

<https://doi.org/10.70265/NKYH9976>

СИГУРНОСТ НА Е-ДОСИЕТА С БЛОКЧЕЙН

Теодора Личева

SECURITY OF E-FILES WITH BLOCKCHAIN

Teodora Licheva

Резюме: Изследването разглежда приложението на блокчейн технологиите в създаването и управлението на електронни досиета за информационна сигурност. Анализират се основните предимства като децентрализация, криптографска защита и прозрачност на данните. Разгледани са практическите приложения в различни сектори – държавна администрация, образование, здравеопазване и финансов сектор. Обсъдени са техническите предизвикателства като скалируемост, криптографски уязвимости и управление на достъпа, както и съответните мерки за сигурност. Представени са стратегии за внедряване и оптимизация на блокчейн базирани системи за електронни досиета, които осигуряват високо ниво на защита и оперативна ефективност.

Ключови думи: блокчейн технология, електронни досиета, информационна сигурност, криптографска защита, децентрализирани системи

Summary: The research examines the application of blockchain technologies in creating and managing electronic records for information security. It analyzes key advantages such as decentralization, cryptographic protection, and data transparency. Practical applications across various sectors are explored – public administration, education, healthcare, and financial sector. Technical challenges including scalability, cryptographic vulnerabilities, and access management are discussed, along with corresponding security measures. Strategies for implementing and optimizing blockchain-based electronic record systems are presented, ensuring high levels of protection and operational efficiency.

Keywords: blockchain technology, electronic records, information security, cryptographic protection, decentralized systems

УВОД

През последните години технологиите, свързани с блокчейн, стават все по-важни за сферата на информационната сигурност. Едно от най-обещаващите им приложения е създаването и управление на

електронни досиета, които предлагат иновативни решения за прозрачност, неизменяемост и децентрализация. Това изследване разглежда задълбочено потенциала на блокчейн технологиите при формирането на цялостни системи за създаване и поддържане на електронни досиета, анализира заплахите, уязвимостите, мерките за сигурност и практическия опит от внедряването в различни сектори. Проучването е всеобхватен анализ на преимуществата и предизвикателствата, с който да се гарантира сигурна информационна инфраструктура за съхранение и управление на данни (Личева, 2022а).

Основната цел на изследването е да разгледа в детайли потенциала на блокчейн технологията при създаването и управлението на електронни досиета, като представи изчерпателен анализ на преимуществата и предизвикателствата. Стремешът е да се предложи сигурна информационна инфраструктура за съхранение и управление на данни в различни сектори. Използваната методологията включва:

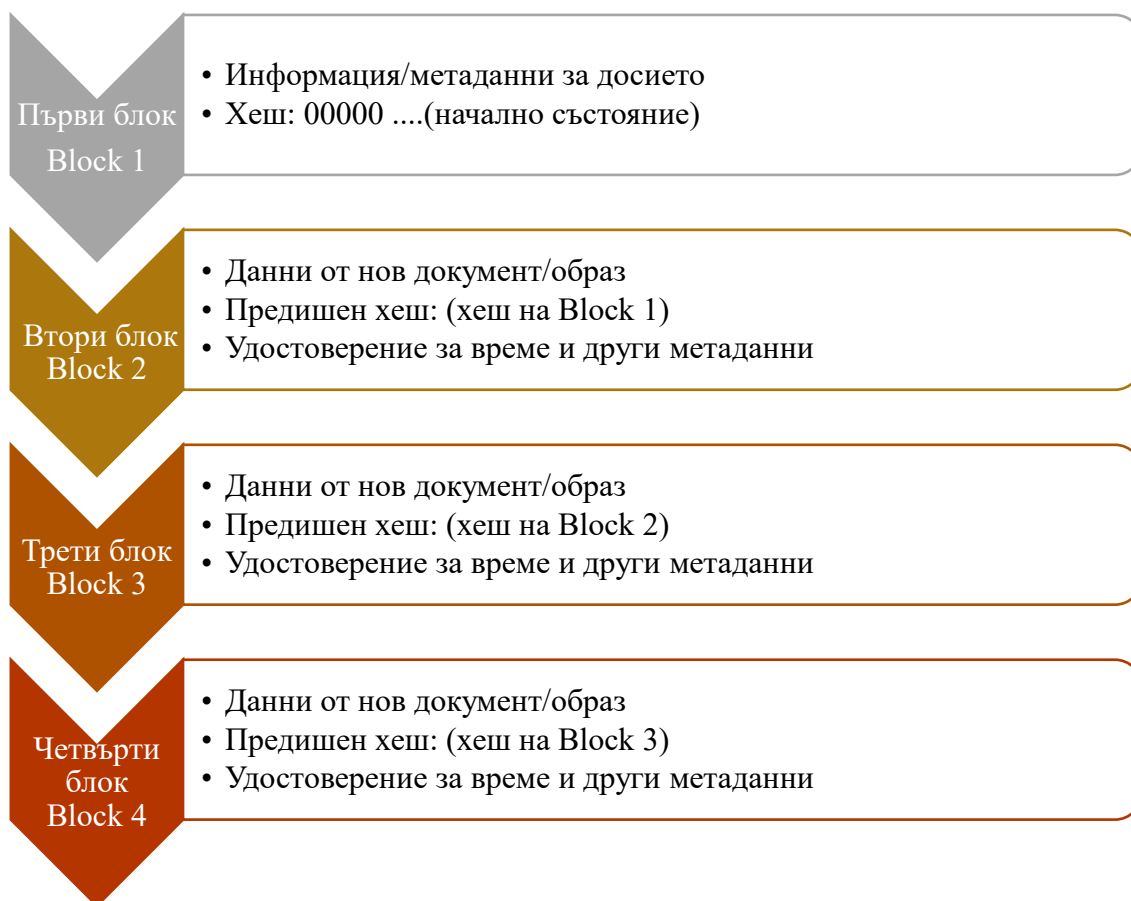
- Анализ на предимства;
- Изследване на практическите приложения;
- Разясняване на технически предизвикателства;
- Представяне на стратегии за внедряване и оптимизация.

Обектът на изследването е внедряване на блоковата верига, като допълнителен слой за сигурност, в информационната сигурност и управлението на електронни досиета.

Предмет на изследването е анализът на техническите и организационни аспекти, свързани с използването на блокчейн технологии за гарантиране на сигурност, прозрачност и ефективност в управлението на електронни досиета.

1. ХАРАКТЕРИСТИКА НА БЛОКЧЕЙН ТЕХНОЛОГИИТЕ

Блокчейн е децентрализирана и неизменяема цифрова книга, която съхранява данни чрез последователно свързани блокове. Всеки блок съдържа криптографски подпис (хеш), който гарантира автентичността и целостта на записаната информация (Личева, 2022b). Основните принципи включват децентрализация, прозрачност, сигурност чрез криптография и консенсусни алгоритми, които предпазват от неоторизирана манипулация (Личева, 2022c).



Фигура 1. Схематично представяне на технологията блокчейн

Първоначално блокчейн технологията стана известна с появата на криптовалутата Биткойн, но с течение на времето нейното приложение се разширява и извън сферата на финансите. Сегашните приложения включват електронно управление на данни, проследяване на веригата на доставки, здравеопазване и разбира се, създаването на електронни досиета (Личева, 2023а). Тази еволюция е продиктувана от нуждата за подобрена сигурност и намаляване на зависимостта от централно управлявани системи (Florkin, 2024).

2. ХАРАКТЕРИСТИКИ НА ЕЛЕКТРОННИТЕ ДОСИЕТА

Електронните досиета представляват дигитални архиви на информация, които се управляват с помощта на компютърни системи. Те предлагат редица предимства пред традиционните хартиени досиета, като бърз достъп, възможност за автоматизация и по-висока степен на сигурност благодарение на технологията за криптиране (Kejriwal, 2023). Основните предимства, свързани с електронните досиета, са:

- **Непроменяемост:** След като данните са записани, те не могат да бъдат променени без да оставят следа за това;

- **Проследимост:** Всяка транзакция или промяна е отразена с точен времеви маркер и идентификатори, което позволява пълна проследимост;

- **Достъпност:** Достъпът до данните може да бъде контролиран чрез криптографски ключове и други мерки за сигурност, намалявайки риска от неоторизиран достъп.

