НОВ БЪЛГАРСКИ УНИВЕРСИТЕТ

**Магистърски факултет**

**Департамент Национална и международна сигурност**

**Програма: „**Стратегии и политики за сигурност“

# АВТОРЕФЕРАТ

## НА ДИСЕРТАЦИЯ

на тема:

# ПОВИШАВАНЕ НА ПРИЛОЖИМОСТТА НА БЛОКЧЕЙН-ТЕХНОЛОГИИТЕ В КОНТЕКСТА НА ИНФОРМАЦИОННАТА СИГУРНОСТ

**за получаване на образователна и научна степен *„доктор“* в област на висше образование *9. Сигурност и отбрана*, професионално направление *9.1. Национална сигурност***

**Дипломант:**

Веселин Монев

**Научен ръководител:**

проф. д-р Николай Радулов

София, 2020 г.

*Този автореферат е изготвен и предаден на английски език.*

*Предоставена е версия, преведена на български език.*

# Съдържание

# 1. ОБЩИ ОСОБЕНОСТИ НА ДИСЕРТАЦИЯТА

## КЛЮЧОВИ МЕТРИКИ ОТНОСНО ДИСЕРТАЦИОННИЯ ТРУД

| **Общ брой страници:** | | **Брой страници на основната част:** | |
|---|---|---|---|
| Версията на английски език (оригинал): | 144 | Версията на английски език (оригинал): | 122 |
| Версията на български език (превод): | 166 | Версията на български език (превод): | 143 |
| **Брой на фигурите:** | 15 | **Брой на таблиците:** | 16 |
| **Брой източници на информация:** | 148 | **Брой на публикациите:** | 5 |

## АКТУАЛНОСТ НА ТЕМАТА

Блокчейн-технологиите получават нарастващо внимание откакто първият блокчейн – Биткойн, започва работа през 2009 г. Както се случва при всяко развитие в информационните технологии (ИТ), възниква въпросът за сигурността. Нещо повече, сигурността е програмирана като основен и значим компонент във всяка блокчейн-технология. Тъй като блокчейн е един сравнително нов феномен, концепциите, занимаващи се с разработката, придобиването, конфигурирането, управляването и използването на тези технологии са в много ранен етап от своето историческо развитие и много въпроси предстоят да бъдат зададени и да им бъде отговорено.

Разработката представлява проучвателно изследване чрез качествена методика, което разглежда разностранни аспекти на информационната сигурност при блокчейн-технологиите, за да установи каква е тяхната роля в този нов технологичен контекст. Недостатъчното и неточното разбиране на общата рамка на феномена вероятно би могло да попречи на въвеждането на адекватни механизми за сигурност.

## ОБЕКТ И ПРЕДМЕТ НА ИЗСЛЕДВАНЕТО

Обект на изследването в дисертацията са *блокчейн-технологиите*. Предмет на изследването е повишаване на приложимостта на тези технологии в контекста на *информационната сигурност*.

## ИЗСЛЕДОВАТЕЛСКА ТЕЗА

Блокчейн е феномен, който е заобиколен от разностранни аспекти на информационната сигурност. Различни организации и индивиди имат различни гледни точки, цели и нужди относно сигурността на тези технологични решения. Професионалистите в сигурността трябва да разберат цялостната картина на теорията за информационна сигурност, приложена в областта на блокчейн-технологиите, за да използват адекватни стратегии за повишаване на приложимостта на тези технологии и за да дават професионални и релевантни експертни съвети.

## ЦЕЛИ И ЗАДАЧИ

Настоящото изследване търси отговори на следните два въпроса:

1. Кои са най-важните аспекти на информационната сигурност, когато организации или индивиди започнат да се занимават с блокчейн-технологии?
2. Каква е важността на сигурността на блокчейн-технологиите за различни организации и индивиди?

В търсене на отговори на тези два въпроса, това изследване си поставя следните задачи:

- Задаване на теоретична рамка за понятията, свързани с блокчейн-технологии и информационна сигурност. Също така, дефиниране на концепцията „важност“ в този контекст.
- Изследване на разностранните аспекти в сигурността на блокчейн.
- Описване на открития и разглеждането им в рамката на изследователската теза.
- Предлагане на стратегии за повишаването на приложимостта на блокчейн-технологиите след вземане предвид на откритията. Стратегиите демонстрират полезността на откритията във връзка с *Изследователската теза*.

## СТРУКТУРА НА ИЗСЛЕДВАНЕТО

Изследването се състои от компонентите, показани в таблица 1.

*Таблица 1. Основни и второстепенни части на дисертационния труд.*

<table>
<tr><td rowspan="3">Основни части</td><td colspan="4">Увод</td></tr>
<tr><td>Глава 1: Теоретична рамка</td><td>Глава 2: Аспекти на информационната сигурност при блокчейн-технологиите</td><td colspan="2">Глава 3: Открития. Стратегии за повишаване приложимостта на блокчейн-технологиите в контекста на информационната сигурност.</td></tr>
<tr><td colspan="4">Заключение и препоръки</td></tr>
<tr><td>Второсте-пенни части</td><td>Абстракт</td><td>Списък на фигури и таблици</td><td>Списък на съкращенията</td><td>Библиография</td></tr>
</table>

Основните части са очертани по следния начин.

1. ***<u>Увод</u>***

Уводът полага основата на изследването, включително методологията.

2. ***<u>Глава 1:Теоретична рамка</u>***

Първата глава задава рамката с основните теоретични концепции на изследването. Основните компоненти включват:

- **а.** Блокчейн-технологии – описване на фундаменталните аспекти;
- **б.** Фундаменти на информационната сигурност – установяване на база за информационна сигурност в контекста на блокчейн-технологиите; Също така, дефиниране на концепцията за *важност* на информационната сигурност по отношение на блокчейн-технологиите.

3. ***<u>Глава 2: Аспекти на информационната сигурност при блокчейн-технологиите</u>***

Втората глава изследва разностранни аспекти на информационната сигурност по отношение на блокчейн-технологиите, групирани в следните категории:

- **а.** Сигурност при архитектурата и разработката на блокчейн-технологии

*Кои са основните проблеми при дизайна и разработката на блокчейн-технологии?*

**б.** Предизвикателства в сигурността при организациите

*Върху какви проблеми се фокусират различните организации, когато се занимават в областта на блокчейн-технологиите (например когато разработват, използват, проучват, регулират или докладват за блокчейн-решения)?*

**в.** Сигурност от потребителска гледна точка

*Какви въпроси за сигурността трябва да задават крайните потребители на продуктови решения, свързани с блокчейн, и какво трябва те да знаят за сигурността на блокчейн?*

4. ***Глава 3: Открития. Стратегии за повишаване приложимостта на блокчейн-технологиите в контекста на информационната сигурност.***

В тази глава са представени основните открития на изследването, в отговор на изследователските въпроси. След това са предложени стратегии за повишаване на приложимостта на блокчейн-технологиите, отчитайки откритията.

5. ***Заключение и препоръки***

Тази част има три основни цели:

**а.** Обобщаване на предходните части;

**б.** Описание на приносите и на начина, по който изследването запълва теоретични пропуски;

**в.** Предлагане на нови идеи за последващо изследване.

## МЕТОДОЛОГИЯ

Общата стратегия на изследването преглед и анализ на значителен брой източници на информация, за да се позволи разбирането на разностранни аспекти на сигурността при феномена блокчейн.

***Изследователски дизайн и подходи***

Основа характеристика на изследването е неговият ***качествен дизайн***, противопоставен на количествения. Главната причина за този избор е защото качественият дизайн е по-подходящ за *Изследователската теза* и въпросите с отворен отговор в *Цели и задачи*.

Втора характеристика на изследването е неговата ***описателност***. Описанията опосредстват идентифицирането на проблем и факти според предварително зададени критерии, както и за демонстрация на логически взаимовръзки.

Третата характеристика на изследването са ***обясненията*** на феномени и специфики, за да се проучат причинно-следствените взаимовръзки.

***Системният подход*** е четвъртата основна характеристика. Той позволява сложни концепции като „блокчейн“ и „информационна сигурност“ да бъдат разделени на по-малките им съставни части, които могат по-лесно да бъдат разбрани.

На следващо място, петата характеристика на работата е приложението на ***дедуктивен подход***, който опосредства употребата на установени теории за проучването и обяснението на феномени, релевантни при това изследване.

***<u>Изследователски методи</u>***

Методите са групирани в следните категории:

А) Методи за събиране на информация

Б) Методи за обработка и анализ на информация

***А) Методи за събиране на информация***

Изследването проучва множество източници на информация, използвайки няколко общи и специализирани машини за търсене. Фундаменталното допускане е, че повече машини за търсене на голям брой от заглавия носят по-голяма стойност, отколкото ако се използват по-малко.

