Д-р ДИЯНА БАНКОВА
Преподавател в Академията на МВР

Дияна Банкова е родена в град Добрич и завършва средното си образование в направление „Счетоводна отчетност" с профилирано изучаване на английски език във ФСГ „Васил Левски". Притежава бакалавърска степен по *„Счетоводство и контрол"* и магистърска по *„Одит и риск мениджмънт"* към Висше училище по застраховане и финанси (ВУЗФ) – гр. София. От 2018 година е доктор по икономика отново в същия университет, като темата на дисертационния труд е *„Методологически проблеми на публичния надзор над регистрираните одитори"*.

Част е от Академичния съвет и участва в Студентския съвет на ВУЗФ по време на бакалавърската си степен. Удостоена е със специална награда от Националния конкурс по одит за студенти „Млад одитор" (2014 г.). Благодарение на това събитие започва стаж в международната одиторска компания *„HLB Bulgaria"*.

Участва в инициативата на президента на Република България, г-н Росен Плевнелиев – *„Младежка визия за развитие на България"* в Съвета по икономика (2014 г.), както и в Съвета по икономическо развитие (2015 г.).

Кариерното си развитие започва в областта на мениджмънта и търговията. Работи в държавната администрация, като стажант в Централното управление на Националната агенция за приходите (ЦУ НАП), дирекция *„Разследване на особени случаи"*. След това продължава в Министерството на инвестиционното проектиране, дирекция *„Финанси и управление на собствеността"*, отдел *„Финансово-счетоводен"*.

От 2015 година, в продължение на две години и половина, работи като старши инспектор в Комисията за публичен надзор над регистрираните одитори (КПНРО), като *извършва инспекции и разследвания* върху качеството на одиторските практики.

През 2018 г. работи в международната одиторска компания *„Moore Stephens Bulgaria – Audit" OOD* като асистент одитор.

През 2019 г. започва като хоноруван преподавател в Академията на министерството на вътрешните работи (АМВР), към *факултет „Полиция", специалност „Противодействие на престъпността и опазване на обществения ред", Катедра „Оперативно-издирвателна дейност" (ОИД).* През 2020 г. провежда лекции и в катедра *„Сигурност и граничен контрол" (СГК).*

Включена е в списъка на Софийски градски съд (СГС) като вещо лице по съдебно *финансово-икономически експертизи* – ДВ, бр. 41/2020 г.

Одобрена е като *независим експерт, извършващ икономическа оценка* на проектни предложения към Национален иновационен фонд (НИФ) на Агенцията за малки и средни предприятия (АМСП) със Заповед на министъра на икономиката № РД-16-754/20.08.2020 г.

ЗА НЯКОИ ОСОБЕНОСТИ ПРИ ОДИТИРАНЕТО НА ДРУЖЕСТВАТА ЗА ЕЛЕКТРОННИ ПАРИ

Резюме

*В студията е представено значението на електронните пари, както и тяхната съпоставка с други вариации на парични еквиваленти. Отразени са предимствата и недостатъците на различните платежни средства. По този начин се отразят някои особености и специфики при одитирането на дружествата за електронни пари. Изцяло дигитализираният процес при този тип дружества изисква от одиторите да придобият съответните компетенции и допълнителен ресурс в тази област, както и да присъединят съответните експерти към одиторския екип. Иновативните технологии изискват и нови методи и подходи. Като ключова област за одита на ДЕП може да се отбележи – „**Дигитално управление и информационна сигурност**“.*

Злоупотребите с този тип дейност са все по-често срещани, а финансовото изражение е най-голямо като размер, в сравнение с всички видове престъпност (конвенционална и икономическа). Затова е необходимо дипломираните експерт-счетоводители да се съобразят със законодателната рамка и да подават информация и сигнали към компетентните органи.

В Република България все още не са толкова добре развити дружествата за електронни пари, в сравнение с държавите – членки в Европейският съюз (ЕС), Съединените американски щати (САЩ), Япония и Китай. Ще бъдат представени примери за нарушение на дейността на този вид дружества в някои страни. Важно е да бъдат изследвани както „добрите”, така и „лошите” практики, за да се минимизират рисковете от злоупотреби.

DIYANA BANKOVA, PhD
Visiting Professor
Academy of the Ministry of Interior

FOR CERTAIN FEATURES IN AUDITING TO ELECTRONIC MONEY COMPANIES

Summary

The aim of the study is to present the importance of electronic money, to be compared with other variations of cash equivalents, reflecting the advantages and disadvantages of different means of payment. In this way to reflect some features and specifics of auditing electronic money companies. The digitalized process for this type of company requires the auditors to acquire the relevant competencies and additional resources in this area, as well as to join the relevant experts to the audit team. Innovative technologies also require new methods and approaches. As a key area for the audit can be noted - "Digital Management and Information Security".

Abuses of this type of activity are becoming more common, and the financial expression is the largest in size, compared to all types of crime (conventional and economic). Therefore, it is necessary for certified public accountants to comply with the legislative framework, and to submit information and signals to the competent authorities.

Electronic money companies are still not so well developed in the Republic of Bulgaria, compared to the member states in the European Union (EU), the United States of America (USA), Japan and China. Examples of breaches of this type of company in some countries will be presented. It is important to analyze and study both "good" and "bad" practices in order to minimize the risks.

ЗА НЯКОИ ОСОБЕНОСТИ ПРИ ОДИТИРАНЕТО НА ДРУЖЕСТВАТА ЗА ЕЛЕКТРОННИ ПАРИ

„Можете да платите за достъп до база данни, да закупите софтуер или бюлетин по имейл, да играете компютърна игра през мрежата, да получите 5 долара, дължими ви от приятел, или просто да поръчате пица. Възможностите са наистина неограничени."

проф. Дейвид Чаум[1]

Авторът изказва специалните си благодарности за подкрепата и съдействието за настоящата разработка към колегите от Академията на министерството на вътрешните работи, както и към отдел „Киберпрестъпност" към Главна дирекция „Борба с организираната престъпност" (ГДБОП) към МВР!

Увод

Вследствие на пандемията, свързана с ***COVID-19***[2], потребността от дигиталните технологии и системи стана още по-необходима и приложима. На това основание дигиталните разплащания и електронните пари достигнаха своя възход. Това е така, тъй като те навлязоха като усъвършенстван алтернативен начин за разплащане – лесно, бързо и практично. Всеки клиент (независимо юридическо или физическо лице) може да извърши превод от всяка една точка на света. Освен тези положителни страни се крият и някои опасности като – анонимност на лицата, непрозрачност на валутните трансфери, злоупотреба с лични данни, слабости в киберсигурността и други. ***Целта*** *на тази разработка е да бъде подобрена одиторската практика, извършвана върху дружествата за електронни пари в България.* Съответно тя може да бъде реализирана с изпълнението на следните **задачи**:

- ✓ анализ на терминологичното значение на различни валути – биткойни, дигитални пари, криптовалути, електронни пари (ДЕП), виртуални валути;

[1] Цитатът е на криптографа проф. Дейвид Чаум, който говори на първата по рода си конференция CERN в Женева през 1994 година относно електронните пари (eCash).

[2] Инфекциозно заболяване, причинявано от Коронавирус.

- ✓ запознаване с регулаторната рамка на ДЕП и начините за получаване на лиценз за тази дейност;
- ✓ анализ на проблематиката в тези иновативни дружества;
- ✓ предложени примерни модели на въпросници, подходящи за ДЕП;
- ✓ синтезирани ключови области за одита на ДЕП;
- ✓ запознаване с чуждестранната практика на дружества от този род;
- ✓ анализ относно развитието през годините на одиторската професия и значението от дигитализацията на одиторското досие.

1. ТЕРМИНОЛОГИЧНА ОБОСНОВКА И РАЗГРАНИЧЕНИЕ НА ВАЛУТИТЕ

Голяма част от обществото е на мнение, че дигиталните валути поставят своето начало с разновидността на криптовалутата ***„биткойни"***[3]. Това твърдение не е точно така поради факта, че има сведения и концепция за тяхното разработване още от миналото хилядолетие. През 1981 година проф. Дейвид Чаум (**Chaum,1981:p.84**) полага основите на анонимността в разплащанията със статията *„Непроследима електронна поща, обратни адреси и цифрови псевдоними"*. През годините авторът, който е криптограф, продължава изследванията в тази посока и ги доразвива по отношение на **непроследимите плащания**.

