



ПРИЛОЖЕНИЕТО НА ИЗКУСТВЕНИЯ ИНТЕЛЕКТ В БОРБАТА С ПРАНЕТО НА ПАРИ ВЪВ ФИНАНСОВИТЕ ИНСТИТУЦИИ

THE APPLICATION OF ARTIFICIAL INTELLIGENCE IN THE FIGHT AGAINST MONEY LAUNDERING IN FINANCIAL INSTITUTIONS

Бойчо Бойчев
Boycho Boychev

Великотърновски университет „Св. св. Кирил и Методий“
St. Cyril and St. Methodius University of Veliko Tarnovo

Abstract: With the advent of universal banking, the problems with this activity increase. As the volume of information on financial transactions, customer data and transactions increases, it becomes increasingly difficult to detect this type of crime. This is due to the nature of the human data processing and analysis process. The process is significantly complex and time-consuming and can be used to use the capabilities of artificial intelligence, which can significantly increase the speed of data processing, information analysis and help decide on the confirmation or rejection of a crime.

The report focuses on the use of artificial intelligence in the fight against money laundering. The benefits and legal risks of its implementation in Europe are highlighted. Three software proposals are considered, which offer specific solutions against money laundering. The developments are by the companies - Ayasdi, SAS and Comarch. It is concluded that the use of AI by financial institutions helps to combat money laundering, which contributes to a significant reduction in operating costs.

Keywords: Anti-Money Laundering; Artificial intelligence (AI); Artificial intelligence (AI) solutions; Fighting financial crime with Artificial intelligence (AI).

JEL: G21, G22

ВЪВЕДЕНИЕ

Голямото предизвикателство пред финансовия сектор в световен мащаб е свързано с процеса „пране на пари“, при който престъпниците прикриват незаконния произход на имуществото или доходите си (EUR-Lex, n.d.). Борбата с този вид престъпления става все по-трудна поради все по-динамичния характер на финансовите услуги и тяхното непрекъснато усъвършенстване и дигитализация. Тя е свързана с големи разходи, като например големите оперативни разходи по наблюдаване на транзакциите (Salonia, 2020a). Изчисляват се годишни разходи на базата на 220 работни дни и резултатът е около 10 млн. евро. В своята разработка Salonia (2020a) разглежда разходите по мониторинг и разследване. При мониторинга разходите за един разгледан случай са малки – до 80 евро, но за сметка на това се проверяват до 20 случая на ден. Причината за голямото количество разглеждани случаи е, че при тях информацията може да бъде проверена или придобита от всеки член на екипа поради несложния им характер. Това обаче не важи за ситуациите, при които се води задълбочено разследване, осъществявано от специално обучен следовател, разходите за него могат да достигнат до 600 евро.

Все по-строгите регулации и кратките срокове за осъществяване на проверките създават финансови и репутационни рискове за финансовите институции (Radukanov, 2017). Отделно хората, занимаващи се с пране на пари, не спират да се адаптират и разработват нови техники в своята дейност, като се възползват от развитието на технологиите онлайн банкиране, електронни разплащания и криптовалуты. Огромният обем транзакции в реално време затруднява откриването на реалните действия по прането на пари. Изчислено е, че около 2 трилиона долара се укриват на година, а биват разкрити около 0,2% от тях (Ghenne, 2019).

Стандартните практики генерират много фалшиви сигнали за открити нередности. Изкуственият интелект (ИИ) дава възможността за бързо намаляване на оперативните разходи, като същевременно подобрява ефективността чрез въвеждане на техники за машинно обучение на различни етапи от процеса на следене на транзакциите. ИИ все по-често се използва в световен мащаб при проверки на клиенти, прилагайки техники за обработка на естествения език и обработка на текст (Craig, 2019), снимки и други (Salonia & Aguilar, & Dragosavac, 2020).