***Б) Методи за обработка и анализ на информация***

Методите за обработка на информация отчитат качествения изследователски дизайн, подходи и стратегия. Тези методи включват:

- *Анализ на документи*, което включва бърз поглед през документа, пълен прочит и интерпретация.

- *Тематичен анализ* като форма за разпознаване на белези в документа. Той позволява идентифицирането на много специфики на информационната сигурност при блокчейн-технологиите.
- *Дедукцията* позволява употребата на установени теории от информационната сигурност, ИТ и други дисциплини, за да се проучат специфики и феномени.
- *Описание* се използва през цялото изследване като метод за установяване на ключови характеристики на технологии, системи и феномени.
- *Обяснения* подпомагат ключови специфики на блокчейн и информационната сигурност. Освен това те аргументират изследователски решения.
- *Контент анализ* се използва за идентифициране на специфична комбинация от думи в конкретен документ. Например ако думата „сигурност“ е използвана в статия/документ, контент анализът позволява разпознаването на сходни думи, като например „криптография“, „хеш стойност“, „частен ключ“, „таен“ и др.
- *Категоризация* е метод за подреждане на елементи в класове или категории. Този метод е използван из цялото изследване, за да се разграничат компоненти от теорията за информационна сигурност в контекста на блокчейн-технологиите, както и за блокчейн-компоненти.
- *Сравнителен анализ* се използва като ключов метод за сравняване на елементи от откритията на изследването в глава 3. Освен това *сравнения* помагат за обяснение на аспекти на блокчейн в глава 1.
- *Обобщаване* се използва в следните случаи: 1) Във връзка с резултатите на сравнителния анализ в глава 3, за да се направят полезни наблюдения; 2) За предлагането на стратегии с релевантност в информационна сигурност, за повишаване на приложимостта на блокчейн-технологиите; 3) В края на всяка основна глава, за генериране на заключения.

## ДОПУСКАНИЯ И ОГРАНИЧЕНИЯ

Изследването прави следните допускания:

- Аспектите на сигурността, свързани с блокчейн-технологиите, могат да бъдат изследвани дедуктивно чрез установени концепции в теорията за информационна сигурност.
- Читателят има базисни знания по компютърни науки и информационна сигурност. Въпреки че настоящата работа има глава за теоретичната рамка, която очертава основата на изследването, тя също така разчита на установена терминология за ИТ и сигурност.

Както с всяко изследване, разработката има следните ограничения:

- Източниците на информация за това изследване са на английски език, поради удобството от това.
- Блокчейн-технологиите са изследвани чрез концепции на информационната сигурност. Въпреки че индустрията за сигурност работи с установени концепции, една по-различна и по-широка рамка би могла да разкрие повече перспективи за изследване.
- Някои потенциални източника на информация, които са известни на автора, не са проучени, поради ограничения в ресурсите.
- Поради естеството на дисертацията, качествени методи са избрани като подходящи инструменти за изследване.
- Подробно проучване на индивидуалните особености на повечето блокчейни и приложения не е извършено, за да се избегне прекомерно съдържание на разработката и ограничена обща полза за целите и задачите на изследването.

## ИЗТОЧНИЦИ НА ИНФОРМАЦИЯ ЗА ИЗСЛЕДВАНЕТО

Изследването е подпомогнато от множество източници, които обясняват различни елементи на блокчейн-технологиите, свързаните с тях аспекти на сигурността, обща информационна сигурност и насоки за извършване на изследване. Таблица 2 показва източниците на информация, групирани в категории.

*Таблица 2. Метрики за източниците на информация.*

| *Тип* | *Брой* | *Процент* |
|---|---|---|
| Уеб-страници / уеб-статии | 107 | 72,3% |
| Изследвания / доклади / статии в списания | 21 | 14,2% |
| Книги / раздели в книги / стандарти | 16 | 10,8% |
| Видео записи | 3 | 2% |
| Разни | 1 | 0,7% |
| *Общо:* | 148 | 100% |

## АДРЕСАТИ НА ИЗСЛЕДВАНЕТО

Професионалисти по информационна сигурност и мениджмънт на организации могат да използват това изследване, за да придобият по-подробно разбиране за всичките компоненти, които дефинират информационната сигурност в сферата на блокчейн-технологиите.

## ДРУГИ МЕТРИКИ

Таблица 3 включва допълнителни количествени метрики, свързани с разработката.

*Таблица 3. Количествени метрики на дисертационния труд.*

| **Метрика** | **Стойност** |
|---|---|
| Брой на предложените стратегии с релевантност при информационната сигурност за повишаване на приложимостта на блокчейн-технологиите | 19 |
| Брой на идентифицираните ключови аспекти на информационната сигурност, които са свързани с блокчейн-технологиите | 23 |
| Брой на препоръките за последващо изследване | 5 |
| Брой на точки с данни за сравнение на степента на важност на информационната сигурност при блокчейн-технологиите между категории от субекти (организации и индивиди) | 621 |
| Брой на категориите от субекти за сравнение | 9 |
| Брой на разгледаните типове атаки и уязвимости, свързани с блокчейн-технологиите | 8 |
| Брой на разгледаните теоретични уязвимости, които могат да засегнат блокчейн-технологиите | 15 |
| Брой на разгледаните успешни атаки и уязвимости | 13 |
| Брой на темите, които представляват интерес за потребителите, които решават дали да използват, или когато | 18 |

| | |
|---|---|
| вече използват определено продуктово решение, свързано с блокчейн | |
| Брой на споменатите наименования на блокчейни | 11 |
| Брой на споменатите алгоритми за единодушие | 16 |
| Брой на разгледаните ключови концепции и дефиниции в информационната сигурност (без подконцепциите) | 24 |
| Брой на разгледаните цели на информационната сигурност | 11 |

## 2. НАУЧНА НОВОСТ И АПРОБАЦИЯ

Изследването има няколко основни научни приноса, резюмирани в таблица 4. Части от тях са прегледани от независими пиъри и приети за научно публикуване. Те са планирани за обсъждане по време на научна технологична конференция през септември 2020 г. Глава 5 на този автореферат предоставя допълнителна информация относно тези публикации и тяхната връзка с изследователската работа.

Освен това, професионалист по информационна сигурност прегледа подробно дисертационната работа. Той предостави следния текст за включване в този автореферат:

*От равнището на общ преглед смятам, че откритията в глава 3 на дисертационната работа на Веселин Монев са полезни/добри и се съгласявам с тях. Равнището на информация е добро начало, което дава гъвкавост за по-задълбочен преглед в рамките на директно приложимите области за всеки субект, който обмисля използването или вече използвайки технологията. Деветнадесетте стратегии са също полезни/добри и подходящи от перспективата на общ преглед. Това, отново, предоставя гъвкавост на различни субекти и техните сценарии. Авторът споменава няколко пъти необходимостта от специализирани експерти за всяка компетенция в технологията; съгласен съм с това и е полезна препоръка за вземане предвид от субект, който търси начин да се възползва от технологиите.*

*Добра разработка, интересна тема и образователна. Би била плашеща за средностатистическия читател, особено за такъв без представа от ИТ.*

***Прегледал :*** *Алън Хибърт,*

*Анализатор разузнаване в киберсигурността и инженер по операции в киберсигурността; старши софтуерен архитект*

*Кинг оф Прусия, Пенсилвания, САЩ*

*17 юли, 2020 г.*

*Контакт: allenr.hibbert@gmail.com*

***

Допълнително одобрение може да бъде очаквано при сценария на успешна защита на дисертационната работа според държавните и университетските изисквания.

*Таблица 4. Очертание на основните приноси на изследователската разработка.*

| **No.** | **Принос** | **Тип** | **Местополо-жение** |
|---|---|---|---|
| 1 | Идентифициране на фундаментите на блокчейн | Подобрена точност и яснота на съществуващо познание | Глава 1 (първа част) |
| 2.1 | Обяснение на взаимоотношението между фундаментите на теорията за информационна сигурност и блокчейн-технологиите | Нова интерпретация на съществуващо познание в контекста на блокчейн-технологиите | Глава 1 (втора част) |
| 2.2 | Дефиниция на важността на информационната сигурност по отношение на блокчейн-технологиите за организации и индивиди | Нова идея; Фокус върху практическата приложимост | Глава 1 (трета част) |
| 3 | Идентифициране на ключовите аспекти на информационната сигурност, които са свързани с блокчейн-технологиите | Нова идея; Фокус върху практическата приложимост | Глава 3 (първа част) |
| 4 | Сравняване на степента на важност на информационната сигурност (компетенции) между категории организации и индивиди | Нова идея; Фокус върху практическата приложимост | Глава 3 (втора част) |
| 5 | Предлагане на общи управленски стратегии за повишаване на приложимостта на блокчейн-технологиите чрез методи, релевантни при информационната сигурност | Нова идея; Фокус върху практическата приложимост | Глава 3 (трета част) |

# 3. РЕЗЮМЕ НА ОСНОВНИТЕ ГЛАВИ

## 3.1. ГЛАВА 1 – ТЕОРЕТИЧНА РАМКА

Първата глава задава контекста на изследователския труд като описва и обяснява ключовите аспекти на:

- Блокчейн-технологиите като обект на изследването
- Информационната сигурност, като част от предмета на изследването

### Ключови дефиниции при блокчейн

- ***Блокчейн***

Блокчейн е вид разпределен регистър за поддържане на непроменяеми и устойчиви на фалшификация записи с данни за транзакции. Блокчейн функционира като децентрализирана база данни, която се управлява от компютри, които принадлежат към мрежа от вида точка-до-точка (P2P). Всеки от компютрите в разпределената мрежа поддържа копие на регистъра, за да се предотврати единична точка на повреда (single point of failure) и всички копия се актуализират и валидират едновременно.

