данных. Однако для фрода излагается необходимость учитывать такие меры, как сложность доступа к конфиденциальным финансовым данным и сложность их реализации при использовании скрытой Марковской модели, высокие требования к четкому описанию матрицы переходов исходных состояний.

Однако при использовании скрытой Марковской модели для выявление фрода необходимо учитывать такие меры, как сложность доступа к конфиденциальным финансовым данным и сложность алгоритма их реализации, высокие требования к четкому описанию матрицы переходов исходных состояний.

Ключевые слова: *антифрод, фрод, вероятность, скрытая марковская модель, машинное обучение, темпоральные данные, анализ потока данных.*

N. BAISHOLAN*, K. S. BAISHOLANOVA

Al-Farabi Kazakh National University, Almaty, Kazakhstan
*e-mail: *baisholan@gmail.com, baisholanova.k@gmail.com*

APPLICATION OF THE HIDDEN MARKOV MODEL AGAINST FRAUD

The article analyzes a machine learning method that reduces risk by using a hidden Markov model with a view to prevent fraud in the financial sphere. It is related to the fact that in the annual reports of the World Economic Forum on global risks, special attention was given to measures of cyber vulnerability and cybersecurity, for which cause the need to prevent and predict them became necessary. When anomalies are detected in a transactional environment, using machine learning method, the risks are accurately identified, and the probability of fraudulent acts is assessed using analysis. The probabilities of unexpected deviations occurring for an antifraud system and the properties of the states of the system can be considered as a stochastic model or process in accordance with requirements of Markov chain. Therefore, if a fault or, in this case, fraud is detected, the time between steps is considered constant, and the transition to a new state depends only on the final state.

It is supposed that it is possible to simulate the required sequence of data in hmmlearn software, using CMM to predict fraud-related actions using machine learning, and it is also possible to update the predicted statement using a posteriori probability. As a result, it is noticeable that the effectiveness of application of statistical approaches and rules in identifying and reducing the risk associated with financial fraud depends on the correct analysis of large amounts of data. Moreover, for fraud, it is necessary to take into account such measures as the complexity of access to confidential financial data and the complexity of their implementation when using a hidden Markov model, high requirements for a clear description of transition matrix of initial states.

Key words: *anti-fraud, fraud, probability, hidden Markov model, machine learning, temporal data, data flow analysis.*

Кіріспе. Электрондық ортадағы жиі ақпараттық шабуылдарға ұшырап жататын маңызды салалардың бірі – қаржы саласындағы объектілер мен ондағы транзакциялық әрекеттер. Бүкіләлемдік экономикалық форумда жыл сайын қарастырылатын жаһандық тәуекелдер туралы есеп берулерде де киберосалдық пен киберқауіпсіздік шараларына аса назар аударылып, бұл туралы өзекті деректер келтіріліп отырады.

Жалпы қаржылық жүйеге жасалатын шабуылдар мен қатерлердің салдары біршама ақшалай шығындарға ұшыратыны белгілі. Мысалы, банк жүйесіне жасалатын ақпараттық қауіп-қатерлер әлемдегі ақпараттық шабуылдардың 17 пайызын құраса, онлайн-банкинг бойынша алаяқтық әрекеттер 2021 жылы 11,7 пайызды, Visa төлем жүйесі бойынша 9,4 пайызды және PayPal жүйесінде 37,8 пайызды құраған. Осылайша, сол жылдың өзінде қолданушылардың 8,2 пайызы фишингтік шабылудан зардап шеккен. Бұл әрекеттер көбінесе қатерлі бағдарламалық жабдықтар арқылы жасалуда. Оған 2021 жылы 12,2 пайыздық көрсеткішпен сегізінші орыннан екінші орынға көтерілген банктік троян SpyEye бағдарламасы (12,2 пайыз), CliptoShuffer (10,2 пайыз) немесе Zbot (20,5 пайыз) Emotet ботнетінің белсенділігі мысал бола алады [1].