Електронните досиета, управлявани чрез блокчейн, предоставят няколко основни предимства в сферата на сигурността:

- **Децентрализирано управление:** Разпределението на данните сред множество възли добавя допълнителен слой на защита срещу атаки, като елиминира централизирани точки на уязвимост;

- **Криптографска защита:** Използването на съвременни криптографски алгоритми предпазва от неоторизирано изменение и осигурява автентичност на данните;

- **Висока проследимост:** Всеки запис е обвързан с уникален цифров подпис, който прави манипулациите практически невъзможни (EITCA, 2024).

3. АСПЕКТИ И НАДГРАЖДАНЕ НА ЕЛЕКТРОННИТЕ ДОСИЕТА ЧРЕЗ БЛОКЧЕЙН

При интегрирането на блокчейн в системите за електронни досиета се включват следните компонента:

- **Децентрализирана мрежова инфраструктура:** Данните се съхраняват върху разпределена мрежа от възли, което елиминира потребността от централен сървър;

- **Интелигентни договори:** Тези самоизпълняващи се кодови модули управляват логиката на записа и проверката на данните, като осигуряват автоматично изпълнение на зададените условия (Дочева, 2024);

- **Криптографски алгоритми:** За защита на данните се използват алгоритми като SHA-256, които гарантират непроменяемостта на записите (EITCA, 2024);

За предприятия и организации, които вече имат информационни системи, интеграцията с блокчейн може да бъде постигната чрез използване на API-та, мостове и други междинни слоеве, които позволяват синхронизиран обмен на данни между централизирани и децентрализирани системи. Тези интеграционни технологии осигуряват плавен преход и гарантират, че новата система подсилва съществуващите мерки за сигурност, без да нарушава оперативната ефективност (Личева, 2023а).

За да бъдат технологиите реализирани ефективно, международни организации и регулатори се стремят да определят стандарти за използването на блокчейн в електронните досиета. Стандарти като

ISO/TC 307 са насочени към разработването на рамка за сигурност, управление на данни и оперативна устойчивост, базирана на блокчейн решения (Florkin, 2024). Също така, стандартите гарантират, че различни системи могат да комуникират помежду си при спазване на високите изисквания за сигурност (Kejriwal, 2023).

4. ПОЛЗИ ОТ ИЗПОЛЗВАНЕТО НА БЛОКЧЕЙН ЗА Е-ДОСИЕТА

- **Подобряване на целостта и сигурността на данните**

Блокчейн предоставя невъзможност за неоторизирани модификации на записите, тъй като всяка промяна изисква консенсус от всички възли в мрежата. Този децентрализиран модел намалява риска от вътрешни и външни заплахи, като прави атаките, като например 51% атаки, значително по-трудни за осъществяване (Личева, 2023b). При електронните досиета това означава, че прозрачността и автентичността на данните са гарантирани на всяко ниво (Дочева, 2024).

- **Намаляване на риска от измами и корупция**

При традиционните централни системи за съхранение съществува възможност за манипулация на данни и измами от страна на служители или външна намеса. Използването на блокчейн елиминира този риск, тъй като данните се записват по начин, който не позволява обратимо изменение. Това е от ключово значение за електронните досиета, които често съдържат чувствителна и критична информация (ЕИТСА, 2024).

- **Повишаване на оперативната ефективност**

Премахването на посредници и осигуряването на автоматизация чрез интелигентни договори води до значително намаляване на времето за обработка на транзакции и управление на данни. Това позволява на организациите да се фокусират върху анализа и използването на данните, вместо върху административни и рутинни задачи, свързани с ръчното въвеждане и верификация (ЕИТСА, 2024).

- **Гарантиране на съответствие със законодателството**

Въведението на регулации, свързани с поверителността и сигурността на данните (като GDPR¹ в Европейския съюз), поставя високи изисквания към управлението на електронните досиета. Блокчейн системите могат да подпомогнат спазването на тези регулации чрез осигуряване на проследимост и неизменяемост на данните, което улеснява одита и вътрешните проверки.