- ***Регистър***

*Разпределен регистър* е дигитална система за записване на транзакции от активи, при която транзакциите и детайлите за тях се записват в множество компютри едновременно.

- ***Блокчейн-система***

Блокчейн-системата се състои от:

1) Блокчейн-мрежа от компютри, наричани също така *възли* (nodes);
2) Блокчейн-структура от данни за регистъра, която е репликирана в блокчейн-мрежата. Възли, които съхраняват пълно копие на регистъра, са известни като *пълни възли* (full nodes);
3) Мрежови протокол, който определя права, отговорности и методи за комуникация, проверка, валидиране и единодушие между възлите в мрежата. Това включва осигуряване на авторизация и автентификация

на нови транзакции, механизми за добавяне на нови блокове, механизми за насърчаване (в случай, че е необходимо) и други подобни аспекти.

- ***Блокчейн-платформа***

Блокчейн-платформа е технологията, необходима за работата на блокчейн. Тя се състои от клиентски блокчейн-софтуер за възлите, локалното хранилище за данни за възлите и всички други клиенти за достъпване на блокчейн-мрежата.

- ***Умен договор***

Умните договори са приложения (програми), вместени като данни в блокчейн-регистъра и изпълнявани чрез транзакции в блокчейн. Умни договори могат да съхраняват и трансферират дигитални активи (жетони), управлявани от блокчейн и могат да извикват други умни договори, съхранявани на блокчейн. Кодът на умните договори е предопределен и неотменим, след като веднъж е вместен.

- ***Публичен блокчейн***

Блокчейн на единодушието, който е достъпен за всеки. На участниците е позволено да изпращат и валидират транзакции. Най-общо този тип блокчейн се счита за „напълно децентрализиран“. Типичен пример за такъв блокчейн е Биткойн.

- ***Частен блокчейн***

Блокчейн, при който разрешението за записи е в рамките на една организация. В тази организация може да има допълнителни опции, като например управление на база данни, одит и др. В повечето случаи не е необходим публичен достъп. Частните блокчейни са известни и като технологии за разпределени регистри (DLT) и клонят към това да са малки и да не използват криптовалута или жетон (token). Този тип блокчейн намира приложение в консорциуми, които се състоят от доверени членове и търгуват поверителна информация.

- ***Консорциум-блокчейн***

Блокчейн, който има характеристики от публичния и частния. Предварително избрани възли контролират процеса на единодушие. Различна организация управлява всеки възел и процент от тях трябва да потвърди

валидността на всеки блок, за да бъде добавен към веригата. Правото за четене на блокчейн може да бъде публично достъпно, ограничено до участници или комбинация от двете – „хибридно“. Такива блокчейни мога да бъдат счетени за „частично децентрализирани“.

- ***Жетони***

Жетоните са репрезентация на определени активи или полезност, които обикновено се намират върху друг блокчейн. Жетоните на практика могат да репрезентират всякакви активи, които са заменяеми и търгуеми, от стоки, през точки за лоялност, до дори други криптовалути.

- ***Възел***

Възел (node) е компютър, който е свързан с мрежата на определен блокчейн. Възелът/компютърът поддържа мрежата чрез потвърждаване и препращане на транзакции. В същото време той получава копие на целия блокчейн. Възелът може да бъде предназначен за точка за препращане на транзакции, която увеличава достъпността на мрежата, или той може да спомогне за сигурността на транзакциите като отхвърля невалидни транзакции. Възелът също така може да спомага за дейността по добиването (mining), за да има финансова добавъчна стойност от експлоатацията му.

## Основни концепции при блокчейн

- ***Криптографията*** е компонентът, който гарантира, че транзакциите са защитени: оторизирани потребители стартират транзакции и те не могат да бъдат фалшифицирани.
- Компонентът ***теория на игрите*** спомага *криптографията,* за да възпира операторите на възли умишлено да се опитват да разрушат системата, като например чрез фалшификация на транзакции или да отказват легитимни такива. Съществуват две основни концепции за реализацията на *теорията на игрите* при блокчейн: алгоритъм за единодушие и свързаният с него протокол. Първият дефинира основните правила на блокчейн, а вторият осигурява механизма, чрез който тези правила се следват. *Доказателство за работа* (Proof of Work - PoW) и

*доказателство за залог* (Proof of Stake - PoS) са двата най-известни алгоритъма за единодушие.

- Третият компонент – ***компютърни науки*** комбинира другите два компонента чрез структури данни и техника точка-до-точка за мрежова комуникация. Също така техники за компютърно инженерство позволяват вграждането на *криптографията* и *теорията на игрите* в софтуерно приложение, позволявайки децентрализирано и разпределено изчисляване между възлите със структури данни и компоненти за мрежова комуникация.

### Основни компоненти на блокчейн

Те включват *възел; транзакции; блокове; верига; миньори; алгоритъм за единодушие и протокол за единодушие*.

### Ключови характеристики на блокчейн-архитектурата

Те включват:

- ***Криптография*** - използва се за валидиране истинността на блокчейн-транзакции чрез сложни изчисления и криптографско доказателство между участващите страни.
- ***Непроменимост*** – блокчейн функционира на принципа за *неопровержимост* и *необратимост* на записите.
- ***Произход*** - отнася се за способността да се проследи произходът на всяка транзакция в блокчейн-регистъра.
- ***Децентрализация и разпределение*** – всеки член на блокчейн-структурата има достъп до цялата разпределена база данни.
- ***Анонимност или псевдонимност*** – всеки участник в блокчейн-мрежа има създаден адрес, а не потребителска самоличност.
- ***Прозрачност*** – записите могат да бъдат одитирани от предварително определени участници.

### Участници в блокчейн

Те могат да варират между блокчейни и включват *потребител в блокчейн; регулатори; разработчици; архитекти; мрежови оператори; традиционни компютърни платформи; традиционни източници на данни; сертификационен орган; оператори на миньорски системи; оператори на възли.*

### Сценарии за приложения на блокчейн

Някои от тях включват плащания/транзакции; валидиране на данни; достъпване/споделяне на данни; защита на самоличността; дигитална валута; издирване и проследяване; сертифициране; достъп до интелектуална собственост; съгласуване на записи; трансфер на активи; споделяне на приходи; жетони, поддържани от активи; акции под формата на жетони; активи под формата на жетони; отбелязване на времето; попечителство.

### Популярни блокчейни

Някои популярни блокчейни и техните характеристики са показани в таблица 5.

*Таблица 5. Ключови характеристики на пет популярни блокчейна за компаниите.*

| | ***Ethereum*** | ***Ripple[1]*** | ***Hyperledger Fabric*** | ***R3 Corda*** | ***Quorum*** |
|---|---|---|---|---|---|
| ***Индустриален фокус*** | Много индустрии | Финансови услуги | Много индустрии | Финансови услуги | Много индустрии |
| ***Управленска единица*** | Ethereum разработчици | Ripple Labs | Linux фондация | R3 Consortium | Ethereum разработчици и JP Morgan Chase |
| ***Тип мрежа*** | Неизискващ разрешение[2] | Изискващ разрешение | Изискващ разрешение | Изискващ разрешение | Изискващ разрешение |
| ***Криптовалута и жетони*** | Ether (ETH); Жетони чрез умни договори | XRP | Няма; Жетони чрез умни договори | Няма; Жетони чрез умни договори | Няма; Жетони чрез умни договори |
| ***Пазарна капитализация[3]*** | $23.5 милиарда | $8.9 милиарда | Неприложимо | Неприложимо | Неприложимо |
| ***Алгоритъм за единодушие*** | PoW[4] | Low-latency BFT | Модулен алгоритъм[5] | Модулен алгоритъм [5] | Istanbul BFT; Raft-based Consensus; Clique POA Consensus |

| | | | | | |
|---|---|---|---|---|---|
| ***Възможност за умни договори*** | Да | Не | Да | Да | Да |

[1] Някои експерти не считат Ripple за блокчейн, а за разпределен протокол с отворен код, предназначен за мрежа за обмен на валута.
[2] Съществуват и реализации *изискващи разрешение*.
[3] Пазарната капитализация е базирана на данни от 18 май 2020 г.
[4] В момента на писането на тази разработка тече план за замяна на PoW с PoS.
[5] Разработени са модули за няколко алгоритъма. Например възможни типове са алгоритмите за единодушие, базирани на гласуване и лотария. Единодушие се постига на ниво транзакции.