Әлемдегі географиялық аймақтар бойынша төлем жүйелеріне жасалатын компьютер арқылы шабуылдардан зардап шегушілер қатарында Ауғанстан, Түрікменстан және Тәжікстан азаматтары болса, ал мобильді құрылғылар бойынша Турция, Испания және Япония азаматтары болған. Касперский зертханасының есебі бойынша жалпы фишинг инциденттердің 11,1 пайызын құрайтыны анықталды. Төлем жүйелерінің ішінде әсіресе банктік карталардың қауіпсіздігін қорғау өзекті шара. Оның қаншалықты қорғау мехнизмдерімен жабдықталғандығына қарамастан, алаяқтық қатерлерден тәуелді болып қала береді. Бұл фактілердің барлығы банк жүйесіндегі кибератакаларға үлкен мән беру керектігін білдіреді. Сондықтан, ақша нарығын реттеуде IOSCO халықаралық қаржылық ұйымы банк саласындағы ақпараттық қауіпсіздікті күшейту мақсатында ондағы ақпараттық жүйелердің сенімді болуын міндеттеді. Ұйым биылғы жылы өзінің кезекті жұмыс бағдарламасында маңызды сұрақтар бойынша «Қаржылық тұрақтылықты күшейту - Strengthening Financial Resilience» және «Тұрақтылық пен финтектегі жаңа тәуекелдерді шешу - Addressing New Risks in Sustainability and Fintech» атты мәселелерді қойды [2] .

Банк жүйесінде жиі кездесетін ақпараттық шабуылдарға фишинг, DDoS-атакалар, жүйені қасақана бұзу, жеке мәліметтер мен қаржылық құжаттарға қол жеткізу қауіпін айтуға болады. Осылардың алдын алу үшін банк жүйесі фрод-модульдерді ендіруде. Мысалы, Халық банк 2022 жылдың наурызынан Анитфрод жүйесін ендіріп, қаржылық алаяқтықты 90 пайызға төмендеткен [3]. Ендірліген жүйеде клиенттердің мінез-құлық портретін жасап, және алаяқтардың да мінез-құлқтарын ескеретін ереже қалыптастырылған. Сол арқылы күдікті клиенттерді айқындау мүмкіндігіне қол жеткізілген. Оған көбінесе:

– алаяқтық жарнамалар арқылы сенген клиенттердің банктік шоттарына қол жеткізіп, олардың атынан қаржылық операциялар жасау;

– банк қызметкері ретінде қоңырау шалу – клиентті сендіре отырып, жеке деректерден басқа, алаяқтардың шотына ақша аударту әрекеттерін жасату;

– құрылғыға алыстан қол жеткізу бағдарламасы арқылы алаяқтық жасау кезінде клиенттің телефонына немесе компьютеріне орнатылған жалған «клиентті қолдау қосымшалары» көмегімен банк шотына қол жеткізулері кездеседі. Оған TeamViewer немесе AnyDesk бағдарламалары себепші болып жатады.

Осындай әрекеттерге жол бермеу үшін фродпен күресіп, антифрод жүйесін ендіру өзекті. Антифрод жүйесі нормативтік-құқықтық актілер аясында төлем арналарындағы алаяқтықты анықтаудан бастап, күмәнді алаяқтың аккаунттарға тосқауыл қоюға, фрод-талдаушылар арқылы қауіптің жаңа түрлерін талдауға, RBA технологиясы арқылы легитимді қолданушылардың авторизацияларын жеңілдетеді.

Банк жүйесіндегі қызметке қатысты транзакциялық алаяқтықты айқындау үшін машиналық оқыту әдісітері немесе сараптама жүйесімен статистикалық деректерді талдау әдістері қолданылады. Осы әдістердің көмегімен ішкі және сыртқы фродтармен, фишингпен күресіп**,** тәуекелдерді азайтуға болады. Ол үшін кросс-каналдар жүйесін қолданып, түрлі жүйелерде жасалаған қаржылық операцияларды талдау, күмәнді қаржылар мен оқиғаларды айқындау, күдікті тұлғаларды - клиенттер мен банк қызметкерлерін табу, осыларды айқындауға көмектесетін деректерді жинау секілді шаралар жасалады. Жоғарыда аталған әдістердің соңғысында өз кемшіліктері бар, олар: деректерді қолмен өңделуі, антифрод-аналитиктедің шешімдерінен тәуелді болып қалу, алақтық технологиялардың алуан түрлілігі болуы мүмкін.

Банк саласына қатысы машиналық оқытуды қолданғанда, ондағы басты есептер біршама тиімділіктер әкелетіні сөзсіз. Мысалы, регрессия арқылы – стратегиялық мақсаттарға жету үшін экономикалық болашақ дамуды болжауға, негізделген ішкі, сыртқы ақпарат түрлерін белгілі қасиеттерге сәйкес жіктеуге, кластеризациялауға, клиенттердің деректер өлшемін азайтуға және қаржылық операциялардағы тосын құбылыстарды айқындауға болады. Әрбір клиент туралы жинақталған ақпарат көлемі көп болған сайын, нәтиже де айқын бола түседі. Клиентке көрсетілетін әрбір банктік операциялар арқылы осы деректерді жинауға болады.