5. СЕКТОРИ НА ПРИЛОЖЕНИЕ

- **Държавния сектор и административни услуги**

¹За повече информация виж: Регламент (ЕС) 2016/679 относно защитата на физическите лица във връзка с обработването на лични данни и относно свободното движение на такива данни (GDPR).

Държавните институции използват блокчейн за създаване на електронни досиета, свързани с граждански регистрации, издаване на разрешителни и други публични услуги. Тези решения увеличават доверието на гражданите в административните процеси, като предоставят надеждна и проследима документация, която е защитена от нерегламентирана намеса (Kejriwal, 2023). Това е от особено значение за борбата с бюрокрацията и подобряването на ефикасността на публичните услуги, като същевременно гражданите имат възможност да проверят автентичността на документите в реално време.

• **Образование**

В сферата на образованието електронните досиета, базирани на блокчейн, се използват за издаване и проверка на дипломи и сертификати. Университетски програми, които използват тази технология, позволяват работодателите да потвърдят автентичността на квалификациите директно през цифрова платформа, намалявайки риска от фалшифицирани документи. Това подобрява както качеството на образованието, така и доверието в академичните институции. Спестява време и разходи, както за кандидатстване за стажове и практика, така при поискване от бъдещ работодател.

• **Здравеопазване**

В здравеопазването електронните досиета са от критично значение за управлението на пациентски данни, история на медицински прегледи, епикризи и рецепти. Блокчейн технологията гарантира сигурно споделяне на информация между болници, лаборатории и застрахователи, като същевременно запазва пълната проследимост и неизменяемост на данните. Това позволява по-бърза диагностика, намалява административните грешки и подобрява цялостната грижа за пациента (Личева, 2023а).

• **Финансов сектор**

Финансовата индустрия е сред първите сектори, които адаптират блокчейн технологиите, благодарение на способността им да осигурят сигурност и прозрачност за транзакции. Електронните досиета, управлявани чрез блокчейн, са използвани за съхранение на информация за банкови операции, застрахователни полици и други ключови финансови данни. Това предоставя допълнителна защита срещу измами и фалшификации, гарантирайки, че всяка финансова транзакция може да бъде проверена и проследена (Костов, 2025).

• **Управление на веригите за доставки**

В логистиката и управлението на веригите за доставки, блокчейн осигурява нов начин за проследяване на движението на стоки и материали. Електронните досиета в тази сфера документират всички стъпки от производството до крайната дестинация, което улеснява идентифицирането на уязвимости в процеса и предотвратява

измамите(Личева, 2023b). Тази технология значително повишава прозрачността и намалява риска от загуби и несъответствия.

6. ТЕХНИЧЕСКИ ПРЕДИЗВИКАТЕЛСТВА И МЕРКИ ЗА СИГУРНОСТ

При внедряването на блоковите вериги в създаване на нови досиета или цифровизиране на вече съществуващи досиета (т.нар.наследствени) е необходимо да се обърне внимание на следните предизвикателства:

Скалиране на блокчейн мрежите

Едно от основните технически предизвикателства пред внедряването на блокчейн системи за електронни досиета е скалирането. Повече участници и по-голям обем от данни могат да доведат до забавяния при обработката на транзакции и увеличаване на разходите за изчислителни ресурси. За да се решат тези проблеми се предлагат решения като използване на вторични мрежи (sidechains), офчейн транзакции и оптимизирани консенсусни алгоритми (Florkin, 2024). Тези мерки позволяват по-гъвкаво управление на ресурсите и осигуряват ефективно разпределение на натоварването в системите.

Криптографски уязвимости

Извършването на атаки върху криптографските алгоритми, използвани в блокчейн системите, представлява сериозна заплаха за електронните досиета. Възможни атаки като 51% атаки, атаки чрез квантови изчисления или слабости в конкретни алгоритми могат да компрометират сигурността на данните. За да се справят с тези заплахи, се препоръчва да се въведат следните дейности:

- Редовен одит на криптографските протоколи;
- Прилагане на хибридни модели за консенсус;
- Инвестиране в нови и устойчиви алгоритми, като квантово-устойчиви решения (Костов, 2025).