*** *** ***

## Цели на информационната сигурност

Информационната сигурност е свързана с предмета на изследователската разработка. Съществуват три конвенционални цели (конфиденциалност, интегритет и достъпност – КИД), но допълнителни могат да бъдат добавени за постигане на по-обстойна дефиниция, като например одитируемост, отговорност и неприкосновеност на личния живот. Таблица 6 резюмира тези цели като основа за изследването.

*Таблица 6. Цели на информационната сигурност.*

| Цел на сигурността | Същност |
|---|---|
| Конфиденциалност | Предоставяне на данни само на целевите получател(и). |
| Интегритет | Гарантиране, че данните са променени според дизайна и намеренията. |
| Достъпност | Данните са достъпни в предварително определени време и скорост. |
| Одитируемост | Данни, система, програма, или други елементи могат да бъдат одитирани в приемлива степен. |
| Отговорност | Има ясна връзка между човешките отговорности и електронната (онлайн) самоличност. Също така участниците в комуникацията са приемливо отговорни за своите действия. |
| Неприкосновеност на личния живот | Индивидите могат да избират какви данни споделят и с кого. Тази възможност за избор е реализирана с приемливи контроли. |

- ***Информационна сигурност*** е запазването на конфиденциалността, интегритета, достъпността, одитируемостта, отговорността и

неприкосновеността на личния живот (когато е приложима) при информация и системи.

### Контроли на информационната сигурност

Контрол за информационна сигурност е решаващ термин за областта на информационната сигурност и поради това също е проучен.

- ***Контроли за информационна сигурност*** са административни, технически и физически механизми/предпазни мерки, предписани за система, за да се запази и защити нейната конфиденциалност, интегритет, достъпност, одитируемост, отговорност и неприкосновеността на личния живот, както и информацията, обработвана през системата.

Контролите за информационна сигурност се вместват в три категории:

- ***Технически/логически*** контроли са хардуерните или софтуерните механизми за защитата на ресурси и системи.
- ***Административни контроли*** са писмени регулации, като политики за сигурност, процедури, стандарти, инструкции и др.
- ***Физически контроли*** са елементи, които могат да бъдат докоснати физически. Те включват физически механизми, въведени за предотвратяване, засичане или мониторинг на събития в сигурността при системи или зони в сграда.

Съществуват няколко вида *контроли за сигурност*, които могат да принадлежат към една (а често повече от една) от трите категории, дефинирани по-горе. Те са следните:

- ***Възпиращи контроли*** се използват, за да се обезсърчи нарушаването на регулациите в сигурността.
- ***Превантивен контрол*** се използва, за да отблъсква или спира възникването на нежелани или неоторизирани действия.
- ***Засичащ контрол*** се въвежда за да се разкрият или засекат нежелани или неоторизирани действия.

- ***Компенсационен контрол*** е допълнителен контрол, който подпомага съществуващ или се прилага вместо основни контроли.
- ***Коригиращ контрол*** се използва, за да се върне система към нормално състояние след възникването на нежелани или неоторизирани действия.
- ***Контроли за възстановяване*** са специфични коригиращи контроли с по-сложни способности.
- ***Директивен контрол*** се въвежда, за да се напътстват, ограничават или контролират действията на индивиди, които да спазват регулациите в сигурността.

## СЪЩЕСТВЕНИ КОНЦЕПЦИИ В ИНФОРМАЦИОННАТА СИГУРНОСТ

Изследователската работа проучва няколко ключови концепции в информационната сигурност, които допълват целите в сигурността и контролите, и ги поставят в контекста на блокчейн. Концепциите и връзката им с блокчейн са резюмирани в таблица 7.

*Таблица 7. Съществени концепции в информационната сигурност и тяхната връзка с блокчейн.*

| |
|---|
| ***Сигурност при разработката на софтуер:*** Разработка и внедряване на методи и процеси за обезпечаване, че софтуерът функционира очаквано и е без дефекти в дизайна и уязвимости при внедряването му.<br>Сигурността при разработката на софтуер е критичен фактор при разработката на блокчейни, умни договори и друг подпомагащ софтуер. Успешното компрометиране на която и да е от целите КИД би могло да навреди на планираните функционалности на конкретен блокчейн/приложение или дори да ги направят безполезни. Уязвимости биват откривани рано или късно във всеки софтуер и имат различна тежест, в зависимост от леснотата на експлоатацията им и потенциалните щети. Уязвимости, които са с критична или с висока степен на тежест често изискват разработчиците бързо да създадат софтуерна кръпка. |
| ***Малуер***, известен още като ***зловреден код/софтуер*** се отнася за софтуер, който е проектиран с намерението да повлияе по лош начин на компютър или мрежа.<br>Малуер може да използва уязвимост в система или устройство, за да компрометира конфиденциалността на личен ключ, мнемонична фраза или парола на портфейл за криптовалута. Малуер може да се използва и заедно с други атаки, като например социално инженерство, за да се компрометират контролите за сигурност на уеб-сайтове и да се откраднат чувствителни данни, включително лични и финансови данни на потребители. Малуер е възможно да |

бъде използван за добиване на криптовалута от компютъра на жертвата. Блокчейн-технологиите могат да се използват и за борба с малуер атаки.

***Наслагване***, също така известно като ***защита в дълбочина***, е използването на няколко контроли за по-ефективна защита срещу заплахи.

Дизайнът на блокчейн може да включва повече от един технологически механизми за предотвратяване на конкретни заплахи. Освен това организациите, които решат да въведат конкретно блокчейн-решение в своята ИТ-инфраструктура, ще трябва да я защитят с няколко контроли.

***Криптографията*** осигурява конфиденциалност, интегритет, автентификация и неопровержимост за чувствителна информация.

Криптографските механизми са интегрален компонент от всяка блокчейн-технология. Криптографията защитава интегритета на блокчейн-транзакциите и в зависимост от дизайна определя мрежовата пропускателна способност и устойчивост срещу атаки и проблеми, свързани с достъпността. Наред с това асиметричната криптография се използва за автентификация на потребители.

***Пригаждане на сигурността към бизнес цели и задачи:*** Ролята на информационната сигурност в организациите, в основата си, цели да подкрепя бизнес нуждите, целите, задачите и мисията.

Блокчейн-технологиите се използват, за да задоволят специфични бизнес нужди. Когато се въведат в организациите, нивото на сигурността трябва да се пригоди към бизнес нуждите, рисковете и апетита към риска на мениджмънта.

***Класификацията на данни*** е основният метод за защита на данните според необходимостта от тайност, чувствителност или конфиденциалност.

Едно блокчейн-решение и данните, които то обработва, трябва да бъдат класифицирани според специфичните за организацията нужди и това в основата си изисква различен набор от контроли. Например ако едно блокчейн-решение обработва лични потребителски данни, подходящите контроли трябва да бъдат по-добри, отколкото при друго блокчейн-решение, което се използва единствено за проследяване на активи.

***Роли и отговорности при сигурността:*** Съществуват различни роли в сигурността и свързаните с тях отговорности.

Частните или консорциум-блокчейни изискват идентифицирането на подходящи роли, които да управляват и поддържат блокчейн-мрежата, в съгласуваност с общи добри практики за сигурност и специфични технологични изисквания.

***Рамка за управление на сигурността:*** Рамката за информационна сигурност представлява серия от документи, съгласувани и разбрани регулации, като например политики, процедури и процеси, които определят как информацията се управлява в дадена организация, за да се ограничават риска и уязвимостите и да се увеличава увереността във все по-свързания свят.

Организациите, които са въвели една или повече рамки за сигурност, трябва да интегрират всяка технология, в това число блокчейн, в нея. Някои организации, които разработват софтуер, могат да желаят да използват рамка за сигурност при разработката на софтуер и тестване, за да обезпечат, че тяхното продуктово решение отговаря на определен набор от минимални или препоръчителни изисквания. Други организации биха се придържали към рамка, която предписва преглед на контроли за сигурност на доставчик, от който те искат да придобият облаково блокчейн-решение.

***Заплахи и уязвимости:*** Заплахата е възможна опасност, която може да експлоатира уязвимост. Уязвимост е слабост в софтуер, система или мрежа, която може да бъде експлоатирана.

Блокчейн-технологиите, в своята същност, са софтуер, който работи върху компютри, свързани към мрежи. Уязвимости в сигурността на софтуера, хардуера или мрежа могат да влияят на субектите, които използват блокчейн-платформи или програми.

***Оценка на риска в информационната сигурност, одит, тестване и третиране на риска:*** Оценката на риска в информационната сигурност е процес на идентификация, оценяване и приоритизация на събития, които могат негативно да повлияят на операциите и целите на организация. Одитирането може да бъде счетено като форма на формално тестване.