В тази връзка през 1990 година в Амстердам се създава първата компания, която изцяло променя света – *"DigiCash", като водеща е разработката на система за електронни пари (eCash)*[4]. Първоначално тази идея изглежда фантастична като дейност според мнението на икономисти. Въпреки това е предложена концепция за холандски държавен проект, свързан с подмяна на разплащанията в брой за входни такси на магистралните пътища със смарт карти.

В края на 1995 година *eCash* са лицензирани от ***Mark Twain Bank в Сейнт Луис.*** През годините много други банки осъзнават потребността от тази иновация и се присъединяват. Част от тях са - ***Deutsche Bank, Credit Suisse, Advance Bank, Norske Bank и Bank Austria, ING, ABN Amro.***

Тук е съществено да се обърне внимание по отношение на ***правото на интелектуална собственост***. Различни компании, в това число и **Microsoft**[5], проявяват желанието да закупят правото на интелектуална собственост, но **проф. Чаум** отказва. Развитието на компанията не е толкова блестящо.

След поредица от неуспешни проекти и сделки *DigiCash* претърпява промяна в управлението. Освен нов управляващ – в лицето на **Michael Nash**[6], се премества и централата от Амстердам в Силициевата долина. Макар и с

---

[3] Платежна система, подсигурена от блокчейн технология и работеща с едноименна единица биткойн. Представлява виртуална валута или криптовалута, но не отговаря на общоприетата дефиниция за валута поради законовите изисквания.

[4] Вариация на електронните пари DigiCash.

[5] Американска транснационална компания, развиваща дейност в областта на компютърните технологии и разработката на софтуери.

[6] Медиен магнат, който е изпълнителен директор и изпълнителен вицепрезидент по дигитална стратегия в Universal Music Group.

ново управление компанията фалира през 1999 година. Друга съществена причина, според проф. Чаум, за която споделя в интервю пред ***Форбс***[7], е неприемането на този метод за разплащане от страна на обществото. Трудно би могъл по онова време да се пречупи навикът на статуквото.

Още едно фундаментално изследване в тази насока от 1997 година е извършено от **Александър Беренстън (1997)** – *„Monetary Policy Implications of Digital Money".* Авторът анализира както силните, така и слабите аспекти на **дигиталните пари**. Като положителни страни отбелязва: разплащания на стоки на дребно, свободно преминаване на международни трансакции, ниски такси и лихви, спестяване на време, поради това, че не е необходимо физическото посещение до офис. За слабости са отбелязани – нарушение на сигурността, фалшификации, анонимност и непроследимост на разплащанията, по-слаб надзор над дейността.

Около 10 години след фалита на *DigiCash* **Сатоши Накамото** през 2008 година създава **криптовалутите** – **Биткойни**. С този иновативен метод се променят изцяло разплащанията. Това е радикална промяна, която изцяло трансформира глобалната икономика. Възникват и доста високи рискове във връзка с извършването на трансфери за нелегални дейности. Липсата на веществени доказателства и информация дава голямо преимущество на нарушителите на закона (изпиране на незаконно придобити средства, финансиране на тероризъм, поръчка на похищения, убийства, изнасилвания и всички възможни деяния). Само ако дигиталните валути бяха проследими, по-горе споменатата проблематика би била разрешена из основи.

Друг интересен начин за разплащане е чрез **електронни пари**. Високотехнологичният процес изисква и допълнителни компетенции. Извършваният надзор на национално ниво от **Българска народна банка**[8] **(БНБ)** е добра основа. С предстоящото ни присъединяване към еврозоната европейските надзорни органи ***ERM II***[9] гарантират допълнителна сигурност за повишаване на контрола върху банките и банковите институции, както и дружествата за електронни пари.

Важно е да се отбележи, че и от страна на одиторите ще се изискват допълнителни процедури. Трудно установимо е да се идентифицират изпратените и получените преводи чрез тези дигитални приложения. Точно тук е важно да се фокусира внимание. Често пъти средствата биват използвани за изпиране на пари, финансиране на трафик, тероризъм и други нелегални дейности. Одиторите не са криминалисти, но когато извършват процедури, обвързани с разплащанията на дружествата за електронни пари, е приоритетно да са запознати с нормативната рамка. Не става въпрос за изземване на функциите на ***Държавна агенция национална сигурност***[10] ***(ДАНС)*** и ***отдел „Киберпрестъпност"*** на ***ГДБОП***[11] към ***МВР***, а за субординация и координация между различните професии и институции, които защитават обществените интереси на национално и транснационално ниво. Освен дейността на оперативните органи за защитата на публичните интереси, от съществено значение е паричната политика на една държава. Тя се определя от **централната банка**

[7] Топ таблоид, свързан с бизнес и финанси в САЩ.
[8] Централната банка, емитент на левова валута в Република България.
[9] Валутен механизъм на Европейската централна банка (ЕЦБ).
[10] Орган, защитаващ националните интереси и сигурност.
[11] Дирекция към МВР, която се бори с тежката и организирана престъпност.

на съответната страна. Освен това важен инструмент са контролът и надзорът, които се упражняват върху тази политика. Със създаването на разнообразни валути може да се установи, че банките вече не са монополни структури, и са налични и други междубанкови системи за сетълмент[12].

Дотук се спомена за няколко разновидности на паричните и мрежовите еквиваленти – *валута, дигитални пари, криптовалута, електронни пари.* Тяхното разнообразие е изключително широко. Някои от тях притежават сходни признаци, но и различия.

За тази цел е необходимо да се направи репрезентация на различните валути. По този начин ще могат да бъдат разграничени една от друга. На първо място ще се разгледат **стандартните валути**.

Те са строго специфични за всяка една държава. Регулират се от централните банки. Стандартната валута има лимитирано използване, тъй като е официална само в конкретна(и) държава(и). Притежават материален характер. Например в България БНБ е емитент на левовата валута.

Позицията в доклада на **Европейската централна банка** (**ЕЦБ**) (**2015:p.33**) по отношение на валутите е, че представляват монети и банкноти. Когато става въпрос за конкретна валута, „като еврото или щатския долар, значението става по-концептуално, представяне на стойност, която е подкрепена от закон и/или правителство (фиатната валута)".

Вследствие на модернизацията и достигането на високо технологично развитие вече се говори за „**виртуални валути**". Те представляват цифрово представяне на стойност, която не се емитира или гарантира от централна банка или друг публичен орган. Не е свързана със законово установена валута и няма правния статут на валута или на пари, но се приема от физически или юридически лица като средство за обмяна и може да се прехвърля, съхранява и търгува само и единствено по електронен път. Представляват нерегулирани пари, които се контролират от създателя си и се използват от определени членове на виртуални групи (например онлайн игри). ***Нямат статут на легално платежно средство***, което не означава, че не могат да бъдат закупувани стоки и услуги чрез тази валута.

Според **ЕЦБ** виртуалните валути имат „дигитална репрезентация на стойност, не се издават от централна банка, кредитна институция или институция за електронни пари и при някои обстоятелства може да бъдат използвани като алтернатива на парите"[13]. Тяхното разнообразие е изключително голямо. Срещат се и други техни прототипи.

Председателят на **ЕЦБ** – ***Кристин Лагард***, дава изявление във връзка със създаването на **дигитално евро**. По този начин разплащанията ще се осъществяват по-бързо и лесно. Обявена е информация,че европейските банки проучват рисковете в тази посока. В допълнение са отразени и други предимства, свързани със смекчаване на въздействието от природни бедствия, както и пандемията.

Друг тип дигитални валути с финансово изражение за покупко-продажба онлайн са „**електронните валути**". Налични са редица

[12] Систематично прехвърляне на парични средства по сметки.
[13] Ibid.

лицензирани **дружества за електронни пари** (**ДЕП**). Най-ярък международен пример за ***ДЕП*** е компанията **Revolut**[14]. Чрез мобилните приложения тяхното потребление се увеличава многократно. Тези дружества издават и карти от пластика спрямо желанието на своите потребители. Паричният баланс се записва върху картата и трансакциите се осъществяват.