Ползи от използването на ИИ в борбата с прането на пари

Според проучените източници употребата на ИИ в борбата с прането на пари може да предостави значителни ползи за финансовите институции (Shroff, 2020), (Ghenne, 2019). По-важните от тях са:

- дава възможност за нови подходи в борбата с прането на пари;
- подобрява ефективността;
- повишава доверието в институцията, което води до повече клиенти;
- намалява броя на фалшивите сигнали за нередности;
- открива по-лесно сложни взаимовръзки;
- намалява оперативните разходи по разследванията, както и времето за разследване;
- дава възможност за редуциране на операциите, осъществявани от хора;
- открива по-лесно поведенческите промени в клиентите;
- намалява рисковете от санкции от страна на регулаторните органи и тези, свързани с репутацията на финансовата организация;
- намалява рисковете, свързани с репутацията на финансовата организация.

Правни рискове, свързани с използването на ИИ в Европа

Внедряването на ИИ подпомага повишаващите се изисквания на регулатора за борбата с прането на пари и използването му трябва да бъде добре прецизирано с местното законодателство. В контраст с законодателството на САЩ, Израел и други държави в Европейския съюз използването на личните данни на клиентите и тяхната защита е разписано във вече влезлия в сила *Общ регламент относно защитата на данните (ОПЗД) (General Data Protection Regulation – GDPR)*. Според ОПЗД дори центърът за обработка на данни да не е в рамките на Съюза, след като се проверяват негови граждани, трябва да се спазват правилата, произтичащи от европейското законодателство. Допълнително затруднение за финансовите институции е чл. 22, ал. 1, който гласи: *Субектът на данните има право да не бъде обект на решение, основаващо се единствено на автоматизирано обработване, включващо профилиране, което поражда правни последици за субекта на данните или по подобен начин го засяга в значителна степен* (General Data Protection Regulation 2016), т.е. не може да бъде взето напълно автоматично решение за разследвания клиент. В следващата алинея е казано, че може да се направи при някои изключителни обстоятелства или ако е дадено изричното съгласие (посочена е тази опция в ал. 1). От така представения текст не става ясно какви ще са последиците за разследващата организация и какъв би бил изходът от дело, започнато срещу клиент на финансова институция на база селектиране от страна на ИИ. Трябва да се вземе предвид, че ИИ работи благодарение на събрани данни. Строгите правила за съхраняването, обработката и използването на получената информация от тези данни може да се окаже съществен проблем за използването на тази технология за клиенти от Европейския съюз.

От друга страна, има съмнения в обществото относно начина на използване на технологията от финансовите институции. На базата на чл. 22 от ОРЗД не става ясно каква е възможността разследваното лице да се противопостави срещу разследването и как финансовите институции ще могат да докажат, че конкретният случай трябва да бъде в тази категория от изключения, която позволява автоматизирано вземане на решение.

Използване на ИИ в борбата с прането на пари

Въпреки тези притеснения вече има примери за използване на ИИ в борбата с прането на пари. Сред първите, използвали ИИ в своите операции в борбата с прането на пари, е една от най-големите европейски банки – HSBC (Arnold, 2019). Разработката на Quantexa позволява на банката да комбинира човешкия опит с ИИ, като по този начин успява да подобри ефективността на служителите, разследващи този тип престъпления (Quantexa, 2018). ИИ подобрява процедурата по опознаване на своите клиенти, като от значителен обем ръчно изпълнявани операции се преминава към непрекъснат контекстуален подход, който позволява да се повишат резултатите и да се реагира адекватно на повишената сложност, обхват и регулаторни очаквания. Благодарение на ИИ може да се анализират значителните обеми информация за клиентите и да се открие подозрително поведение, както и нови методи и подходи в прането на пари. Резултатите за такъв тип дейности за банката са:

- Увеличаване на ефективността и намаляване на времето за разследване чрез намаляване на фалшивите сигнали.
- Откриване на нови и подозрителни връзки и същевременно разкриване на липсващите връзки при реалните взаимоотношения.
- Адаптиране към различни и нови сценарии и сложни схеми за пране на пари.
- Подобро идентифициране на подозрително клиентско поведение при анализиране на сложните връзки във веригите от доставки и откриване на съмнителни взаимодействия.
- Значително намаляване на оперативните разходи по разследване, намаляване на риска от глоби от регулаторните органи, намаляване на риска за репутацията на финансовата организация.