Оценките на риска са задължителен инструмент в организациите като част от зряла система за управление на информационната сигурност (СУИС). Когато такива организации разработват или използват блокчейн-решения, оценка на риска може да спомогне за идентифицирането и разрешаването на уязвимости, като част от установената програма за управление на уязвимостите. Освен това възможности за подобрение могат да бъдат идентифицирани и обсъдени при заседания на мениджмънта.

***Обучение за осъзнаване на сигурността и образование по сигурност:*** Обучението за осъзнаване на сигурността е контрол за промяна на поведението на потребителите, за да спазват целите за сигурност в организацията. Образованието по сигурност е следваща стъпка за образование на потребителите много отвъд политиките за сигурност на организацията и обикновено визира персонала за сигурност или хора, които имат стремеж към позиции в сигурността.

Обучението за осъзнаване на сигурността и образованието целят директно да засягат хората, които използват или разработват блокчейн-технологии. Хората трябва да са запознати със стратегии за сигурност, за да могат безопасно да внедряват и управляват блокчейн-платформи и приложения или да извършват транзакции.

***Закони и регулации, неприкосновеност на личния живот:*** Правителства и други регулатори дават насоки и налагат регулации спрямо компютърни системи, технологии и организации.

Правителства и други регулатори влияят върху решенията на субекти, които използват или разработват блокчейн-решения. Създатели на блокчейн и криптовалути, оператори, крайни потребители и борси могат да са обект на специфични финансови регулации, които да изискват и специфични контроли за сигурност.

***Анонимизация и псевдонимизация:*** Анонимизацията е процес на отстраняване на чувствителни данни (обикновено лични), когато те са обработвани и съхранявани. Псевдонимизацията е процес на използване на псевдоними, за да се идентифицират хора директно.

Блокчейн-решенията биха изисквали различна степен на анонимност и защита на личните данни, в зависимост от целта им. Съществуват криптовалути, които са проектирани да защитават самоличността на потребители, които извършват транзакции. В други случаи частни блокчейн-решения може да изискват ограничена защита, защото транзакциите се извършват върху частни

блокчейни, при които потребителските самоличности са предварително установени.

***Основи, определяне на обхвата и пригаждане:*** *Определяне на обхвата* е процес на преглеждане и избиране на контроли от *основа* с контроли. *Пригаждане* означава изменяне на списък с контроли, така че те да са съобразени с мисията на организацията.

Тези техники могат да бъдат използвани когато се създават стандарти или процеси за сигурност при разработката на софтуер за блокчейн-решения, или когато се вземат решения относно необходимите контроли за сигурност при използването на блокчейн-решения в рамките на дадена организация.

***Сертифициране и акредитация:*** Сертифицирането е процес на оценка на техническите и нетехническите функционалности на ИТ-система, за да се подпомогне акредитацията. Акредитацията е формално мениджърско изявление, че системата отговаря на проверените критерии в сертификационната фаза.

Заедно с независими одити, някои организации, които внедряват частни блокчейн-решения като част от бизнес-операциите си, могат да бъдат обект на процеси за сертификация и акредитация.

***Управление на уязвимости:*** Управлението на уязвимости е критичен процес за идентифициране на уязвимости и поправянето им, обикновено чрез софтуерни актуализации. То е жизнено-важен контрол, който цели поддържането на системите с последните актуализации за сигурност, стабилност и функционалност.

Блокчейни и компютри, свързани и извършващи транзакции през блокчейни, могат да бъдат уязвими на известни или все още публично неизвестни уязвимости. Всички хора и организации, които използват свързан с блокчейн софтуер, трябва редовно да инсталират актуализации в ИТ-инфраструктурата, включително ОС, програми, мрежови устройства, портфейли за криптовалути и др. Наред с това архитекти и разработчици на блокчейни и приложения са пред предизвикателството да пускат кръпки за уязвимости, скоро след те биват открити.

***Мрежова сигурност:*** Мрежовата сигурност се състои от дейности, които са проектирани да защитават ползваемостта и интегритета на определена мрежа и на данните, пренасяни през мрежата.

Блокчейните работят в компютърна мрежа, която трябва да бъде защитена както всяка друга мрежа. Рисковете от зловредни атаки, които могат да засегнат която и да е от целите на КИД, трябва да бъдат смекчени до ниво, което позволява нормална работа. Много от конвенционалните мрежови контроли се очаква да са приложими и при блокчейни, особено при частни и консорциум-блокчейни. Публичните блокчейни също изискват мрежова сигурност. Обаче, тъй като няма централна власт, която да ги управлява, различен набор от контроли за сигурност е проектиран за тях.

***Сигурност на мобилни устройства:*** Сигурността на мобилните устройства включва обхвата от потенциални възможности или функционалности за сигурност, които могат да са налични за мобилни устройства.

Мобилните устройства могат да бъдат причина за безпокойство, когато служители или частни лица използват своите устройства, за да извършват транзакции през блокчейн. Потребителите трябва да предпазват своето

| |
|---|
| удостоверение за самоличност (credentials), за да подпомогнат конфиденциалността и интегритета на изпращаните данни. Компрометирани устройства могат да компрометират самоличността на потребителя, други чувствителни данни или да му попречат да използва блокчейн. |
| ***Управление на самоличността и достъпа:*** Управлението на самоличността и достъпа (IAM) е цяло поле в информационната сигурност, фокусиращо се върху потребителска идентификация, автентификация, оторизация и отговорност.<br>Контролите за IAM са критически компоненти в архитектурата и внедряването на което и да е блокчейн-решение. Потребителите трябва да бъдат идентифицирани и техните действия автентифицирани. В частните блокчейни, целите за оторизация и отговорност също играят съществена роля, заедно с регистрирането на достъпа и мониторинг. |
| ***Управление на инциденти в сигурността:*** Управлението на инциденти в сигурността е процес на идентифициране, записване, управление и анализиране на инциденти в сигурността.<br>Този процес се очаква да е значим при частни и консорциум-блокчейн-решения, при които има формални контроли за сигурност, наложени и контролирани от централна власт. Ако организации използват публични блокчейн-решения, които не са под техен контрол или контрола на доставчик, то процесът по всяка вероятно би имал ограничена приложимост. |
| ***Физическа сигурност:*** Физическата сигурност е защитата на персонал, хардуер, софтуер, мрежи и данни от физически действия и събития, които могат да причинят загуби или повреди на организацията.<br>Физическата сигурност е съображение при частните блокчейни, които се управляват от ИТ-персонал и когато възлите и допълнителната ИТ-инфраструктура е под защитата на организацията-хост. Физическата сигурност е важна и за частни лица, които съхраняват информация за достъп до криптовалути в преносими устройства или на своите настолни компютри. |

## ВАЖНОСТ НА *ИНФОРМАЦИОННАТА СИГУРНОСТ* ВЪВ ВРЪЗКА С БЛОКЧЕЙН-ТЕХНОЛОГИИТЕ

Изследването установява следната дефиниция за *важност на информационната сигурност във връзка с блокчейн-технологиите*:

*Информационната сигурност подпомага целите на организацията (или индивида) за безопасно и компетентно занимаване с блокчейн-технологии. Това занимаване може да включва разработката на блокчейн-софтуер, както и използване, внедряване, управляване, защита, консултиране, докладване, регулиране или други дейности, свързани с блокчейн*. Организациите могат да бъдат всички формални или неформални групи от хора или субекти – частни или държавни. Индивидите са лица, които се занимават самостоятелно с блокчейн-технологии.

## ОБОБЩЕНИЕ НА ГЛАВА 1

- Блокчейн може да бъде описан като дигитална система за записване на транзакции по непроменим и защитен от фалшификации начин. Съществуват няколко блокчейни, които могат да хостват различни софтуерни програми (умни договори). Някои блокчейни са публично достъпни, докато други подпомагат индивидуалните нужди на отделни организации или обединени в консорциум. Ключови свойства на блокчейн са децентрализацията и разпределението, които, когато се комбинират с криптография, теория на игрите и компютърни науки, могат да послужат като решение на много недостатъци на централизираните системи, включително подобряване на ефективността, намаляване на разходите, увеличаване на скоростта на транзакции, издръжливост на грешки и устойчивост на цензура.
- Информационната сигурност е сложен термин, който се състои от няколко основни цели: конфиденциалност, интегритет, достъпност, одитируемост, отговорност и неприкосновеност на личния живот. Очакването е, че всички цели са приложими към блокчейн-пространството, макар че тяхната индивидуална важност варира, в зависимост от функциите и употребата на блокчейн-решения, и индивидуалните цели на различните организации.
- *Контроли за информационна сигурност* са механизми, необходими за защита на ценни активи и информация. Обяснени са също така няколко други съществени концепции и термини, заедно с тяхната връзка с блокчейн-технологиите.
- *Важността на информационната сигурност по отношение на блокчейн-технологиите* е дефинирана, за да бъде използвана като основа за отговаряне на двата изследователски въпроса на по-късен етап от изследователската работа.