Изследването на **FinTech** – *"Implementing a Central Bank Digital Currencies Working Group: Lessons Learnt and Key Insights Policy Report",* също акцентира върху финансовите иновации. От концептуална гледна точка издаването на цифрови фиатни пари ще повлияе значително за намаляване на разходите, свързани с банкови такси. Работната група на Латинска Америка разглежда детайлно проекта за електронно-песо валута.

В съответствие с английското законодателство са разработени насоки във връзка със създаването на *ДЕП*. Като определения са заложени следните: издателите на електронни пари са всички лица, имащи право да издават електронни пари; институциите за електронни пари са лица, упълномощени или регистрирани да издават електронни пари. Съответно има специфични изисквания и режим за тези правомощия.

Често пъти електронните пари биват считани за „**криптовалути**". Това е погрешно, тъй като те са **средство за разплащане, използващо критография за защита и контрол по създаването на нови единици.** Официално са създадени през 2009 година с разработката „**Биткойн**". Създадени са и други прототипи като: ***Ethereum, XRP*** и ***Litecoin***. **Те представляват дигитална криптовалута, а не дигитални пари**!

Според ***Security Exchange Commission*** *(**SEC**)* „биткойнът е описан като децентрализирана виртуална валута *„peer-to-peer"*[15], която се използва като пари – тя може да бъде обменена за традиционни валути, като американския долар, или използвана за закупуване на стоки или услуги, обикновено онлайн. Отличава се от другите валути, защото липсва централен управляващ орган.

Али Вейсел твърди в своето изследване, че „за да се отговори на въпроса дали криптовалутите представляват пари или измама, е необходимо да се изследват техните" (**2018: с. 131**) характеристики. Мненията по отношение на критовалутата са различни. Затова ще се представят част от силните и слабите им страни.

За тях може да се каже, че се считат донякъде за сигурно разплащане, причината е специфичната технология „блокчейн", която представлява публичен счетоводен запис. Криптовалутите са защитени с криптография, т.е. те са криптирани и поддържани от математически алгоритми, като по този начин осигуряват сигурност при трансакциите и контрол при създаването на нови единици. Интерес представлява това, че тя притежава високо ниво на прозрачност заради публичният адрес на потребителя и същевременно поверителност.

---

[14] Revolut Ltd е британска компания със седалище в Лондон, създадена през 2015 година. Извършва финансови, банкови и електронни услуги.

[15] Начин за разплащане чрез специален софтуер, без посредници. Извършва се директно между лицата.

В този ред на мисли е нужно да се спомене, че криптовалутите са и ***„цифрови валути“***. Зад това разплащателно средство стоят редица кодове, сложни математически алгоритми, които се променят постоянно. Криптовалутите се добиват чрез „копаене“ (от англ. език „minning“), което представлява процес по трансформация на кодовете, възпроизведен от компютър.

Основната им слабост е децентрализацията, липсва контрол и надзор над функционирането на криптовалутите. Отличават се със своята анонимност за всички участници в мрежата. Това е най-притесненият момент, защото могат да бъдат открити в т.нар „**dark net**”[16] – **порнография, насилие, оръжия, наркотици, поръчки за убийства, изпиране на пари, крадени стоки.**

Нужно е да се направи разграничение между всички разгледани понятия. Затова в таблицата по-долу ***(Таблица № 1)*** ще се представят някои характеристики на част от представените термини. Данните са упоменати от 1997 година и това дело е от изследване на **проф. Беренстън**.

Таблица № 1. Характеристика на валути

Характеристики	**Дигитални пари**	**Валута**	**Чекове**	**Дебитни карти**
Законно платежно средство	Не	Да	Не	Не
Приемливост	?	Широко разпростра-нени	Ограничена	Ограничена
Пределна цена на трансакция	Ниска	Средна	Висока	Средна
Окончателно плащане лице в лице	Да	Да	Не	Не
Окончателно плащане, което не е лице в лице	Да	Не	Не	Не
Анонимност на потребителите	Да	Да	Не	Не

Източник: Berentsen, A., Monetary Policy Implications of Digital Money, University of Bern, 1997, p. 4.

Първият и най-важен признак на валутите, според **проф. Берентсън**, е ***„законността”***. Като най-сигурна се определя регулираната стандартна валута, тъй като тя подлежи на надзор и се счита за нерискова. По тази логика може да се отбележи, че и ДЕП също може да се смятат за сигурни разплащателни институции, защото са поставени под надзор.

[16] Превод от английски език (тъмна мрежа).

Друг характерен белег е ***„приемливостта”***. Винаги може да съдим по потреблението доколко даден продукт се приема. В случая най-масово разпространени и приети са стандартните валути.

„**Таксите**” също имат съществена роля за потреблението от обществото. Банките и банковите институции начисляват редица такси на своите потребители. Най-съществени са при международни плащания. Тази характеристика дава най-голямо предимство за електронните пари, защото таксите са много по-ниски. При криптовалутите дори механизмът е още по-опростен, тъй като липсва регулатор.

В забързаното ежедневие дори вече се счита като недостатък разплащането лице в лице. С разразяването на пандемията *COVID-19* предимно се избягва този начин. Тук отново разплащанията с дигиталните технологии са с предимство пред фиатните валути.

Отличителен признак спрямо това изследване е и „**анонимността**”. Тя поражда съществени рискове за извършването на престъпления. Тяхната разкриваемост е почти невъзможна – поради високотехнологичното развитие, липсата на следи и заблуждаващата информация.

Като обобщение от краткия анализ следва да се отбележи за електронните пари, че те ***може да се считат за заместител на фиатните пари***. Те са удобни, най-вече за трансгранични плащания, регулирани са, спестяват се различни такси в зависимост от поставените условия от дружеството. Поради това се усеща, че се явяват конкуренти на банковите институции. Тези дружества притежават редици специфики, затова е необходимо да се обърне внимание на нормативната уредба.

2. НОРМАТИВНА РАМКА. ПОЛУЧАВАНЕ НА ЛИЦЕНЗ ЗА ДЕП

Електронните пари са централизирана валута, която отговаря пред строго определена законодателна рамка. Това преимущество драстично намалява рисковете от нарушения. Необходимо е да се разгледа установената нормативна база, която е строго специфична. Едно от изискуемите условия за започването на финансов одит е да бъдем запознати с правната рамка.

В тази връзка с ***Регламент (ЕС) №1093/2010*** на ***Европейския парламент*** и Съвета от 2010 година е създаден **Европейският надзорен орган над банките** (**ЕБО**). В него също са описани и методите на компетентните органи за извършване на надзорна дейност над банките и банковите институции.

Спрямо европейското законодателство *ДЕП* подлежат на принудителен надзор спрямо ***Директива 2009/110/ЕО*** към Европейския парламент и Съвета. Предвид спецификата и характера на дейността тяхното приложение е „като електронен заместител на монети и банкноти, които следва да се използват за извършване на плащания, обикновено на ограничени суми, а не като средство за спестяване”. В случая не се използват за депозити.

За допускане стартирането на тази дейност е фундаментално да бъде доказана финансова стабилност. Едно от изискванията е за начален капитал

в размер не по-малък от 350 000,00 евро. Необходимо е да бъде доказан и произход на средствата от потенциален собственик на дружеството.

Дейностите, които могат да бъдат извършвани от едно ДЕП, спрямо европейското законодателство, са изброени в ***чл. 6*** от ***Директивата***. Включват: *предоставяне на платежни услуги, предоставяне на кредит, свързан с платежни услуги, предоставяне на оперативни услуги и на тясно свързани спомагателни услуги по отношение на издаването на електронни пари или на предоставянето на платежните услуги, експлоатация на платежни системи.* Всяка дейност има своите специфики.

Поради широкото разпространение на електронните пари в цял свят европейското законодателство разширява законодателната рамка. Създава се и ***Директива (ЕС) 2015/2366*** за платежните услуги в целия ЕС, която да развие пазара на електронната валута. Целите са насочени към: повишените изисквания за сигурност; прозрачността; спазване на правата и задълженията.

Например дейностите, свързани с издаването и обратното изкупуване на електронни пари, са задължени да бъдат по номинална стойност. Това се посочва в договор между страните. Също така се забранява и начисляването на допълнителни лихви. Затова биват и предпочитани като начин на разплащане. Дейността и услугите, които се предлагат, са изключително разнообразни.