Тосунян Г.А. және Экмалян А.М. зерттеулері бойынша [4], банктік қызмет көрсетуде машиналық оқытудың белсенділігі көбінесе: скоринг пен андеррайтинг үшін, алаяқтықпен күресуде және клиенттер мен қызметкерлерді қолдауда, инкассация жасауда пайдаланылатыны байқалады. Әсіресе нейрон желісі, кездейсоқ орман, градиентті бустинг әдістері қолданылады.

Несие беруді автоматтандыруда да машиналық оқуытудың ықпалы зор. Ол тәуекелді бағалау әдісін қолдану арқылы тәуекелді басқаруға мүмкіндік береді. Бұл жерде тәуекелдің өзі бағаланған ықтималдылық. Сондықтан ақпараттық қауіпсіздік архитектурасын тұрғызуда келесідей: хакерлік шабуылдар мен вирус қаупі; банктің конфеденциалды ақпараты мен клиенттердің дербес мәліметтерінің жарияланып кетуі, техникалық немесе бағдарламалық үзілістер, технологиялық ақаулар секілді тәуекелдер ескеріледі.

Шабуылдардың бинарлық жіктелуі туралы айтатын болсақ, ол мәліметтерді дайындау, алу және алгоритмді үйрету арқылы жасалып оқыту сапасы сандық түрде

бағаланады. Банктік антифрод жүйесі осы бинарлы жіктеу есебі арқылы шешілуі мүмкін.

Мысалы, транзакциялардың қауіпсіз, алаяқтық немесе тәуекелді топтарға анықтауда машиналық оқытудың ықтималдылық, корреляциялық және метрикалық әдістері қолданылады. Нәтижелі болжам ақпарат шынайы фактілік мәндермен салыстырылып, төмен нәтиже берсе, онда осы операцияға қатысты тағы басқада деректермен толықтырылып, қамтылады. Антифрод жүйесі онлайн ортадағы аномалияларды анықтағанда машиналық оқыту арқылы тәуекелдерді дәл бағалай алады. Машиналық оқыту талдау арқылы алаяқтық әрекеттердің ықтималдылығын көрсетеді [5, 6]. Қаржылық операцияладағы мәліметтерді темпоральды түрдегі мәліметтер ағыны ретінде қарастыруға болады. Олардан нақты уақыт кезіндегі қажетті білім үзіндісін немесе білім құрылымын алуға болады. Бұл жерде мәліметтер ағынын талдау, Бифет А. пікірінше келесідей шектеулерді ескереді [7]:

1) мәліметтер ағынының өлшемі шексіз болуына байланысты, оны шектеулі өлшеммен сақтаудың мүмкін еместігі, яғни кез келген уақытта шағын мәліметтер ағынын алып, сақтау қажеттілі туындайды;

2) нақты уақыт сәтіндегі мәліметтерді шығарып алу жылдамдығына сұраныс жаңа мәліметтерді генерациялау жылдамдығына ұқсас, яғни мәліметтерді өңдеу уақытының шектеулілігі;

3) генерацияланатын мәліметтердің негізі таралуы уақыт өте келе өзгеруі мүмкін, яғни тек соңғы түскен мәліметтер өңделуі тиіс.

Мысалы, темпоральді мәліметтер бойынша ауытқуларды анықтауда уақыт маңызды фактор болып табылады. Уақыттық қатарлардағы мәліметтер ағынынан ауытқуларды табу туралы біршама жеткілікті зерттеулер жасалған. Ауытқуларды табуда, мәліметтер типі, ұзындығы, белгісі (қалыпты немесе ауытқулы), интерпретациялануы (сипатталуы) және сипатталу деңгейі қарастырылады [8]. Антифрод жүйесі үшін болатын тосын ауытқулардың ықтималдылығы мен жүйе күйлерінің сипаттарын Марков тізбегінің талаптарына сәйкес стохастикалық модель/процесс ретінде қарастыруға болады. Сондықтан ақауларды немесе біздің жағдайымызда алаяқтықты анықтауда қадамдар арасындағы уақыт тұрақты емес және жаңа күйге көшу тек соңғы күйге ғана байланысты.