## 3.2. ГЛАВА 2 – АСПЕКТИ НА ИНФОРМАЦИОННАТА СИГУРНОСТ ПРИ БЛОКЧЕЙН-ТЕХНОЛОГИИТЕ

Втората глава изследва разностранни аспекти на информационната сигурност при блокчейн-технологиите, които са групирани в следните категории:

- Сигурност при архитектурата и разработката на блокчейн-технологии
- Предизвикателства на сигурността при организациите
- Сигурност от перспективата на крайния потребител

### НАБОР ОТ УМЕНИЯ ЗА РАЗРАБОТКАТА НА БЛОКЧЕЙНИ И ПРИЛОЖЕНИЯ

Професионалистите, които се ангажират с разработката на блокчейн-технологии, трябва да имат компетенции в няколко технологични и нетехнологични сфери, включително програмни езици, структури данни, изследване и други. Общо разделение на отговорности и специализирано знание може да бъде приписано на два типа блокчейн-разработчици – същински разработчици и софтуерни разработчици.

Във връзка с информационната сигурност, в конкретика, съществените области на сигурността включват криптография, надеждно програмиране, сигурност на архитектурата и дизайна, и мрежова сигурност.

### СЪОБРАЖЕНИЯ ПРИ ПУБЛИЧНИ, ЧАСТНИ И КОНСОРЦИУМ-БЛОКЧЕЙНИ

Разработката на блокчейни и свързани решения включва архитектурното съображение относно това дали те трябва да бъдат публични, частни или част от консорциум.

Частните блокчейни позволяват само познати организации да се присъединят към мрежата, докато публичните позволяват на всеки, свързан към мрежата, да взема участие. Очаквано тази разлика оказва значителни импликации върху дизайна на механизмите за конфиденциалност на блокчейна за предотвратяване на външни опити за фалшификация на данни.

Друг аспект на частните и публичните блокчейни е *неприкосновеността на личния живот*. Докато някои публични блокчейни целят да въведат принципа за

анонимност или псевдонимност, частните блокчейни обикновено не целят това, тъй като организациите искат да знаят и в много случаи са задължени по закон да идентифицират лицата, с които си имат работа.

Консорциум-блокчейнът е подобен на частния, с изключението, че повече от една организация контролира процеса за единодушие.

### Особености на сигурността при софтуерната архитектура на блокчейн

- Едно съществено архитектурно съображение е относно това какви части от функционалността да бъдат възложени на кои софтуерни компоненти. По същество трябва да бъде взето решение кои части от данните и изчисленията да бъдат разположени във веригата или държани извън нея. Разполагането на повече функционалности в блокчейна би изисквало повече изчислителна мощност и място за съхранение на данни за обезопасяване на транзакциите. Освен това колкото по-сложно е едно приложение (умен договор), толкова по-предизвикателен би бил дизайнът на неговите механизми за сигурност.
- ***Конфиденциалността*** е една от основните цели на информационната сигурност, която цели да предотврати неоторизираното разкриване на информация. Тази цел е предизвикателство да бъде постигната, тъй като базираните на блокчейн системи правят по подразбиране информацията видима за всеки. Криптографски методи и техники дефинират свойствата за конфиденциалност на блокчейн и свързани решения.
- ***Неприкосновеността на личния живот*** при данни е свързана с конфиденциалността и анонимността, защото тя засяга правенето на *поверителни* транзакциите в блокчейн, често чрез същите методи на криптографията. Тъй като личните данни са обект на регулации, разработчиците и потребителите на блокчейн трябва да вземат предвид дали и при какви условия конкретна блокчейн-технология би била законна.

- Контроли за ***интегритет*** се използват, за да се предотврати неоторизирано изменение на данни и са решаващи белези на блокчейните. Веднъж добавена транзакцията в регистъра, тя не може да бъде променяна. Интегритетът, подобно на конфиденциалността, разчита на криптографски механизми за техническа реализация.
- ***Достъпността*** се отнася за способността на потребителите да задействат функции в блокчейн-системата. Това свойство понякога се комбинира с друго – ***благонадеждност***, което се свързва с това, потребителите да получават последователно правилни резултати от задействането на тези функции.
- ***Отговорност*** може да се намери в организации, използващи блокчейн-технологии и имащи нужда от свързване на електронни действия с потребители. Отговорността е често свързана с изисквания за ***съвместимост*** с политиките на организацията. В друг контекст, отговорността може да бъде едно от предназначенията на дадено блокчейн-решение.
- Свойството ***непроменимост*** на блокчейн опосредства отговорността на извършени действия, но става по-сложно когато са използвани техники за ***анонимизация.***
- ***Одитируемост*** е често свързвана с *отговорност* – одитите обезпечават, че потребителите мога да бъдат държани под отговорност за техните действия, чрез преглеждане на одит-логове. Освен това одити или други видове оценки на сигурността помагат за идентификацията на уязвимости, или възможности за подобрение в архитектурата и софтуерния код на даден блокчейн или приложение. Нещо повече, когато одитите са независими и приложени към инфраструктурата на субект, който използва определено блокчейн-решение, адекватността на контролите за сигурност, въведени от организацията, могат да бъдат проучени, както и да бъде засечена зловредна дейност.
- ***Безопасност*** означава проектиране или използване на система, която не води до катастрофални последствия за потребителите и средата. Ако блокчейн се използва като компонент в приложение,

което е критично за безопасност, то отказ на компонент може да доведе до последствия за безопасността. Една различна гледна точка на безопасността включва проектирането на блокчейн, който е невредящ на околната среда, като например въвеждане на алгоритъм за единодушие, който води до по-нисък енергиен разход, отколкото при PoW, какъвто е случаят с Биткойн.

- Двигателят ***ремонтопригодност*** обозначава предразположеността на дадена система да претърпи промени и поправки. Обикновено блокчейн-решенията се променят/актуализират по-трудно, дори ако това би било жизненоважно за работата им, като например в случай на новооткрита уязвимост. Докато частните блокчейни могат да бъдат по-лесно актуализирани, защото тяхната децентрализация е между възлите, които са под контрола на една или няколко организации, то публичните блокчейни биха изисквали по-сложни механизми за доверие. Освен това някои блокчейни, като Етериум и Hyperledger, се считат за по-безопасни за актуализация, отколкото други (например Биткойн), поради техния модулен дизайн на архитектурата, който ограничава вероятността неумишлено да се повлияе негативно на друга функционалност при промяната на съответния код в блокчейн.
- ***Скалируемостта*** се свързва с други концепции – ***пропускателна способност*** (блокове, добавени към блокчейн за секунда) и ***производителност*** (количество данни/блокове, движещите се от една точка до друга за секунда). Постигането на повече скалируемост води до по-малко децентрализация и сигурност (интегритет и/или конфиденциалност).

### КРИПТОГРАФСКИ МЕХАНИЗМИ

Различни проблеми изискват различни криптографски решения. Тези проблеми могат да бъдат групирани в четири категории:

- ***Конфиденциалност на данни*** (понякога също наричана *поверителност* или *тайност*) обезпечава, че само желаният получател може да разбере едно съобщение.
- Механизми за ***интегритет на данни*** обезпечават, че умишленото или неумишленото изменение на данни се засича.
- ***Неопровержимост*** – изпращачът на съобщение не може да отрече, че е изпратил съобщението / не може да отхвърли притежаването на предходен ангажимент или действие.
- ***Автентификация*** – автентичността на изпращача е обезпечена.

Блокчейн-технологиите използват добре известни механизми от компютърните науки и криптографски примитиви (криптографски хеш-функции, дигитални сигнатури, асиметрична криптография), смесени с концепции за съхранение на записи.

- ***Криптографски хеш-функции*** се използват в много операции на блокчейн. Хешинг е методът за прилагане на криптографска хеш-функция към данни, който изчислява относително уникални изходни данни (дайджест) (digest) за входни данни, с какъвто и да е размер. Дори най-малката промяна на входните данни би довело до напълно различен дайджест на изходните данни. Затова хешингът обезпечава интегритета на данните.
- ***Транзакциите*** могат да включват адреса на изпращача или друг идентификатор; публичния ключ на изпращача; дигитална сигнатура; входни и изходни данни за транзакцията.
- ***Асиметричната криптография*** е широко използвана в блокчейн. В същността си тя се състои от един ключ, който може да бъде направен публичен и друг, който трябва да остане таен (частен ключ), за да могат данните да останат криптографски защитени. Частният ключ не може да бъде изчислен посредством публичния. Това позволява постигането на взаимоотношение на доверие между потребители, които не се познават или доверяват едни други, като се осигурява механизъм за проверка на интегритета и автентичността на транзакциите, и в същото време допускайки транзакциите да останат публични.