Поради редицата предизвикателства пред функционирането на ДЕП от **ЕБО** издават ***насоки,*** включващи 4 направления: *платежни институции (ПИ), доставчици на услуги по предоставяне на информация за сметка (ДПИС),* ***институции за електронни пари*** *(**ИЕП**) и компетентните органи (КО).*

За да получи едно *ДЕП* одобрението от компетентните органи и лиценз, е необходимо да бъдат изпълнени насоките. Въз основа на тях ще бъде извършен кратък анализ. Изследването се насочва към един **ключов въпрос**: *какви са изискуемите условия за лицензирането на тази дейност на държавите – членки на Европейския съюз (ЕС)*:

- ✓ *идентификационни данни* – наименование на дружеството, учредителни документи, правен статут, адрес на управление и седалище, уебстраница, координати на отговорниците по досието за кандидатстване, финансова история на заявителя, информация за опит в банките и банковите институции, справка от ТР, удостоверение за платена такса за кандидатстване;
- ✓ *програма на дейност* – описание на дейностите, които ще извършва институцията, видове платежни услуги и продукти, участващи страни, планиране на времето за изпълнение на дейностите, обекти на дейности и посредници, пазар, на който ще се предлагат услугите, 3-годишен план за дейност с очаквани финансови резултати, застраховка „Професионална отговорност" или друга гаранция;
- ✓ *бизнес план* – маркетингов план (представящ как и къде ще се развива дейността и изследване на пазара); ако дружеството е развивало дейност, е нужно да се предоставят годишните финансови отчети, за да се проследят финансовите резултати; ако е новоучредено, трябва да

се изготвят прогнозни финансови отчети за 3 години напред, произход на изискуемия собствен капитал;

- ✓ *организационна структура* – органиграма на дружеството, необходим персонал и определение на функциите, задълженията и правата на служителите, вътрешни правила и политики, разписване на процесите и контролите, договори с външни организации, ако са необходими;
- ✓ *доказателство за начален капитал* – изискуемият според европейското право е 350 000,00 евро. Притежателят е задължен да докаже произход на средствата, например чрез одитиран годишен финансов отчет на вече съществуващо предприятие. Ако дружеството е в процес на регистрация, е достатъчно банково извлечение от сметката на титуляра;
- ✓ *мерки за защита на средствата на ползвателите на електронни пари и/или на ползвателите на платежни услуги* – политика по управление на риска (напр. операционен риск, ликвиден риск, валутен риск, риск от контрагента, кредитен риск, вътрешноприсъщ риск и др.), политика за защита на личните данни, копие на застрахователна полица;
- ✓ *управленска рамка и механизми за вътрешен контрол* – описание на контролите и процедурите, идентифициране на одиторите, идентифициране на отговорните лица, които имат съществена функция за някои от контролите;
- ✓ *процедура за наблюдение, обработване и проследяване на инциденти, свързани със сигурността, и жалби на клиенти във връзка със сигурността* – разработване на правила, насочени срещу риска от измами, контакти с клиенти, регистър, възможност на клиентите да подават жалби и сигнали, данни за ангажираните лица, указващи помощ;
- ✓ *процедура за записване, наблюдение, проследяване и ограничаване на достъпа до чувствителни данни за плащанията* – криптиране на информацията, аутсорсинг процеси, политика за сигурността на информацията;
- ✓ *мерки за осигуряване на непрекъснатост на дейността* – описание и анализ на работна среда и процеси, начини за отработване на пропуснатите ползи при настъпването на инцидент или природно бедствие;
- ✓ *политика за задълженията във връзка с изпирането на пари и финансирането на тероризма* – оценка на риска от изпиране на пари и финансиране на тероризъм, разписване на критерии за съмнителни операции, подаване на сигнали към компетентните органи при наличието на съмнение за изпиране на пари; да се разпишат процедури по отношение стопиране на трансакции и други по-специфични, свързани с предотвратяването и разкриването на престъпления; преценка на рисковете на национално и международно ниво.
- ✓ *одобрение на управляващите съдружници* – доказване на професионален опит и компетентност в областта на банковия сектор,

добра репутация, почтеност, да не са образувани досъдебни производства, липса на данъчни задължения и изпадане в несъстоятелност.

Макар и да изглеждат много на брой изискванията в насоките на **ЕБО** за придобиването на лиценз за *ДЕП*, в някои страни надзорната функция е още по-разширена. Например в **Обединеното кралство**, преди да излезе като страна – членка на ЕС, е създаден през 2015 година независим орган, който отговаря за надзора върху електронните пари. Органът се нарича „***Financial Conduct Authority*** *(**FCA**).*

Освен че ***ЕЦБ*** регулира процедурите по лицензиране, ***FCA*** също отдава значение на прозрачността в този бизнес. Като иновативен подход са създадени м. октомври 2020 година специални правила за прозрачност, както и ръководство над дейността. Разработени са и технически стандарти с изисквания как трябва да изглежда финансовата отчетност на едно *ДЕП*.

След като се извърши преглед на законодателството на държавите – членки на ЕС, е приоритет да се представи и как функционира юридическата система в Съединените американски щати (САЩ) по отношение на електронните пари. За разлика от правната система на ЕС, в САЩ дейността на емитентите на електронни пари се координира от редица различни органи. Емитентите на електронни пари подлежат на надзор от *“**Office of the Comptrolle of the Currency**” (**OCC**)* и *„**Federal Deposit Insurance Corporation**” (**FDIC**)*. Двете публични институции притежават широк кръг от правомощия и комптенции в банковия сектор.

На пръв поглед изглежда, че липсва основен закон, който да отговаря за електронните пари в САЩ. Обаче тяхната правна система е много по-различна. При тях се наблюдават различни нива на регулиране, които не са централизирани в една институция.

За електронни пари се споменава в *„**The Uniform Money Services Act**”*. Одобрен е и приет само от някои територии като: Аляска, Арканзас, Айова, Пуерто Рико, Тексас, Вирджински острови, Върмонт и Вашингтон. Във всеки един щат са създадени специфични закони. Например законите в щата Флорида са различни, в сравнение с тези в щата Тексас. Това важи и по отношение на електронните пари, което затруднява изследването на политиката за електронни пари в САЩ.

Особеност е, че дори чисто терминологично понятията са различни, но с един и същи смисъл. На федерално ниво *„**Code of Federal Regulations (CFR) § 1010.100**”* въвежда термин като „***предплатен достъп***“, което означава „достъп до средства или стойността на средствата, които са предварително платени и могат да бъдат извлечени или прехвърлени в някакъв момент в бъдеще чрез електронно устройство или превозно средство като карта, код, електронен сериен номер, мобилен идентификационен номер или личен идентификационен номер“. Може да се направи аналогия с използването на електронни пари.

Различните правни основания във всеки щат се различават драстично, в сравнение с единния подход на европейското право. Всеки един щат разполага с финансова комисия, която регулира дигиталните валути. Съответно е нужно всички органи да си взаимодействат, което утежнява надзора и регулацията над дейността.

Предимствата на европейското законодателство са на лице. Всяка страна – членка на ЕС, избира свой компетентен орган, който да извършва надзорна дейност над кредитните, банковите институции и електронните пари. В линия на упражнявания контрол над дейността финансовият одит не е за пренебрегване.

ЕБО отбелязват и като съществена насока избора на одитор. За одитора и неговия екип е важно да разполага с необходимия ресурс (време и компетенции) за извършването на одита. Логично е, че тези специфични изисквания важат в пълна сила и за националното ни законодателство.

Българското законодателство урежда създаването на *ДЕП* чрез:

- ✶ *Закона за платежните услуги и платежните системи (ЗПУПС), чл. 1, т. 4, глава трета;*
- ✶ *Закона за кредитните институции (ЗКИ), чл. 3а, ал. 1;*
- ✶ *Наредба № 16 на БНБ за издаване на лиценз и одобрения, за вписване в регистъра по чл. 19 от ЗПУПС и за изискванията към дейността на операторите на платежни системи с окончателност на сетълмента.*

В България пазарът на електронни пари не е все още толкова добре развит, както в някои други страни в ЕС. Основният регулатор на *ДЕП* в Република България е **БНБ**. Затова ще бъдат представени лицензираните *ДЕП (**виж Таблица № 2**)* от профилирания регистър на **БНБ**. Освен че ще бъде установен техният брой, ще се покаже и кои са одитиращите ги дружества.