Друг пример за използване е свързан с Royal Bank of Scotland, която заедно с Vocalink сканира транзакции на малки и големи бизнес клиенти за откриване на фалшиви фактури и опити за измама (Aziz & Dowling, 2019, p. 44). С времето европейските банки започват да внедряват ИИ в своите операции за борба с прането на пари.

Софтуерните решения срещу изпирането на пари

Има различни решения, предоставяни от ИТ фирми, но в тази разработка ще бъдат разгледани само три от тях. Първото е на компанията Ayasdi, второто е на компанията SAS, а третото е на Comarch.

Решението на първата компания е Ayasdi AML (Symphony AyasdiAI, 2019), който анализира поведението на клиентите и търси признаци за пране на пари. На фигура 1. е представено обобщено как функционира Ayasdi AML.



Източник: адаптирано по Symphony AyasdiAI, 2019, p. 3

Фиг. 1. Модел на функциониране на Ayasdi AML

Детайлизиращият поглед към процеса показва, че чрез „Auto Feature Engineering“ се откриват атрибути в данните, които съдържат сигнал за нередност. След това решението автоматично създава нови производни атрибути, които ускоряват интелигентната сегментация. Чрез „Behavioral Insights“ се изготвят ежедневно списъци на всякакви промени в поведението на клиентите във всичките им данни за транзакциите. Благодарение на „Intelligent Segmentation“ клиентите се разделят на различни нива според степента на отклонение от нормалното им поведение. На базата на това разделяне вниманието може да се фокусира към по-рисковите клиенти на банката поради по-голямото отклонение от нормалното им поведение.

С помощта на „Intelligent Event Triage“ се сортират сигналите за възможно нарушение, след като е извършен топологичен анализ на данните. Това позволява да се средоточат специалистите върху най-рисковите случаи, като по този начин се минимизира рискът и се увеличи ефективността.

За анализ дали е извършено нарушение, или не трябва доказателства. Чрез предходните стъпки се осигурява на анализаторите необходимата информация, за да може да се вземе такова решение. Това се случва в „Contextual Alert Information“, където се показват подозрителните действия от страна на клиентите на банката. Според компанията използването на тяхното решение помага за по-бързото вземане на крайно решение по случая дали има, или не нарушение.

Второто разглеждано предложение е на компанията SAS с наименование „**SAS Anti-Money Laundering Features**“ (SAS AMLF). Както и при първото предложение, и тук компанията твърди, че чрез нейния ИИ намаляват значително фалшивите сигнали за нередности – до 80% (SAS, 2020). Според компанията тяхното предложение може да разкрива сложно изградени тайни мрежи за пране на пари, като ги представя в мрежови диаграми. В същото време чрез анализирането на различни източници на информация за даден клиент се използват и непълни записи, несъответствия и т.н., за да може да се определи дали конкретният клиент има съпричастност към даден случай. ИИ позволяват да се разкрият скрити взаимоотношения на разследвания клиент и неизвестни други рискове.

Налице е разделяне на нива по важност, като на базата на тях се приоритизират сигналите, с което се цели повишаване на ефективността. Цялостното наблюдение на транзакциите в реално време позволява да се намалят значително фалшивите сигнали за нарушения.

Третото предложение е на компанията Comarch с името „**Comarch Anti-Money Laundering**“. Подобно на горепосочените две предложения, то обещава по-добро откриване на истински случаи на пране на пари и значително намаляване на фалшивите сигнали с до 20% (Comarch, 2020). Като съществено предимство компанията изтъква, че ИИ е ефективен инструмент и лесно се интегрира с други системи, което е от съществено значение за финансовите институции. Компанията представя своето решение като бързо развиващо се. Способността му да учи от минали случаи спомага за по-добрата му ефективност в откриването на повече истински случаи и за редуцирането

на броя на фалшивите сигнали. Благодарение на ИИ на компанията финансовите институции ще могат да водят по-бързи разследвания чрез откритите скрити модели и връзки. ИИ успява да анализира подозрителното поведение на клиента и да прецени вероятността за опит за пране на пари.

При сравнение на трите ИИ се откроява фактът, че те работят по подобен начин и със сходни показатели. В трите случая се наблюдават припокриващи се позитиви за финансовите институции – повишаване на ефективността, намаляване на оперативните разходи и други, което позволява да се стигне до извода, че за избор на конкретен продукт трябва да се извърши допълнителен анализ.