Управление на достъпа и автентикация

За системи с е-досиета е от съществено значение да бъде осигурено правилно управление на достъпа. Използването на многофакторнаавтентикация, ролеви контрол на достъпа и криптографски ключове са с решаваща роля за предотвратяването на неоторизиран достъп. За да се решат тези предизвикателства е необходимо да се използват хардуерни сигурни модули за съхранение на ключове, което значително намалява риска от компрометиране (Личева, 2023b).

Намалена латентност и запазване на производителност

При мащабни системи, в които електронните досиета трябва да бъдат достъпни в реално време, латентността в мрежата и ограниченията в скоростта на обработка могат да възникнат като

проблем. Оптимизацията на протоколите, презентирането на механизми за компресиране на данните и използването на приложения с ниска латентност са ключови фактори за справяне с този проблем (EITSA, 2024).

7. ПРАВНИ И ЕТИЧНИ ПРЕДИЗВИКАТЕЛСТВА

Все по-бързото и динамично развитие на новите технологични възможности води до навлизането им във всички сфери на общественоекономическия живот, което трябва да доведе и до повишаване на правната култура на гражданите (Lyubenov, 2024). Законово-нормативната уредба за регламентираното им използване обаче изостава чувствително и поражда следните предизвикателства:

Съответствие със законодателството

Въвеждането на блокчейн за управление на електронни досиета поставя въпроси, свързани със спазването на регулаторни изисквания като защита на личните данни и поверителност. Регулации като GDPR изискват, данните да бъдат обработвани прозрачно и с гарантиране на правата на субектите. В този контекст, неизменяемостта на данните, която предлага блокчейн, има двустранен смисъл – от една страна тя улеснява одита, а от друга страна може да затрудни изтриването на лични данни (Kejriwal, 2023).

Етични аспекти и общественото доверие

От гледна точка на етиката, управлението на чувствителни данни чрез блокчейн изисква висока степен на прозрачност и отговорност. Докато технологията може да предотврати измами и корупция, тя също така изисква ясна политика за това кой има достъп до данните и как се използват. Осигуряването на общественото доверие и приемане на системите се постига чрез прозрачни алгоритми, публични одити и активно участие на заинтересованите страни. Прозрачността в дейностите по събиране, обработка и съхраняване на чувствителните данни ще върне доверието на гражданите в административните процеси.

Правни казуси и съдебна практика

В някои страни вече са установени правни стандарти за използването на блокчейн технологии в административните и финансовите сектори. Тези стандарти, макар и в ранните им етапи, предлагат насоки за това как електронните досиета да бъдат използвани в съдебна и административна практика. Правните казуси поставят въпроси относно доказуемостта и автентичността на данните, което прави ясното дефиниране на правата и отговорностите изключително важно (EITSA, 2024).

8. ИНОВАТИВНИ МОДЕЛИ И БЪДЕЩИ НАСОКИ

Развитието на технологичните системи търпи постоянно усъвършенстване с основна цел да се подобри сигурността в създаването и използването на е-досиетата.

Развитие на интелигентните договори

Една от областите на развитие е усъвършенстването на интелигентните договори, които управляват системитена записите в блоковата верига. Новите модели за интелигентни договори се стремят да предложат по-динамични, адаптивни и сигурни решения, които могат автоматично да се актуализират според променящите се изисквания и регулации. Тези модели включват използването на оркестрирани модулни архитектури и интеграция с други блокчейн платформи (ЕІТСА, 2024).

Хибридни модели на данни

За да се използват предимствата на децентрализираните системи и същевременно да се осигури висока производителност, много организации проектират хибридни модели, при които критичните данни се съхраняват в блокчейн, докато останалата информация остава в традиционни бази данни. Този подход позволява оптимално използване на ресурсите и повишена скалируемост, като същевременно се запазват сигурността и проследимостта (Личева, 2023b).

Връзка с Интернет на нещата (IoT)

Интеграцията на блокчейн с устройства от Интернет на нещата предлага нови възможности за създаване на сигурни и проследими електронни досиета. Устройствата могат автоматично да събират, криптират и изпращат данни в блокчейн мрежата, гарантирайки в реално време контрол и мониторинг на процесите. Този модел е от особено значение за индустриални приложения, където данните трябва да бъдат не само сигурни, но и налични в реално време (Florkin, 2024).