Таблица № 2. Дружества за електронни пари в България

№	Име	Дата на решение за получаване на лиценз	Одитор за 2019 година
1.	„Айкарт“ АД (предишно наименование „Интеркарт Файнанс“ АД)	Решение № 74 от 21 юли 2011 г.	„Грант Торнтон” ООД
2.	„Транзакт Юръп“ ЕАД (предишно наименование „Ти Би Ай Кредит“ ЕАД)	Решение № 73 от 21 юли 2011 г.	„ПрайсуоъурхаусКупърс Одит” ООД
3.	„Пейнетикс“ АД (предишно наименование „Кредибул“ ЕАД)	Решение № 44 от 11 април 2016 г.	„Ърнст и Янг Одит” ООД
4.	„Изипей“ АД	Решение № 258 от 25 октомври 2018 г.	„Грант Торнтон” ООД
5.	„Изи Пеймънт Сървисиз“ ООД	Решение № 259 от 25 октомври 2018 г.	„Мур Стивънс България - Одит” ООД
6.	„Майфин“ ЕАД	Решение № 71 от 27 февруари 2020 г.	- (новоучредено)

Източник: *БНБ, Регистър на лицензираните дружества за електронни пари в Република България, както и на техните клонове и представители (по чл. 19 от Закона за платежните услуги и платежните системи), Търговски регистър*

В Република България към момента има 6 на брой ДЕП. Всяко едно от тях е предпочело одиторско дружество от ***Big 10***[17]. Това ограничава по-малките одиторски компании, но много наподобява критериите за избор на одитор за застрахователно дружество или банка/банкова институция.

Необходимостта от ИТ специалист за тази дейност стои в основите. Малките одиторски компании не могат да си позволят да влагат допълнителен ресурс и средства. Само че без вещо лице в областта няма как да бъдат извършени ефективни проверки на водещите ИТ контроли на ДЕП, както и да се провери доколко е устойчива техническата част на софтуерното изпълнение. Това може да се счете за сериозен законодателен пропуск по отношение на изискванията за извършване на одит на ДЕП.

3.СЪЩНОСТ НА ПРОБЛЕМА

Както всеки сравнително нов бизнес, така и дейността с електронните пари може да се отчете като по-рискова, защото не е толкова добре позната за обществото. За разлика от вариациите с криптовалутите, електронните пари подлежат на надзор във всяка една държава. Въпреки това оперативните органи са установили редица нарушения в тази дейност. Одиторите също трябва да обърнат внимание на това заради необходимостта да се извършват процедури относно рисковете от измами в съответствие с ***Международните одиторски стандарти (МОС)***.

В този случай престъпленията и измамите могат да бъдат от различно естество. **Компютърните престъпления** са все по-често срещани. Изцяло дигитализираната валута е на фокус от кибератаки на хакери. **ДЕП** имат ангажираността спрямо националното законодателство, по-конкретно **чл. 212** от **Наказателния кодекс** (**НК**): *„Който с цел да набави за себе си или за другиго облага възбуди или поддържа заблуждение у някого, като внесе, измени, изтрие или заличи компютърни данни или използва чужд електронен подпис и с това причини на него или на другиго вреда, се наказва за компютърна измама с лишаване от свобода от една до шест години и глоба до шест хиляди лева“.*

Често срещан пример ***за киберпрестъпление и данъчно престъпление същевременно*** е манипулирането на софтуерните продукти и касови апарати към **Националната агенция за приходите** (**НАП**)[18]. Почти невъзможно е да се установи дори и от дипломиран експерт-счетоводител подобна манипулация. Това важи в пълна сила и за ДЕП. Потребността от ИТ познания е основна за разкриването на подобен тип деяние.

Друга спекулация за електронните пари е, че могат да се използват **за пране на пари и финансиране на тероризъм**. Според **Руси Янев** „слабости“ и „бели полета“ в нормативната уредба в сферата на икономиката и в наказателното законодателство са благоприятни условия за извършване

[17] Десетте най-големи одиторски компании в цял свят.
[18] Специализиран държавен орган към министъра на финансите.

на престъпления“(2011: 57). Затова е необходимо одиторите да познават по-добре законодателната рамка. Причината е, че често пъти ДЕП се смятят от широката общественост за механизъм за изпиране на нелегално придобити средства.

Не случайно **ЕБО** задължава тези дружества да разработят политика срещу тези престъпления. Европейското законодателство реферира към **Директива на Европейският съюз (ЕС) 2018/843**, съдържаща изисквания срещу изпирането на пари и финансирането на тероризма. Тя се разширява и биват включени и емитентите на електронни пари. Максималният размер на един превод възлиза до 250 евро. Малката трансакция не буди сериозно съмнение за това престъпление.

За да бъде минимизиран този риск, са въведени ограничения на сумите съгласно *Четвъртата директива срещу противодействието на пране на пари и тероризъм*[19]. От страна на одиторите е нужно да бъдат извършени процедури, свързани с риска за изпиране на пари и финансиране на тероризъм. За целите на изследването е създаден рамков въпросник (Таблица № 3), относим за предмета на дейност на ***ДЕП***. За всеки един от въпросите е желателно да бъдат прикрепени и доказателства.

Таблица № 3. Определяне на риск от изпиране на пари и финансиране на тероризъм за ДЕП

№	Въпросник	Да	Не	Коментар
1.	*В коя държава е регистрирано ДЕП?*			
2.	*Гражданството на действителния собственик от държава извън ЕС ли е, или от държава с висок риск?*			
3.	*ДЕП издава ли акции?*			
4.	*ДЕП има ли други свързани лица?*			
5.	*Налице ли са данни за промяна на предмета на дейност на ДЕП?*			
6.	*С какви активи разполага ДЕП?*			
7.	*Има ли информация за заведени съдебни и досъдебни производства за финансови престъпления към ДЕП или към свързани с него компании?*			
8.	*ДЕП има ли множество сметки в различни банки?*			
9.	*ДЕП има ли отношения с компании, които са регистрирани в страни извън ЕС и/или офшорни зони?*			
10.	*Оперират ли повече от едно упълномощено лице сметките на ДЕП?*			

[19] Directive (EU) 2015/849 on preventing the use of the financial system for money laundering or terrorist financing (4th anti-money laundering Directive).

11.	*Входящите преводи на дружеството предимно от държави с висок риск ли ще са, или от държави извън ЕС?*			
12.	*Дружеството декларира ли, че ще прави чести тегления на суми в брой от сметките си?*			
13.	*В кои държави ДЕП декларира, че осъществява чести международни преводи от сметките си?*			
14.	*Основната дейност на дружеството лицензионна ли е?*			

Друга специфична функция на ***ДЕП*** е **мобилността**, която поражда съществени рискове за изпирането на пари. Средствата могат да се изпратят до държава, в която няма правна защита срещу прането на пари (т.нар. офшорни зони). Могат да бъдат откраднати при пробив в сигурността: лични данни, номер на сметка, пин на картата.

Препоръчително е одиторите да извършат тестове и процедури към **мобилността на апликацията**, като базисна за предмета на дейност на тези дружества, например да се документира: кой е създал апликацията, кой я поддържа, какви са вътрешните правила за нейната сигурност, пробен акаунт, какви са функциите на приложението и други.

Това е от значение, тъй като през месец септември 2020 година в Япония 5 компании (*Post Bank Co. Among the five, Z Holdings Corp., a subsidiary of SoftBank Corp.*) заявяват за неправомерно теглене на електронни пари чрез мобилната услуга ***PayPay***[20]. Стойността на измамите възлиза на около 1,41 милиона йени. Този случай не е прецедент в Япония. *Дружеството NTT Docomo* го сполетява същата участ и загубата е 26,7 милиона йени.

Друга разновидност на тази престъпност е чрез създаване на карти близнаци или „клониране на картите". Често основание за това е вътрешната измама от служител на дружеството. Дублирането на картите може да се извърши и от трета страна чрез скимиращо устройство, което записва необходимите данни, за да бъдат клонирани.