За по-лесно възприемане на ИИ първите две компании са качили примери за резултатите след внедряването на техните решения в действащи бизнес организации.

Ayasdi AML е изпробвана от една от големите банки в света (Symphony Ayasdi AI, 2019a). Целта на опита е да се повиши ефективността с 3–5%. В процеса на теста се е увеличава използването на SWIFT данните за сегментиране на клиентите и това води до откриване на нови и незабелязани модели и рискове. В **резултат** на направените тестове обемът на започнатите разследвания намаляват с 20%.

На **SAS AMLF** залага израелската застрахователна компания „Ayalon Insurance“, която избира SAS поради факта, че са работили по-рано с нея по изграждането на дейта център. Застрахователната компания споделя, че са избрали новото решение на SAS, тъй като то може да обработва изключително сложни транзакции с множество критерии, за да провери за валидиране. Те също така твърдят, че SAS е в състояние да им помогне да завършат проекта в кратък срок. След внедряването и опита, който трупат, решават, че в близките 10 години ще работят с този продукт. Amit Geva, Ayalon CIO and Executive Vice President споделя следното:

Познаването на банковия бранш и разработените застрахователни модели помогнаха на SAS да предложи комплексни решения, с които да се справят с предизвикателствата, поставени от кратките срокове, предвидени от регулаторните органи (SAS, 2019).

ЗАКЛЮЧЕНИЕ

Използването на ИИ от финансовите институции помага в борбата срещу прането на пари, което намалява значително оперативните им разходи за тази дейност. В същото време намалява времето за разследване, минимизира фалшивите сигнали за този тип дейност и подобрява откриването на сложни създадени модели, схеми и връзки за осъществяването на този тип престъпление. Това спомага за намаляването на финансовите санкции от страна на регулаторите, намаляване на необходимостта на допълнителен персонал поради повишаване на регулаторните изисквания и снижава риска за репутацията на институцията.

Изяснихме, че съществуват разработени такива решения в борбата с прането на пари от различни доставчици. Въпреки това финансовите институции могат да изградят свой ИИ в помощ на своите инспектори. Трябва да се има предвид, че основната дейност на банките не е вземането на такъв тип решения. От една страна, изграждането на такъв тип инструмент ще изисква значително време и средства, но ще бъде изцяло съобразен с нуждите и работните процеси на финансовата институция. От друга страна, закупуването на готово решение би било много по-евтино и значително по-бързо внедрено в работния процес. Естествено съществува вероятността закупеното решение да не отговаря изцяло на нуждите и очакванията на финансовата институция поради непълна съвместимост на процесите и данните.

Подходящо решение на тази ситуация е финансовите институции да се спрат на хибриден подход. Освен споменатия по-горе ИИ, който HSBC използва, те включват и свои ИТ специалисти в подкрепа на разбротването на решение за борба с изпирането на пари на Ayasdi (Mejia, 2020). ИТ персоналят на HSBC помага на Ayasdi да разбере вътрешните данни за AML, а екипът за моделиране на HSBC помага на Ayasdi да създаде точни модели за поведение на клиентите (Shroff, 2020). Това сътрудничество позволява банката лесно да използва и интегрира разработените модели в своята дейност, като по този начин избягва споменатите рискове, което позволява на по-късен етап банката да може да се възползва от по-добро решение, отговарящо на нейните нужди.