Жасырын Марков моделін (ЖММ) қолдануды талдау. Жоғарыдағы күйлерден жасырын тәуелділігі бар бақылаулардың болуы осы ЖММ-ін білдіреді. Оны Байес теормасы арқылы да тұжырымдауға болады:

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

Марков тізбегінің қасиеттерін қанағаттандыратын, бірақ бақыланбайтын кездейсоқ, жасырын жеке күйлер үшін ЖММ қарастыруға болады [9]. Әдетте кездейсоқ шама $y(t) = \{y_1, y_2, \ldots y_M\}$ t уақыты мезетіндегі жасырын күй деп аталады Ал кездейсоқ шама x күйлердің дискретті сандары $x(t) = \{x_1, x_2, \ldots x_N\}$ t уақыты мезетіндегі бақыланатын айнымалылар болады. 1-суретте көрсетілгендей, әрбір элемент кез келген мәнді қабылдайтын кездейсоқ айнымалы күйлерді білдіреді.

1-сурет – Жасырын Марков тізбегінің архитектурасы (моделі)

ЖММ арқылы бақылауларға мүмкіндік беретін параметрлерді анықтау қажет. $S = \{s_1, s_2, \ldots s_N\}$ жүйесі N күйлер санынан тұрса, олардың әрқайсысы $V = \{v_1, v_2, \ldots v_M\}$ жиынындағы M мәндердің бірін қабылдайды және жүйенің q_t күйі Y жиынындағы алдыңғы күйден тәуелді. Күйлердің өзара ауысу ықтималдылықтары $A = \{a_{ij}\}$ матрицасы арқылы беріледі:

$$a_{ij} = p(q_{t+1} = y_j | q_t = y_i), \tag{2}$$

және a_{ij} элементтері стохастикалық шектеулерді қанағаттандырады (1-суреттегі көлденең бағыттармен сипатталған): $a_{ij} \geq 0$, мұндағы $1 \leq i \leq N$, $1 \leq j \leq N$ және $\sum_{j=1}^{N} a_{ij} = 1$.

Әрбір M мәннен бақылаулардың шығу матрицасы әрбір N күй бойынша құрастырылады (1-суреттегі тік бағыттармен сипатталған) немесе жүйенің t уақытында j күйіндегі n-ші белгіні бақылайтын тізбекке беру ықтималдылығы – $B = \{b_j(n)\}$ жиынымен беріледі:

$$b_j(n) = p(v_n | y_j), \tag{3}$$

және $b_j(n)$ элементтері келесі шектеулерді қанағаттандырады:

$b_j(n) \geq 0$, мұндағы $1 \leq i \leq N$, $1 \leq n \leq M$ және $\sum_{n=1}^{M} b_j(n) = 1$, мұндағы $1 \leq j \leq N$. Бастапқы күй ықтималдылықтары $\pi = \{\pi_j\}$, $\pi_j = p(q_1 = y_j)$, мұндағы $1 \leq j \leq N$. Сонда жасырын Марков моделі $\lambda = (A, B, \pi)$ түрінде сипатталады. Оны қолдану үшін үш есептің қойылымы қалыптастырылады:

1) бақыланатын мәліметтер тізбегі $X = \{x_1, x_2, \ldots x_N\}$ мен $\lambda = (A, B, \pi)$ моделі беріліп, $p(X|\lambda)$ есептеледі де, ол модельдің берілген бақылаулар тізбегіне қаншалықты сәйкестігін көрсетеді. Оның аналитикалық шешімі тікелей-кері өту процедурасы болып табылады.

2) жоғарыдағы модель мен X бойынша декодтау, оңтайлы $q_1, q_2, \ldots q_T$ күйлер тізбегін табу. Оны шешуде әдетте Витерби алгоритмі қолданылады.

3) оқу барысында бақылауларды ескеріп, $\lambda = (A, B, \pi)$ модельінің параметрлерін $p(X|\lambda)$ максимизацияланатындай етіп табу. Бұл есеп Баум-Уэлч алгоритмін қолданып шешіледі [10-12].

Есепті шешу үшін динамикалық бағдарламалау тәсілін қолдануға болады. Айталық фродты сипаттайтын оқиғаларды қарастырайық:

$$p(X|\lambda) = \prod_{i=1}^{T} P(x_i|q_i) \cdot \prod_{i=1}^{T} P(q_i|q_{i-1}) \quad (4)$$

Қаржы жүйесіндегі транзакциялық талдаулар негізінде қолданушының мінез-құлқына байланысты болжам жасалсын. Модель үшін жасырын күйлерге «күдікті» және «күдіксіз» деген күйлер шартты түрде қарастырылсын.