Европол също се бори с киберпрестъпността. Компетентния полицейски орган разделя престъпленията на две категории. Едните са относно онлайн измама с наличие на карта, която се случва в търговски обекти, или измама без карта, която се реализира онлайн.

Спрямо статистическите данни на Европол потреблението на безкасови плащания в ЕС е най-високо. Като приоритетна цел се поставя противодействието именно на тези престъпления. За тази цел се създават ***Съвместни екипи за разследвания (СЕР)***.

СЕР представляват международен способ за сътрудничество въз основа на споразумение между компетентните органи (съдии, прокурори,

[20] Мобилно приложение за разплащания.

следователи) и прилагането на закона. Споразумението се сключва между две или повече държави. Създава се за определен срок и с конкретна цел, за да се разследва престъпление в една или повече от замесените държави – членки на ЕС.

Павел Николов детайлно изследва функциите на Европол, включително и на участието на организацията към СЕР. Обобщава за СЕР – „създава се въз основа на сключено официално споразумение между заинтересованите страни за провеждане на разследвания по наказателни дела в една или повече държави членки, които създават екипа" (Николов, 2017:48).

Киберпрестъпността не е само на европейско ниво, за съжаление. ***Интерпол***[21] също взема участие в пресичането на трансграничната престъпност. На официалната уеб страница на този орган е споделено, че е разработен специален софтуер за проследяване на трансакции с криптовалути в тъмната мрежа. Поради колосалните загуби в световен мащаб от киберпрестъпления от страна на одиторите е нужно да се вложат усилия спрямо спецификите на софтуерите или да бъде причислен към одиторския екип външен ИТ специалист, притежаващ нужните специфични умения да се извършат допълнителни тестове, алтернативни процедури на електронната платформа. Затова по-долу е споделен и примерен въпросник, който може да бъде модифициран.

Таблица № 4. Идентифициране и оценка на оперативните рискове на електронните пари

№	Въпрос	Коментар
1.	*Кои са най-сложните части от процеса за осъществяването на превод?*	
2.	*Има ли някакви големи, високорискови трансакции, които се случват редовно?*	
3.	*Има ли механизми за удостоверяване, които лесно се фалшифицират?*	
4.	*Как може някой да злоупотреби със системата?*	
5.	*Как някой може да наруши операциите?*	
6.	*Какви измами са разпространени в страната, свързани с електронните пари?*	
7.	*Колко често се реализират?*	
8.	*Какво е общото ниво на престъпна дейност и силата на правоприлагането в страната?*	
9.	*Каква е вероятността за риск?*	
10.	*Какво е потенциалното въздействие върху бизнеса (финансово и репутационно)?*	

[21] Международната организация на криминалната полиция координира международното сътрудничество на полицейските органи в различните страни в борбата с криминалната престъпност. Седалището на Интерпол е в Лион, Франция.

Източник: *Giliman, L., M. Joyce. Managing the Risk of Fraud in Unbank Mobile Money, The MMU programme in supported by the Bill & Melinda Gates Foundation, The MasterCard Foundation and Omidyar Network, p. 3-4.*

Дотук примерите доказаха потребността от дигитални компетенции. Те не са фундамента обаче на одиторската професия. За пример поради недобра финансова политика може да послужи фалиралото дружество – *„Wirecard”.* Според *Reuters* дружеството е известно като една от топ компаниите в класациите на борсата **DAX** (индекс на фондовата борса). Само че одиторите от *E&Y* Германия установяват сериозни нарушения за фалшифицирани финансови резултати. Според одиторите това е сложна глобална измама, която струва около 4 милиарда долара. По време на одита одиторите са получили фалшиви потвърждения на ескроу сметки. За това е докладвано на компетентните органи. От тяхна страна е обещано да бъдат предприети промени по отношение на упражнявания надзор в Германия над *ДЕП.*

Изправени сме пред редица предизвикателства, едно от тях са електронните пари. За да бъде още по-прецизирано, обществото е изправено пред предизвикателството, наречено *„информационна сигурност”*. Тази цел може да бъде постигната със стратегически подход – обединяване на усилията и сътрудничеството между държавния апарат, оперативните органи, потребителите и одиторите, като неизменна част, която защитава обществените интереси. В следващата точка ще се разгледат някои основни проблематични области за *ДЕП.*

4. КЛЮЧОВА ОБЛАСТ ЗА ОДИТА НА ДЕП

Всяка индустрия има специфика и ключови области за одитиране, за които е нужно да се вложи повече време за работа от стандартното. Без да се претендира за изчерпаемост на изследването, може да се отрази, че *ДЕП* са дружества от ново поколение и е нужно да се акцентира върху **най-съществената и специфична област** – ***„Дигитално управление и информационна сигурност“***. В тази област могат да се извършат процедури относно: *проверка на организацията и мениджмънта, информационна среда, правила и процедури, управление на достъпа.*

За целите на изследването ще бъдат разгледани **четири тематични групи**, които са нетрадиционни за одита като цяло, но са приоритетни за одита на *ДЕП.* Ще се поставят акценти кое е важно да се изследва за всяка една от групите.

За ***група № 1 „Проверка на организацията и мениджмънта“*** е нужно да се установи:

1. кой осъществява функциите за разработване и поддържане на внедрените ИТ системи;
2. по какъв начин се подсигурява сигурността на приложните ИТ системи;
3. проверка на организационната структура;

4. използват ли се информационните системи и канали от други дъщерни дружества;
5. проверка на функционалностите на всяка ИТ система;
6. как и кой извършва поддръжката на системите;
7. какви процедури по преглед и актуализация се извършват.

Група № 2 „Информационна среда на ДЕП“:

1. колко на брой и какъв вид са работните станции в организацията;
2. какви мерки за защита са предвидени;
3. какви са начините за съхранение на информацията;
4. по какви технологии е реализирана системата в ИТ инфраструктурата (напр. класическата клиент-сървър, със съхраняване на данни в релационна база данни), на какъв език са написани (напр. transact SQL (T- SQL, диалект SQL 2008 за сървърната, Microsoft Windows XP или Microsoft Windows 7 и език на управление C# за клиентската).

Група № 3 „Правила и процедури“:

1. създадени ли са достатъчно на брой и обхват политики, уреждащи дейността на информационните системи;
2. задълженията на заетите лица с информационната сигурност включват ли задължения по програмиране или управление на ИТ услуги и други.

Група № 4 „Управление на достъпа“:

1. видове данни за вход;
2. видове пароли за достъп;
3. хардуерни системи за вход;
4. цифрови сертификати;
5. защитни стени;
6. периодичен преглед за прониквания в системата.

Всяка една от групите е изключително специфична и различна от познатите към момента. Могат да бъдат прилагани различни тестове и процедури. Липсата на методология и стандарт за одитиране на ***ДЕП*** налага разгръщане на креативността от страна на одиторите. Затова в следващата точка ще се представи как се развива одиторската професия за периода от 1970 до 2020 година. Освен това ще се отдаде значение на дигитализацията и иновациите в одита.

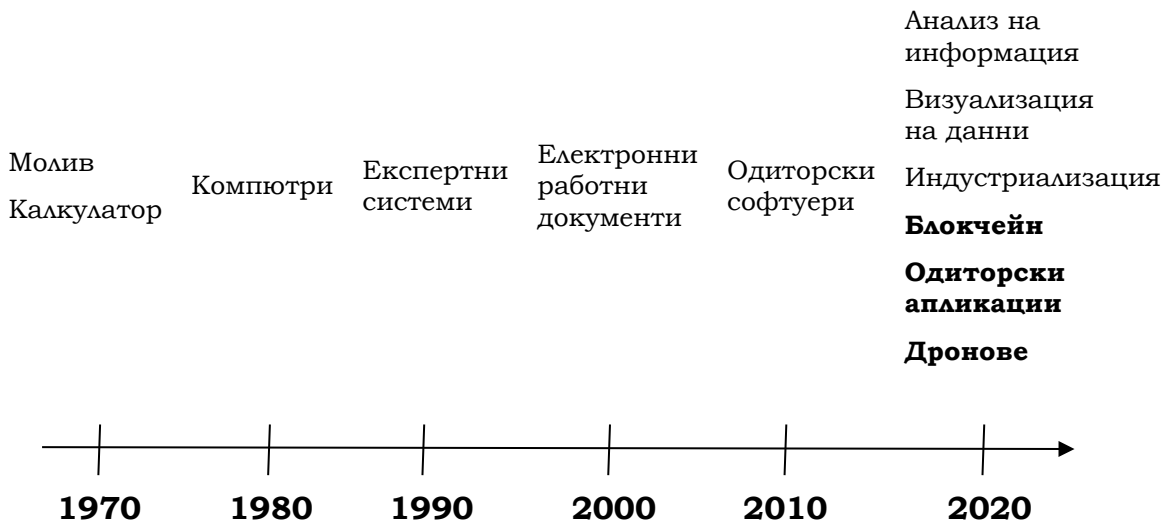
5. ДИГИТАЛИЗАЦИЯ НА ОДИТОРСКАТА ФУНКЦИЯ

Приоритет е да бъдат прилагани иновативни методи и подходи в одиторската професия, за да бъдат защитени обществените интереси.