- ***Управление на криптографски ключове:*** Дори и да се използва силна криптографска технология, за да се достъпи даден блокчейн-адрес, компрометирането на частния ключ би позволило на неоторизирано лице да получи контрол върху адреса. Затова частните ключове, особено при неизискващи разрешение блокчейн-мрежи, трябва да бъдат защитени.

### МОДЕЛИ ЗА РАЗРАБОТКА НА СОФТУЕР

Заради свойството за сигурност на умните договори – *непроменимост*, наследено от базисната архитектура на DLT, традиционните модели за жизнен цикъл на софтуерната разработка (SDLC) са неподходящи, поне частично, за базирани на умен договор приложения, работещи на блокчейн. По-добър метод трябва да бъде изобретен, който адресира въпросите за непроменимостта, сложността на програмирането, разпределената същност на блокчейн-системите, алгоритъма за единодушие, и процесите за потвърждаване и валидиране от участващи възли.

### ТЕХНИКИ ЗА СИГУРНОСТ ПРИ РАЗРАБОТКАТА НА СОФТУЕР

Те включват *компонентно тестване; тестване на производителността /стрес-тест; преглед на код; тестване на функции/интеграция; тестова мрежа; статичен анализ; външни одити; специализирани екипи за сигурност; академични пиър-ревюта; инициативи за търсене на бъгове.*

### УЯЗВИМОСТИ И АТАКИ

Уязвимости, които биват открити в децентрализирани и неизискващи разрешение блокчейни, могат да бъдат трудни за разрешаване, когато тези блокчейни са вече в употреба. Трудността произтича от факта, че процесът за въвеждане на поправка на пролука в сигурността често изисква широко единодушие и обсъждане на алтернативни подходи.

Въпреки всичките усилия на програмистите и организациите, почти невъзможно е да се създаде блокчейн или приложение за него, които да могат да устоят на всички възможни атаки. Организациите, разработващи такива решения,

трябва да се подготвят да пускат поправки неотложно, веднага щом научат за дадена уязвимост. В определени случаи, обаче, архитектурни ограничения изискват поправки, които не могат да бъдат въведени бързо.

Друг проблем е софтуерът, който е създаван, за да комуникира с определен умен договор или блокчейн. Такъв софтуер може да бъде потребителски интерфейс, достъпен чрез браузър, инсталирана програма или мобилно приложение. В други случаи, той може да бъде друг вид интерфейс, например борса за криптовалути. Успешното експлоатиране на уязвимост в този вид софтуер или атаки със социално инженерство могат да доведат до компрометиране на механизмите за интегритет или конфиденциалност на транзакциите, или друг вид трансфери на данни, които тези интерфейси са проектирани да опосредстват.

### ПРЕДИЗВИКАТЕЛСТВА В СИГУРНОСТТА ПРИ ОРГАНИЗАЦИИТЕ

Различни правителствени и неправителствени организации са намесени в сферата на блокчейн. Проблемите, върху които те се фокусират, са обобщени както следва.

- Класификацията на блокчейн обикновено се основава на ***ограниченията на достъпа*** за организациите. Съществуват три вида блокчейн-мрежи: публични (обикновено без разрешение), частни (често с разрешение) и консорциум (подобни на частните). Решението за контрол на достъпа на субекти, които могат да се присъединят към мрежата, има импликации за избора на блокчейн-решение.
- Точното и достатъчното знание е критично за намаляване на рискове със сигурността в организации, използващи блокчейн, като например при кибератаки, вътрешни заплахи или технически прекъсвания. Ако се разделят елементите в тази екосистема, следните ***блокчейн-слоеве*** могат да бъдат разпознати: *приложения, умен договор, насърчаване, единодушие, мрежи, данни*.
- Предизвикателства при управлението на мрежи от правна перспектива: блокчейн може да бъде използван за легални и нелегални цели.

- Нуждата от сравняване на блокчейни.
- Доставчиците на продуктови решения за сигурност проучват блокчейн като инструмент за киберпрестъпност.
- Някои приложения на блокчейн могат да преобразуват и подобрят индустрията за информационна сигурност.
- Организации проучват разностранни аспекти на сигурността на блокчейн, включително уязвимости, атаки, рискове, методи за разработка на безопасен софтуер, неприкосновеност на личния живот и др.
- Одити и оценки в сигурността.
- Нуждата от талантливи професионалисти по сигурност.
- Новинарско съдържание за блокчейн-технологии.
- Правителствени агенции имат задачата да регулират организации, занимаващи се с блокчейн, и често криптовалути, които позволяват дигиталната размяна на монети и жетони.
- Безопасно внедряване на блокчейн-технологии. Това включва предизвикателства с оценката на риска; бизнес и ръководство; процеси; технологии.

### СИГУРНОСТ ОТ ПОТРЕБИТЕЛСКА ГЛЕДНА ТОЧКА

Потребители могат да се намесват в тази технологична област като използват блокчейн-базирани решения, не от името на организация, която те представляват, а за лични цели. Организации, които разработват или предоставят блокчейн-решения или информация, свързана с блокчейн, могат да извлекат полза от разбиране на нуждите на потребителите.

Потребителите на блокчейн-технологии често имат възможността да избират между няколко канала на учене – книги, форуми, уеб-базирани обучения, статии, раздели за помощ в уеб-сайтове на доставчици на блокчейн, обучения в учебна зала, видеа и др. Ученето може да е относно общата сигурност на блокчейн или безопасното ползване на конкретно блокчейн-решение.

Потребителите имат две основни перспективи към теми от сигурността:

- Какви практики от информационната сигурност потребителите трябва да вземат предвид, когато използват определено продуктово решение, свързано с блокчейн, на техните лични устройства и в физическа среда?

- Какви практики от информационната сигурност доставчиците на продуктови решения, свързани с блокчейн, е необходимо да въведат, които потребителите трябва да вземат предвид, когато решават дали да използват определени решения или услуги?

Някои от тези теми са изредени по-долу. Подобни проблеми могат да бъдат полезни и за организациите.

- Политики, процедури, стандарти и насоки за информационна сигурност и неприкосновеност на личния живот
- Сигурност на достъпа на трети страни
- Професионалисти по сигурност и сигурност на човешките ресурси
- Отговор на инциденти в сигурността и нарушения с неприкосновеността на личния живот
- Физическа сигурност на компютърно оборудване и помещения
- Защита от зловреден код
- Резервни копия и продължаване на бизнеса
- Мрежова и комуникационна сигурност
- Боравене с носители на данни
- Контрол на достъпа
- Контрол на операционни системи
- Мониторинг
- Мобилен и дистанционен достъп
- Криптография
- Разработка на безопасен софтуер
- Закони и регулации
- Прегледи и одити за сигурност и съвместимост
- Обслужване на клиенти

## ОБОБЩЕНИЕ НА ГЛАВА 2

- Архитектурата и разработката на което и да е блокчейн-решение изисква професионалисти с умения в няколко области на ИТ и не-ИТ, включително експерти по информационна сигурност. Поради сложността на всяко софтуерно решение, базирано или свързано с блокчейн, както и отсъствието на общи насоки и стандарти за разработка на безопасен блокчейн, доставчиците на решения са пред предизвикателството да въведат надеждни стратегии за пускане и поддържане на софтуер с адекватна степен на сигурност. Във всички случаи, целите на информационната сигурност – конфиденциалност, интегритет, достъпност, неприкосновеност на личния живот, отговорност и одитируемост остават приложими, и трябва да бъдат балансирани с цели за продуктивност и функционалност, като скалируемост, производителност и децентрализация.
- Множеството успешни атаки срещу блокчейн-технологии показва, че софтуер и системи са податливи на технически уязвимости, точно както традиционните технологични реализации. Все още предстои блокчейн-компаниите да намерят начини да минимизират рисковете ефективно, за да защитят своите блокчейн-продукти и услуги, репутация, клиенти, и да останат в бизнес.
- Съществуващи и нови организации са предприели стъпки да се занимават в тази иновативна технологична област, включително консултантски компании, регулатори, изследователски институции, доставчици на услуги за сигурност, компании за разработка на софтуер, както и много получатели на блокчейн-технологии. Всички организации имат подобна, но също така различна гледна точка за целите и нуждите на информационната сигурност, които се развиват с времето.
- Информационната сигурност може да бъде полезна и за крайните потребители. Частни лица, които обмислят използването на продуктови решения и услуги, свързани с блокчейн, трябва да могат да намират и организират релевантна, точна и достатъчна информация, за да минимизират рискове от грешки, измами и кибератаки.