REFERENCES

- Arnold, M. (2019, 4 9).** *HSBC brings in AI to help spot money laundering*. Retrieved 5 29, 2020, from Financial Times: <https://www.ft.com/content/b9d7daa6-3983-11e8-8b98-2f31af407cc8>
- Aziz, S., & Dowling, M. (2019).** Machine learning and AI for Risk Management. In T. Lynn, J. G. Mooney, P. Rosati, & M. Cummins, *Disrupting Finance: FinTech and Strategy in the 21st Century* (pp. 33–50). Cham: Springer Nature Switzerland AG.
- Comarch. (2020, 6 3).** *Comarch Anti-Money Laundering*. Retrieved from Comarch: https://www.comarch.com/comarch-fraud-protection/anti-money-laundering/?utm_source=Bangkok%20post&utm_medium=Advertorial&utm_campaign=Bangkok%20post%20Advertorial%20Krzysztof%20Grzywna
- Craig, P. (2019, 9 3).** *How to trust the machine: using AI to combat money laundering*. Retrieved 5 28, 2020, from Builders of a better working world: https://www.ey.com/en_gl/trust/how-to-trust-the-machine--using-ai-to-combat-money-laundering
- EUR-Lex. (n.d.). *MEASURES TO COMBAT MONEY LAUNDERING*. Retrieved 5 28, 2020, from EUR-Lex: https://eur-lex.europa.eu/summary/glossary/money_laundering.html?locale=bg
- General Data Protection Regulation. (2016, 4 27).** *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC*. Retrieved from EUR-Lex - 32016R0679: <https://eur-lex.europa.eu/legal-content/BG/TXT/?uri=CELEX%3A32016R0679>
- Ghenne, C., (2019, 11 8).** *How AI can help reduce money laundering*. Retrieved 5 30, 2020, from Tech Radar: <https://www.techradar.com/news/how-ai-can-help-reduce-money-laundering>
- Mejia, N., (2020, 2 26).** *Artificial Intelligence at HSBC – 2 Use-Cases*. Retrieved from Emerj: <https://emerj.com/ai-sector-overviews/artificial-intelligence-at-hsbc/>
- Quantexa. (2018).** *Anti-Money Laundering: Prevent money laundering*. Retrieved 5 29, 2020, from Quantexa.
- Radukanov, S., (2017).** Market Risk Assessment Under VaR Risk Methodology – Specifications and Application. *Socio-Economic Analysis*, 9(2), 182–194. (in Bulgarian)
- Salonia, G., Aguilar, A. C., Dragosavac, M., (2020, 1 15).** *TRANSFORMING ANTI-MONEY LAUNDERING AND KYC CONTROLS WITH AI: PART I*. Retrieved from Infosys Consulting: <https://www.infosysconsultinginsights.com/2020/01/15/transforming-anti-money-laundering-and-kyc-controls-with-ai-part-i/>
- Salonia, G., Aguilar, A. C., Dragosavac, M., (2020a, 1 20).** *TRANSFORMING ANTI-MONEY LAUNDERING AND KYC CONTROLS WITH AI: PART II*. Retrieved 5 31, 2020, from Infosys Consulting: <https://www.infosysconsultinginsights.com/2020/01/20/transforming-anti-money-laundering-and-kyc-controls-with-ai-part-ii/>
- SAS. (2019).** *SAS® Anti-Money Laundering helps Ayalon Insurance monitor suspicious activity and meet challenging regulatory requirements*. Retrieved from SAS®: https://www.sas.com/en_us/customers/ayalon-insurance.html
- SAS. (2020).** *SAS® ANTI-MONEY LAUNDERING*. Retrieved 5 31, 2020, from SAS: https://www.sas.com/en_us/software/anti-money-laundering.html
- Shroff, R. (2020, 1 16).** *Artificial Intelligence for Risk Reduction in Banking: Current Uses*. Retrieved from Towards Data Science: <https://towardsdatascience.com/artificial-intelligence-for-risk-reduction-in-banking-current-uses-799445a4a152>
- Symphony AyasdiAI. (2019).** *Anti-Money Laundering Solution Deep Dive*. WHITE PAPER .
- Symphony AyasdiAI. (2019a).** *Improving Anti-Money Laundering Detection in Correspondent Banking*. Symphony AyasdiAI. Retrieved from <https://s3.amazonaws.com/cdn.ayasdi.com/wp-content/uploads/2019/09/23124409/Correspondent-Banking-Case-Study-AML.pdf>

За контакти:

Бойчо Бойчев, главен асистент, доктор
 Служебен адрес: В. Търново 5000, ул. „Арх. Георги Козаров“ № 1,
 ВТУ „Св. св. Кирил и Методий“, Стопански факултет
 катедра „Икономическа теория и международни икономически отношения“
 Ел. поща: b.boychev@ts.uni-vt.bg, b.boychev@abv.bg