Приложения в цифровото управление на идентичността

Цифровата идентичност е друга област, където блокчейн предлага значителни подобрения. Чрез използването на електронни досиета за съхранение и верификация на лични данни, се елиминират рисковете от кражба на самоличност и измами. Този модел осигурява, че гражданите имат контрол върху собствените си данни и че достъпът до тях става само чрез одобрени процеси (Личева, 2024).

8.1. Примерна интегрирана система за създаване на електронно досие с блокчейн

Предложената интегрирана система е с основни задачи да събира, обработка и съхранява данните в електронното досие, като същевременно гарантира автентичност и цялост чрез технологията блокчейн. Е-досието може да съдържа официални документи,

административни данни или информация за конкретни случаи. Архитектурата е комбинация между традиционните информационно-комуникационни решения с иновативните блокчейн елементи. Така предложеното съчетание намалява административните грешки и повишава доверието в самите процеси.



Фигура 2. Примерна интегрирана система за създаване на е-досие с блокчейн технология

Системата обхваща следните ключови модули:

Потребителски модул

– Уеб-базирано или мобилно приложение за събиране на данни и управление на досието;

– Интерфейс за въвеждане, преглед и проверка на данните.

Модул за обработка и валидация

– Интерфейс към вътрешни административни системи за автоматично извличане и синхронизиране на данни;

– Използване на правила за валидация и предварителна обработка, преди данните да бъдат криптирани и подписани.

Блокчейн слой

– Мрежа от възли, които съхраняват криптографски подписани хешове на документите, гарантирайки истинността им;

– Включване на интелигентни договори за автоматизирано управление на процеси като одобрение, проверка на автентичност и проследимост на промените;

– Архивиране на доказателствени данни, които могат да се използват при одити и административен контрол.

Интеграционен слой

– API интерфейс за свързване с вече съществуващи системи за електронен обмен на документи или други информационни платформи;

– Интеграция с национални системи за електронно управление.

Система за управление на достъп и сигурност

– Модул за удостоверяване на самоличността и управление на достъпа до данните в досието;

– Криптографски механизми за защита на информацията във всяка стъпка от жизнения цикъл на досието.

Процесът по създаване и актуализиране на е-досието премивана през следните етапи:

Събиране на данни

– Потребителят или автоматични системи въвеждат данни чрез потребителския модул;

– Данните преминават процес на валидация и предварителна обработка.

Криптографско подписване и създаване на хеш

– Всеки нов документ или изменение в досието се подписва криптографски и се генерира хеш, който се изпраща към блокчейн слоя;

– Интелигентните договори проверяват дали данните отговарят на предварително зададените правила и условия.

Запис върху блокчейн

– Криптографския хеш и свързаните метаданни се записват в блокчейн системата, като се гарантира, че всички трансакции са проследими и непроменяни;

– Това е последната верификация от страна на одитори или външни институции за проверка.

Обработка и предоставяне на обратна връзка

– Потребителят и административните системи могат да следят статуса и движението на досието чрез специален интерфейс;

– Системата осигурява автоматично известяване при промени или неочаквани движения в системата, което ще спомогне за бърза реакция при необходимост.

Ползи и ключови аспекти на проекта

– Сигурност и прозрачност: използването на блокчейн технологията осигурява неизменяемите записи и повишава доверието в системата;

– Интегрирана комуникация: системата позволява лесно интегриране с други национални и административни системи, като подпомага електронното управление;

– Автоматизация чрез интелигентни договори: Автоматизираното управление на процесите намалява човешката грешка и ускорява административните процедури.

Така представеният проект включва изграждане на модулна архитектура, съчетаваща потребителски интерфейс, система за обработка на данни, блокчейн слой за неизменност на записите и интеграционен модул за свързване с други системи. Интелигентните договори и криптографската защита осигуряват високо ниво на сигурност и прозрачност, съответстващи на изискванията за цифрова трансформация в съвременните публични и частни услуги.