„Същевременно технологиите са предизвикателство, особено за" (Динева, 2020: с.441) одиторите. Индустриалната революция промени света, както и одита, не е това, което е бил. Изцяло дигитализираните одиторски досиета откриват нови хоризонти. Разширяват се чрез интегрирането на нови интелигентни системи, чрез блокчейн технологиите, облачното пространство и апликациите. По този начин прозрачността на отчетността се подобрява и най-важното, спестява се време.

На следващата фигура ще бъде представена линия на времето. Върху нея са представени промените в одиторската професия за периода от 1970 до 2020 година. По-конкретно, онагледени са пособията, които одиторите използват в диапазона от последните 50 години до днес.

Фигура № 1. Линия на времето за одиторски ориентираните технологии



Източник:*Dai, J. Three Essays on Audit Technology: Audit 4.0, Blockchain, and Audit APP, Rutgers, The State University of New Jersey, Newark, New Jersey, 2017, p. 2*

В рамките на 50 години се наблюдава как одитът от ръчен, на хартиен носител, се измества към компютърните технологии и дигитализацията. Важно е да бъдат интегрирани иновациите и в тази професия. В тази линия може да говорим за **одита от 4-тата индустриална революция**.

Така наречения „**одит 4.0**"[22] е ангажиран с трансформацията за събирането на доказателства и съхраняването на информацията. В своя дисертационен труд **Jun Dai** е изследвал точно тези иновативни подходи. Фокусът се поставя върху ***автоматизацията на процесите***.

От ниво *Microsoft Office* вече преминаваме в по-бърз или улеснен процес чрез ***ERP системите.*** Само че координирането чрез иновации на вътрешноконтролната среда не е достатъчно. Всеизвестен факт е, че

[22] Одит от ново поколение. Индустриална революция 4.

световноизвестните одиторски компании в цял свят (big 4) разполагат с тези софтуери. Модерният одит налага използването на тези технологии, както например в дружествата за електронни пари. Немислимо е да се проследят и изведат всички трансакции, но чрез дигиталните приложения това е напълно възможно.

За пример може да се представи и ***Бенфорд***[23] ***теста.*** Той служи за отчитане на грешки и измами в големи извадки. Открива промяната на данни в популацията. Ако се открие грешка/измама, е задължително да се приложат аналитичнии процедури, за да се установи причината, (необичайни трансакции, слабости във вътрешния контрол). Този тест се използва за финансово-счетоводни цели още от 1972 година. За този период от време генерирането на данни се е увеличило многократно.

Събирането, обработката и анализа на голям масив от данни не е никак лесна задача. Затова „умните технологии" могат да подпомогнат одиторите в тази дейност. Нужно е да се помисли на корпоративно ниво. Например всеки един институт на дипломираните експерт-счетоводители по света би могъл да осигури прототипен софтуер, който да бъде надграждан и модифициран спрямо нуждите на одита.

В началото на изследването се спомена за революционната блокчейн технология на криптовалутата. Тя може да се използва в различни направления – застраховане, банкиране, лизинг и други. ***Разработена е концепция, че тази технология може да бъде от полза и за одита и съхраняването на документацията***.

Поради чувствителността на информацията и значителния ѝ размер блокчейн технологията се установява като изключително подходяща. В допълнение е икономична заради липсата на такси и децентрализация. Освен това е сигурна поради криптираната информация.

За да бъдат минимизирани рисковете от злоупотреби, могат да бъдат сключени *„интелигентни договори"*[24]. В случая ще бъдат проследими всички трансакции и потребители. Чрез предварително заложена клауза в договора с компанията, която разработва/урежда услугата, може да бъде постигната тази цел.

Тези нови парадигми в одиторската професия са в синхрон със средата. На европейско ниво също се разработва проект в тази насока. Нарича се *„Digital audit"*, а на български може да се назове като ***„дигитален одит"***. Съответно се отдава значение на проверката на дигитализацията в една институция.

Не се имат предвид инспекциите към ИТ контролите, поддръжката на софтуерните системи, нито одитът на финансовите отчети в едно дружество. Важно е да се разграничат тези три направления на одиторската функция. Разработена е концепция, насочена към съвременните компании.

Съгласно изследването на **Мирослава Пейчева** приоритет за всяка една компания е имплементирането на ***киберкултура***. Това е културата,

---

[23] Програма, която подпомага одиторите в разкриването на измами. Синтезиране на информацията от Excel.

[24] Развитие на блокчейн технологията. Интелигентните договори (от англ. език – Smart Contracts) са самоизпълняващи се договори, като условията на споразумението между купувача и продавача се записват директно в кодови редове.

„възникнала от използването на компютърни мрежи за бизнес, комуникация и забавление“ (Peicheva:2019, p.59). Тази култура е нужно да се пренесе като държавна политика.

В изследването *„Big Data and Digital Audit“* са отразени тези иновативни специфики и неограничения на одита. Посочено е, че е необходимо да се използват усъвършенствани техники като извличане на данни от софтуерни роботи. Създава се промяна в обекта на одита, както и в техниката, защото старите методи вече не са подходящи.

Разработеният пилотен проект от ***European Court of Auditors*** създава профилирани групи, като една от тях се насочва изцяло към изкуствения интелект и автоматизацията на процесите в този сегмент. Насоката от ЕК е същият да бъде приложен в държавния апарат – *The Digital Agencies Audit Project.*

Следователно тази вълна ще продължи и в частният сектор. *ДЕП* може да се счете като причина за създаването на подобни институции. Защото вече не е приоритет единствено финансовата информация. За съжаление, с високотехнологичното развитие има индикации за манипулиране на данните по технологичен път. А това е трудноустановимо, ако не притежаваш компетенции в тази област.

Изпитва се потребност от създаването на нови правила и норми по отношение на инспекциите в тази сфера. Одиторите не са ИТ специалисти и не е техен ангажимент да извършват цялостна проверка на софтуери. ИТ одитът е изключително полезен, но той също не би могъл да се сравни до основи със софтуерните специфики на едно ***ДЕП***.

Към момента нито един държавен орган няма тези правомощия и компетенция. БНБ регулира финансово-счетоводната политика, МВР (ГДБОП, отдел „Киберпрестъпност“) извършва разследвания и пресичане на киберпрестъпленията. ДАНС също подпомага и действа в тази насока. Въпреки това е крайно недостатъчно за компании, които се занимават с виртуални валути.

Липсата на ***стандартизация*** за ДЕП в посока към ИТ частта крие множество рискове на транснационално ниво. За да се разрешат тези слабости, е необходим голям финансов и експертен ресурс. Основата е важно да бъде изградена от правилната политика, да се изследва практиката и да се имплементират правилните методи. Това е осъществимо само с добро регулиране, чрез коректно разписани законови рамки. Най-важното е – ИТ специалисти с етични принципи.

ЗАКЛЮЧЕНИЕ

Вследствие на проведеното изследване е явно развитието, насочено към дигитализацията, което е нужно да бъде съобразено и от одиторите в техните практики. Могат да бъдат обобщени следните по-важни **изводи**:

- ✓ ***Разграничиха се ключови понятия*** като термина ***„електронни пари“ (ДЕП)*** от всички останали видове валути.
- ✓ ***Липсва критичен фокус над законовата рамка на ДЕП*** – към този момент се изпитва силна потребност от промяна и актуализация на одиторската методология във връзка с одитирането на ДЕП.