Ал бақылаулар ретінде: бір қолданушының түрлі геоорналасуы мен түнгі уақыттағы белсенділігі және бір қолданушының тұрақты геоорналасуы мен күндізгі уақыттағы белсенділігі секілді жиынтықтар қарастырылсын. Ықтималдылықтың осы екі жиынтықтарын: өтпелі ықтмалдылықтар (жасырын күйлердің басқа күйлерге өтуі) мен шығу ықтималдылықтарын (жасырын күйлерді ескеру арқылы бақылау ықтималдылығы) пайдаланамыз. Оларды анықтап алған соң, үлгіні үйретуге болады. Олар Баум-Уэлч алгоритмі немесе алға қарай алгоритмі арқылы бағаланады. Келесі, Витерби алгоритмі бойынша жасырын күйлердің аса ықтимал тізбегі есептеліп, модельдің орындалуын бағалау кері қайтару арқылы жасалады. Тәжірибе жүзінде жоғарыда қарастырған фродттық мәселені шешуде оған Hmmleran кітапханасын қолдануға болады және модельге қатысты параметрлерді анықтауда «күдікті» және «күдіксіз» күйлер беріледі:

```
# Define the state space
states = ["suspect", "unsuspectingy"]
n_states = len(states)
print('Number of hidden states :',n_states)
# Define the observation space
observations = ["different geoiocations", "night activity", "permanent
geoiocations", "daily activity"]
n_observations = len(observations)
print('Number of observations  :',n_observations)
```

Нәтижесінде:

```
Number of hidden states : 2
Number of observations : 4
```

Осы қадамнан кейін бастапқы екі күйдің бөлінуі ықтималдықтар массиві ретінде айқындалады. Өтпелі ықтималдық бір күйден екінші күйге өту ықтималдығын мысалдағы жиынтықтар бойынша білдіретін 2×4 массив ретінде айқындалады. Бақылау ықтималдығы әрбір күйден әрбір байқаудың пайда болу ықтималдығын білдіретін 2×4 массиві ретінде анықталады. ЖММ hmm көмегімен анықталады және ондағы бақылау тізбегін декодтау үшін жоғарыда айтылған Витерби алгоритмін қолдану арқылы бақылаулар генерациялаған жасырын күйлердің ең ықтимал тізбектілігі есептеледі. Болжам нәтижесін графиктік сипатта көрсету үшін нақты деректерге және олардың арақатынастарына сүйене отырып, matplotlib кітапханасын қолдануға болады.

Сонымен қатар, ЖММ-дегі күйлердің жасырын айнымалылары мен бақыланатын айнымалылыры арасындағы байланысты қолданып, фрод тудыратын жиынтықтардың (немесе алаяқтық фактілердің) қайсысы басым болатынын апостериорлық ықтималдылықты есептеу арқылы нақтылауға болады. Бұл әр күдікті жағдайдағы нақты фактілерді айқындауға алып келеді немесе жаңартылған ақпаратқа сүйене отырып, оған дейінгі тұжырымды жаңартуға немесе нақты пікір, ұсыныс алуға ықпал етеді.

Қорытынды. Қорыта айтқанда, машиналық оқыту арқылы фродқа қатысты әрекеттерді болжауда ЖММ қолдана отырып, hmmlearn бағдарламалық жабдығымен қажетті деректер тізбегін модельдеуге болады және апостериорлық ықтималдылықты пайдаланып, болжанған тұжырымды жаңартуға да болады. Нәтижесінде қаржылық алаяқтыққа байланысты тәуекелділікті айқындап және оны азайтуда статистикалық тәсілдер мен ережелерді қолданудың тиімділігі үлкен көлемді деректерді дұрыс талдауға байланысты екенін байқаймыз. Дегенмен, фрод үшін жасырын Марков модельін қолдануда құпия қаржылық деректерге қол жеткізудің қиындығы мен оны жүзеге асырудың күрделілігі, бастапқы күйлердің өту матрицасының айқын сипаттамалуыа қойылатын жоғары талаптар секілді шараларды ескеру қажет.

ӘДЕБИЕТ

1 Финансовые киберугрозы в 2021 году. https://securelist.ru/financial-cyberthreats-in-2021/104553/

2 IOSCO Commits to Deliver on Sustainability Disclosures and Crypto Exchanges in 2023. https: //www.iosco.org/news/pdf/IOSCONEWS688.pdf

3 https://www.nur.kz/nurfin/personal/2023518-zaschita-sredstv-klientov-v-halyk-pochemu-eto-tak-vazhno-i-kak-eto-rabotaet/?ysclid=lkqfs07omq234884234.