8.2. Сравнителен анализ на традиционните досиета ие-досиета базирани на блокчейн

• Традиционни централно управлявани системи

Традиционните системи за управление на електронни досиета най-често се базират на централизирани сървъри и бази данни, което ги прави податливи на вътрешни атаки, грешки в човешкия фактор и централизирани срывове. При тези системи се изискват допълнителни мерки за защита, като физически достъп и одиторски проверки, за да гарантират сигурността на данните(Личева, 2023b).

• Е-досиета с технологията блокчейн

Блокчейн базираните системи предлагат следните ключови предимства:

• **Децентрализация:** Разпределението на данните премахва централизирани точки на уязвимост.

• **Криптографска сигурност:** Данните са защитени чрез силни криптографски алгоритми, което ги прави изключително трудни за манипулация.

- **Проследимост и одит:** Всяка транзакция се записва публично, което улеснява проверката и бързо установяват грешките (EITSA, 2024).

8.3. Стратегии за внедряване и оптимизация

За да се постигне успешна интеграция на блокчейн системи за електронни досиета, организациите трябва да предприемат следните стъпки:

- Анализ на текущата инфраструктура и оценка на нуждите – определяне на критичните точки и установяване на изискванията за сигурност;
- Избор на подходяща блокчейн платформа – вземане на решение между публични, частни или хибридни блокчейн решения, необходими за нуждите и обхвата на проекта;
- Интеграция с вече съществуващи системи – използване на подходящи API и междинен софтуер, който свързва новите блокчейн решения с традиционните бази данни (EITSA, 2024);
- Внедряване на редовни одити и мониторинг – установяване на процедури за одит, наблюдение и бърза реакция при възникване на проблеми.

Успешното внедряване изисква не само техническа подготовка, но и организационна промяна в институцията. Обучението на персонала и създаването на специализирани екипи, отговарящи за управлението и поддръжката на блокчейн системите, са от ключово значение за дългосрочната устойчивост и сигурност на системата (Florin, 2024).

ЗАКЛЮЧЕНИЕ

Изследването на използването на блокчейн за създаване на електронни досиета в сигурността показва, че технологията предлага значителни предимства по отношение на децентрализация, прозрачност, необратимост и намаляване на риска от измами. Децентрализираните системи, управлявани чрез криптографски сигурни алгоритми и интелигентни договори, гарантират, че данните са защитени от неоторизирани промени, като същевременно позволяват проследимост и автоматизация на процесите. Практическите реализации в различни сектори – от образованието и здравеопазването до финансовите услуги и публичната администрация – са доказателство, че блокчейн технологията може да допринесе за намаляването на бюрокрацията и до повишаване на прозрачността. Въпреки техническите предизвикателства като скалиране, латентност и интеграция със съществуващи системи, разработчиците намират решения чрез оптимизация, хибридни модели и обучение. Правните и етични въпроси, свързани с неизменяемостта на данните и спазването

на регулации за поверителност, остават на преден план. Въпреки това, чрез ясна регулация, стандартни процедури и международно сътрудничество, се изграждат сигурни рамки, които гарантират устойчивост и надеждност на системите. Използването на блокчейн за електронни досиета не само трансформира начина на управление на данни, но също така предлага така търсената информационната сигурност и оперативната ефективност (EITSA, 2024). Изграждането на бъдещи решения ще изисква непрекъсната иновация, обучение и адаптация към новите технологични и регулаторни реалности. Ефективното интегриране на блокчейн технологиите в управлението на електронни досиета има потенциала да бъде катализатор за нова ера в информационната сигурност, където данните са не само защитени, но и лесно достъпни и проверими от всички заинтересовани страни.