Прехвърлянето на отговорности от страна на ДАНС към одиторите не е най-рационалният подход във връзка с противодействието на изпиране на пари. Причината е липсата на юридическа компетенция спрямо наказателно-правните науки. Одиторската работа генерално променя фокуса си на действие през последните години.

- ✓ ***Чрез инициране на законодателна реформа е приоритет да бъде включен като допълнителен участник в одиторския екип*** – ИТ специалист, който да съдейства за целите на одита на ДЕП.
- ✓ ***Дигитализацията на одиторското досие*** – притежава положителни и отрицателни характеристики. Високотехнологичното развитие на света няма как да подмине и тази професия. Само че доколко е сигурна тази технология?

Дори „създаването на различни дигитални решения за оптимизиране на бизнеса се възприема и от страна на държавните органи и институции“ (Георгиева, 2019: с. 38). Фактът, че държавният механизъм има сериозни пропуски в това отношение, е явен от кибератаките към **ТР** през 2018 година, а след това и с тези към **НАП**. Липсата на защита към личните данни на обществото дава индикации за сериозни недостатъци. Необходима е промяна по отношение на сигурността на данните както в държавния сектор, така и в частния. От страна на одиторите е добре да бъдат предприети контрамерки спрямо защитата на информация на техните клиенти, да се включват в одиторските екипи ИТ специалисти, спрямо нуждите и характера на ангажимента, както и да се актуализират и усъвършенстват методологиите на документация при преминаването към софтуерни одиторски продукти.

Библиографска справка:

1. *Вейсел, А. (2018). Счетоводни аспекти на криптовалутите, Дигитални измами и киберсигурност (Първа международна научно-практическа конференция). София: ИК-УНСС.*
2. *Георгиева, Д. (2019). Дигиталните компетенции на счетоводителите в контекста на четвъртата индустриална революция, Икономика 21, бр. 2/2019.*
3. *Динева, В. (2020) Онлайн обучението по вътрешен контрол и вътрешен одит – сбъдната реалност. (Юбилейна международна научна конференция: Икономическа наука, образование и реална икономика: развитие и взаимодействие в дигитална епоха, Том V). Варна: Наука и икономика.*
4. *Директива 2009/110/ЕО на Европейския парламент и на Съвета от 16 септември 2009 година относно предприемането, упражняването и пруденциалния надзор на дейността на институциите за електронни пари и за изменение на директиви 2005/60/ЕО и 2006/48/ЕО, и за отмяна на Директива 2000/46/ЕО, Страсбург, 16 септември 2009.*
5. *Директива (ЕС) 2018/843 на Европейския парламент и на Съвета от 30 май 2018 година за изменение на Директива (ЕС) 2015/849 за предотвратяване използването на финансовата система за*

целите на изпирането на пари и финансирането на тероризма и за изменение на директиви 2009/138/ЕО и 2013/36/ЕС.

6. *Закон за кредитните институции, приет от XL Народно събрание на 13 юли 2006 г., обн., ДВ, бр. 59 от 21 юли 2006 г., посл. изм., ДВ, бр. 64 от 2020 г.*
7. *Закон за платежните услуги и платежните системи, приет от 44-тото Народно събрание на 22 февруари 2018 г, обн., ДВ, бр. 20 от 6 март 2018 г., посл. изм., ДВ, бр. 13 от 2020 г.*
8. *Наредба № 16 на БНБ от 29 март 2018 г. за издаване на лицензи и одобрения, за вписване в регистъра по чл. 19 от Закона за платежните услуги и платежните системи и за изискванията към дейността на операторите на платежни системи с окончателност на сетълмента (Обнародвана в „Държавен вестник“, бр. 32 от 13 април 2018 г.; посл. изм., ДВ, бр. 38 от 2020 г.)*
9. *Насоки относно информацията, която се предоставя за лицензирането на платежни институции и институции за електронни пари и за регистрацията на доставчици на услуги по предоставяне на информация за сметка съгласно член 5, параграф 5 от Директива (ЕС) 2015/2366, EBA/GL/2017/09 08/11/2017.*
10. *Николов, П. (2017). Обмен и анализ на информация в Европол. София: Авангард Прима*
11. *Регламент (ЕС) № 1093/2010 на Европейския парламент и на Съвета от 24 ноември 2010 година за създаване на Европейски надзорен орган (Европейски банков орган), за изменение на Решение № 716/2009/ЕО и за отмяна на Решение 2009/78/ЕО на Комисията (ОВ L 331, 15.12.2010 г., стр. 12).*
12. *Янев, Р. (2011). Противодействие на изпирането на пари. София: Академия на МВР.*
13. *Berentsen, A. Monetary Policy Implications of digital money, University of Bern, 1997.*
14. *Big data and digital audit, Journal No 1, 2020, European Court of Auditors, Luxemburg.*
15. *Chaum, D. Untraceable Electronic Mail, Return Addresses and Digital Pseudonyms, Technical Note Programming Techniques and Data Structures, February 1981, Volume 24.*
16. *Directive (EU) 2015/849 on preventing the use of the financial system for money laundering or terrorist financing (4th anti-money laundering Directive).*
17. *Electronic Code of Federal Regulations (e-CFR) Title 31. Money and Finance: Treasury Subtitle B. Regulations Relating to Money and Finance Chapter X. FINANCIAL CRIMES ENFORCEMENT NETWORK, DEPARTMENT OF THE TREASURY Part 1010. GENERAL PROVISIONS Subpart A. General Definitions Section 1010.100. General definitions*
18. *European Central Bank, Virtual currency schemes – a further analysis, February 2015, ISBN 978-92-899-1560-1.*

19. *Financial Conduct Authority, The FCA`s role under the Electronic Money Regulations 2011, June 2013.*
20. *FinTech, Implementing a CBDC: Lessons Learnt and Key Insights Policy Report, Central Bank Digital Currencies Working Group, October 2020, CEMLA.*
21. *Peicheva, M. (2019). SOFT SKILLS IN THE CENTER OF THE CYBERCULTURE. Journal Association Spike, edition 24, June, 2019.*
22. *Study on an EU initiative for a restriction on payments in cash,Center for European Policy Studies, European Commission, Brussels, December, 2017.*
23. *Uniform Money Services Act, National Conference of Commisioners on Uniform State Laws, Approved and Recommended for Enactment in all the States, Annual Conference Meeting in its One-Hundred-and-Ninth Year, St. Augustine, Florida, July 28 – August 4, 2000.*
24. *A digital Euro, <https://www.ecb.europa.eu/euro/html/digitaleuro.en.html> last available on: 15.11.2020.*
25. *Payment Fraud<https://www.europol.europa.eu/crime-areas-and-trends/crime-areas/forgery-of-money-and-means-of-payment/payment-fraud> last available on: 15.11.2020.*
26. *E-money service scam expands to five other operators, Kyodo, Jiji, 16 September 2020, <https://www.japantimes.co.jp/news/2020/09/16/business/e-money-service-fraud/> last available on: 15.11.2020.*
27. *DISCLOSURE GUIDANCE AND TRANSPARENCY RULES SOURCEBOOK (ELECTRONIC REPORTING FORMAT) INSTRUMENT 2020, By order of the Board 22 October 2020, <https://www.handbook.fca.org.uk/instrument/2020/FCA_2020_65.pdf> last available on: 15.11.2020.*
28. *The money`s gone: Wirecard collapses owing $ 4 billion, Schuete, A., O`Donnell, J., June 25, 2020/11:39 AM<https://www.reuters.com/article/us-wirecard-accounts-idUSKBN23W176> last available on: 15.11.2020.*
29. *Investor Alert: Bitcoin and other Virtual Currency – Related Investments, May 7, 2014, <https://www.sec.gov/oiea/investor-alerts-bulletins/investoralertsia_bitcoin.html> last available on: 15.11.2020.*
30. *Difference between cryptocurrency, virtual currency and digital money, <https://steemit.com/bitcoin/@danielvepa/difference-between-cryptocurrency-virtual-currency-and-digital-money> last available on: 15.11.2020.*