4 Тосунян Г.А. Банковское право Российской Федерации / Г.А. Тосунян, А.М. Экмалян. – М.: Юрист, 2015. – 448 с. ISBN 5-7975-0233-X

5 Флах П. Машинное обучение. Наука и искусство построения алгоритмов, которые извлекают знания из данных – Москва: ДМК Пресс, 2015. – 400 с. ISBN 978-5-97060-273-7

6 Машинное обучение против фрода. https://www.osp.ru/os/2017/02/13052223?ysclid=lgjmg4x1jr320964583

7 Bifet A. Adaptive learning and mining for data streams and frequent patterns // SIGKDD Explorations Newsletter, 11, 2009. P 55-56. DOI:10.1145/1656274.1656287

8 Gupta, M., Gao, J., Aggarwal, C.C. and Han, J. (2014) Outlier Detection for Temporal Data: A Survey. IEEE Transactions on Knowledge and Data Engineering, 26, 2250-2267. https://doi.org/10.1109/TKDE.2013.184

9 Rabiner L.R. A Tutorial on Hidden Markov Models and Selected Applications in Speech Recognition. PROCEEDINGS OF THE IEEE, VOL. 77, NO. 2, FEBRUARY 1989

10 Момзикова М.П., Великодная О.И., Пинский М.Я., Сироткин А.В., Тулупьев А.Л., Фильченков А.А. Оценка вероятности наблюдаемой последовательности в бинарных линейных по структуре скрытых марковских моделях с помощью апостериорного вывода в алгебраических байесовских сетях // Труды СПИИРАН. – СПб: Наука, 2010. – Вып. 2. – С. 122–142.

11 Forney D.G. The Viterbi Algorithm // Proceedings of the IEEE. – 1973. – V. 61. – № 3. – P. 268–278.

12 Welch L.R. Hidden Markov Models and the Baum-Welch Algorithm // IEEE Information Theory Society Newsletter. – 2003. –V. 53. – № 4. – P. 10–13.

REFERENCES

1 Financial Cyber Threats in 2021. https://securelist.ru/financial-cyberthreats-in-2021/104553/

2 IOSCO Commits to Deliver on Sustainability Disclosures and Crypto Exchanges in 2023. https: //www.iosco.org/news/pdf/IOSCONEWS688.pdf

3 https://www.nur.kz/nurfin/personal/2023518-zaschita-sredstv-klientov-v-halyk-pochemu-eto-tak-vazhno-i-kak-eto-rabotaet/?ysclid=lkqfs07omq234884234.

4 Tosunyan G.A. Banking Law of the Russian Federation / G.A. Tosunyan, A.M. Ekmalyan. - M.: Jurist, 2015. - 448 p. ISBN 5-7975-0233-X 4.

5 Flach P. Machine learning. The science and art of building algorithms that extract knowledge from data - Moscow: DMK Press, 2015. - 400 p.ISBN 978-5-97060-273-7

6 Machine learning against fraud.https://www.osp.ru/os/2017/02/13052223?ysclid=lgjmg4x1jr320964583

7 Bifet A. Adaptive learning and mining for data streams and frequent patterns // SIGKDD Explorations Newsletter, 11, 2009. P 55-56. DOI:10.1145/1656274.1656287

8 Gupta, M., Gao, J., Aggarwal, C.C. and Han, J. (2014) Outlier Detection for Temporal Data: A Survey. IEEE Transactions on Knowledge and Data Engineering, 26, 2250-2267. https://doi.org/10.1109/TKDE.2013.184

9 Rabiner L.R. A Tutorial on Hidden Markov Models and Selected Applications in Speech Recognition. PROCEEDINGS OF THE IEEE, VOL. 77, NO. 2, FEBRUARY 1989

10 Momzikova M.P., Velikodnaya O.I., Pinsky M.Ya., Sirotkin A.V., Tulupyev A.L., Filchenkov A.A. Estimation of the probability of an observed sequence in binary linear in structure hidden Markov models using a posteriori inference in algebraic Bayesian networks // Proceedings of SPIIRAS. - St. Petersburg: Nauka, 2010. - Issue. 2. – C. 122–142.

11 Forney D.G. The Viterbi Algorithm // Proceedings of the IEEE. – 1973. – V. 61. – № 3. – P. 268–278.

12 Welch L.R. Hidden Markov Models and the Baum-Welch Algorithm // IEEE Information Theory Society Newsletter. – 2003. –V. 53. – № 4. – P. 10–13.