ЛИТЕРАТУРА:

- Дочева, Т. (2024). *Използване на блокчейн приложения и иновации в киберсигурността*. <https://www.unwe.bg/doi/alternativi/2024.2/ISA.2024.2.06.pdf> // Docheva, T. (2024). *Izpolzvane na blokcheyn prilozheniya i inovatsii v kibersigurnostta*. <https://www.unwe.bg/doi/alternativi/2024.2/ISA.2024.2.06.pdf>
- Костов, Хр. (2025). *Отвъд Биткойн: Блокчейн – технологията, за която не знаем, че ви е нужна, много повече от криптовалутите*. <https://faktor.bg/otvad-bitkoyn-blokcheyn-tehnologiqta-za-koqto-ne-znaehte-che-vi-e-nujna-mnogo-poveche-ot-kriptoaluti> // Kostov, Hr. (2025). *OtvadBitkoyn: Blokcheyn – tehnologiyata, za koyato ne znaehte, che vi e nuzhna, mnogo poveche o tkriptoaluti*. <https://faktor.bg/otvad-bitkoyn-blokcheyn-tehnologiqta-za-koqto-ne-znaehte-che-vi-e-nujna-mnogo-poveche-ot-kriptoaluti>
- Личева, Т. (2022a). Блокчейн и екосистема на сигурност. В *Сборник доклади от научна конференция „Актуални проблеми на сигурността“, 27-28 октомври 2022 г., том 1* (стр. 139-146). Издателски комплекс на НВУ „Васил Левски“. // Licheva, T. (2022a). *Blokcheyn i ekosistema na sigurnost. V Sbornik dokladi ot nauchna konferentsiya „Aktualni problemi na sigurnostta“, 27-28 oktombri 2022 g., tom 1* (str. 139-146). Izdatelski kompleksna NVU „Vasil Levski“.
- Личева, Т. (2022b). Блокчейн технологии – информационна сигурност в архивистиката. *Сигурност и отбрана*, (2), 235-251. <https://doi.org/10.70265/GOMC7464> // Licheva, T. (2022b). *Blokcheyn tehnologii – informatsionnasigurnost v arhivistikata. Sigurnost i otbrana*, (2), 235-251. <https://doi.org/10.70265/GOMC7464>

- Личева, Т. (2022c). *Цифрови трансформации в архивното дело*. Научно-технически съюз по машиностроене „Индустрия 4.0“. // Licheva, T. (2022c). *Tsifrovi transformatsii v arhivnoto delo*. Nauchno-tehnicheski sayuz po mashinostroene „Industriya 4.0“.
- Личева, Т. (2023a). Внедряване на блокчейн в държавния сектор и сигурност на информацията. *Сигурност и отбрана*, (1), 223-235. <https://doi.org/10.70265/DRPF1506> // Licheva, T. (2023a). *Vnedryavane na blokcheyn v darzhavniya sektor i sigurnost na informatsiyata*. *Sigurnost i otbrana*, (1), 223-235. <https://doi.org/10.70265/DRPF1506>
- Личева, Т. (2023b). *Модерна сигурност в управлението*. НТС по машиностроене „Индуктрия-4.0“. // Licheva, T. (2023b). *Moderna sigurnost v upravlението*. NTS po mashinostroene „Induktriya-4.0“.
- Личева, Т. (2024). *Данни 5.0*. НТС по машиностроене „Индустрия-4.0“. // Licheva, T. (2024). *Danni 5.0*. NTS pomashinostroene „Industriya-4.0“.
- ЕИТСА, (2024, June 12). *Как съвременните технологии като контейнеризация, Kubernetes и блокчейн въвеждат нови уязвимости и какви мерки за сигурност са необходими за справяне с тези предизвикателства?* <https://bg.eitca.org/>
- Florkin, J. (2024). *The Future of Blockchain Technology: 10 Key Chapters about Emerging Trends, Scalability Solutions, and Regulatory Developments*. <https://julienflorkin.com/bg/%D1%82%D0%B5%D1%85%D0%BD%D0%BE%D0%BB%D0%BE%D0%B3%D0%B8%D1%8F/blockchain/%D0%91%D0%BB%D0%BE%D0%BA%D0%BE%D0%B2%D0%B0-%D1%82%D0%B5%D1%85%D0%BD%D0%BE%D0%BB%D0%BE%D0%B3%D0%B8%D1%8F/>
- Kejriwal, K. (2023). *AI and Blockchain Integration for Preserving Privacy*. <https://www.unite.ai/ai-and-blockchain-integration-for-preserving-privacy/>
- Lyubenov, L. (2024). Domestic Legal measures for increasing security in the Black Sea region. *Security and Defense*, (2), 9-18. <https://doi.org/10.70265/VIRM1297>