## 3.3. ГЛАВА 3 – ОТКРИТИЯ. СТРАТЕГИИ ЗА ПОВИШАВАНЕ НА ПРИЛОЖИМОСТТА НА БЛОКЧЕЙН-ТЕХНОЛОГИИТЕ В КОНТЕКСТА НА ИНФОРМАЦИОННАТА СИГУРНОСТ

В третата и финална глава на изследването е използвана информацията от предходните глави, за да се отговори на двата изследователски въпроса. Освен това, въз основа на откритията, са предложени конкретни стратегии за повишаване на приложимостта на блокчейн-технологиите в контекста на информационната сигурност. По-специално, главата има следните задачи:

1) Определяне на най-важните аспекти на информационната сигурност, свързани с блокчейни.
2) Определяне на важността на тези аспекти от гледната точка на различните участници в тази технологична област.
3) Предлагане на стратегии за повишаване на приложимостта на блокчейн-технологиите в контекста на информационната сигурност.

### АСПЕКТИ НА ИНФОРМАЦИОННАТА СИГУРНОСТ - ОТКРИТИЯ

Изследването използва конкретна рамка и метода на обобщаване, за да установи 23 аспекта, в отговор на първия изследователски въпрос:

*Кои са най-важните аспекти на информационната сигурност, когато организации или индивиди започнат да се занимават с блокчейн-технологии?*

Тези открития са изредени в таблица 8.

*Таблица 8. Най-важните аспекти на информационната сигурност, свързани с блокчейн-технологиите.*

| | |
|---|---|
| **Аспект 1** | Устойчивост на фалшификации и непроменимост |
| **Аспект 2** | Устойчивост на единична точка на повреда |
| **Аспект 3** | Изложение на риск чрез софтуер, свързан с блокчейн |
| **Аспект 4** | Различни блокчейни изискват различна комплексност на контролите за сигурност |
| **Аспект 5** | Устойчивост на цензура |
| **Аспект 6** | Отстраняване на посредник (намаляване на риска от трети страни) |
| **Аспект 7** | Редуциране на човешки грешки |
| **Аспект 8** | Публичните блокчейни не са подходящи за специфични нужди от сигурност |
| **Аспект 9** | Криптография |

| | |
|---|---|
| **Аспект 10** | Теория на игрите и алгоритми за единодушие |
| **Аспект 11** | Произход и прозрачност |
| **Аспект 12** | Анонимност и псевдонимност |
| **Аспект 13** | Роли в блокчейн |
| **Аспект 14** | Блокчейните могат да бъдат част от иновативни решения със значимост за сигурността |
| **Аспект 15** | Блокчейните имат различни свойства за сигурност и степен на устойчивост |
| **Аспект 16** | Целите на информационната сигурност са широко приложими при блокчейн-технологии |
| **Аспект 17** | Контроли за информационна сигурност |
| **Аспект 18** | Разработка на безопасен софтуер и уязвимости |
| **Аспект 19** | Малуер и атаки |
| **Аспект 20** | Закони и регулации |
| **Аспект 21** | Рамки за сигурност, стандарти и насоки |
| **Аспект 22** | Скалируемост, пропускателна способност и производителност трябва да бъдат балансирани със сигурност |
| **Аспект 23** | Рискове, свързани с процеси, технологии, хора, и бизнес и ръководство |

### Важност на сигурността на блокчейн-технологиите за организации и индивиди

В тази част е използвана методология за сравнителен анализ, за да се отговори на втория изследователски въпрос:

*Каква е важността на сигурността на блокчейн-технологиите за различни организации и индивиди?*

*Важността* на информационната сигурност е директно свързана с *компетенции*. Доводът е, че субектите трябва да имат различен набор от минимални компетенции по информационна сигурност за адекватен отговор на проблеми на информационната сигурност, които са свързани с блокчейн-технологиите.

Методологията използва променливите в таблица 9 за обяснение и сравнение между девет категории от субекти (организации и индивиди).

*Таблица 9. Категории от компетенции и променливи за обяснение и сравнение между категориите субекти (организации и индивиди).*

| | |
|---|---|
| ***Познаване*** | Ниска/Средна/Висока/Променлива/Неприложимо |
| Познаването се отнася за знаене и разбиране на релевантния аспект/концепция. | |

| ***Интерпретация*** | Ниска/Средна/Висока/Променлива/Неприложимо |
|---|---|
| Интерпретацията се отнася за обясняване какво трябва и не трябва да се прави. | |
| ***Действие*** | Ниска/Средна/Висока/Променлива/Неприложимо |
| Действието се отнася за практическото въвеждане/изпълнение на цялостния аспект или релевантната част от него. | |

Сравнителният анализ включва 621 точки с данни за сравнение. Агрегираните резултати са показани в таблица 10.

*Таблица 10. Сравнителен анализ на аспектите на информационната сигурност при блокчейн-технологиите и тяхната важност за категории от субекти (агрегирано представяне).*

| | Разработващи | Поддържащи | Внедряващи | Регулиращи | Консултиращи и одитиращи | Изследващи | Докладващи | Използващи (организация) | Използващи (индивид) | *Сбор (хоризонтала)* |
|---|---|---|---|---|---|---|---|---|---|---|
| Брой на П-В | 13 | 11 | 10 | 9 | 9 | 1 | 0 | 0 | 0 | 53 |
| Брой на И-В | 11 | 10 | 8 | 4 | 3 | 0 | 0 | 0 | 0 | 36 |
| Брой на Д-В | 10 | 10 | 7 | 0 | 0 | 0 | 0 | 0 | 0 | 27 |
| Брой на П-С | 7 | 7 | 13 | 14 | 5 | 0 | 1 | 14 | 5 | 66 |
| Брой на И-С | 6 | 5 | 14 | 15 | 1 | 0 | 0 | 4 | 1 | 46 |
| Брой на Д-С | 1 | 3 | 9 | 0 | 0 | 0 | 0 | 0 | 0 | 13 |
| Брой на П-Н | 3 | 5 | 0 | 0 | 0 | 0 | 22 | 9 | 17 | 56 |
| Брой на И-Н | 6 | 8 | 1 | 4 | 0 | 0 | 23 | 18 | 20 | 80 |
| Брой на Д-Н | 7 | 9 | 5 | 0 | 0 | 0 | 0 | 13 | 1 | 35 |
| Брой на П-П | 0 | 0 | 0 | 0 | 9 | 22 | 0 | 0 | 1 | 32 |
| Брой на И-П | 0 | 0 | 0 | 0 | 19 | 23 | 0 | 1 | 1 | 44 |
| Брой на Д-П | 5 | 1 | 2 | 0 | 23 | 23 | 0 | 3 | 0 | 57 |
| Брой на П-Не | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 |
| Брой на И-Не | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 0 | 1 | 1 |
| Брой на Д-Не | 0 | 0 | 0 | 23 | 0 | 0 | 23 | 7 | 22 | 75 |
| *Сбор (вертикала)* | 69 | 69 | 69 | 69 | 69 | 69 | 69 | 69 | 69 | 621 |

Следните общи наблюдения могат да бъдат направени:

- *Разработващи, поддържащи, внедряващи* и *регулиращи* организации обикновено имат нужда от задълбочена или напреднала степен на компетенции за мнозинството аспекти на информационната сигурност.

- *Докладващи, използващи (организация)* и *използващи (индивид)* са субекти, които имат нужда предимно от ниска степен на компетенции за мнозинството от аспектите на информационната сигурност и нито един от тях обикновено няма нужда от най-високата степен (задълбочена).
- *Консултиращи и одитиращи* и *изследващи* субекти могат да имат нужда от различна степен на компетенции по информационна сигурност, защото в различни случаи те се фокусират върху различни аспекти.
- Различни субекти може да имат необходимост от компетенции по информационна сигурност в една и съща категория и с подобна степен, но в края на краищата да се фокусират върху различни особености.
- Някои субекти могат да са атипични и да изискват различно ниво на компетенции, отколкото е установено в този анализ.
- В сценарий от реалния живот, един субект може да се вмества в повече от една категория.
- По-дълбокото занимание с блокчейн-технологии увеличава общата степен на важност на отделни аспекти на информационната сигурност и обратното.

## СТРАТЕГИИ ЗА ПОВИШАВАНЕ НА ПРИЛОЖИМОСТТА НА БЛОКЧЕЙН-ТЕХНОЛОГИИТЕ В КОНТЕКСТА НА ИНФОРМАЦИОННАТА СИГУРНОСТ

В изследователската работа са предложени конкретни стратегии за повишаване на приложимостта на блокчейн-технологиите в контекста на информационната сигурност. Стратегиите демонстрират полезността на откритията в предходните подглави във връзка с *Изследователската теза*. Стратегиите са изредени в таблица 11.

*Таблица 11. Списък на стратегии за повишаване на приложимостта на блокчейн-технологиите в контекста на информационната сигурност.*

| | | |
|---|---|---|
| **1** | Специфична за блокчейн | Подкрепа за иновации |
| **2** | Специфична за блокчейн | Преосмисляне на устойчиви на подправяне данни и системи |
| **3** | Специфична за блокчейн | Подобряване на достъпността на данни и системи |
| **4** | Неспецифична за блокчейн | Обезопасяване на блокчейн-платформата и други системи и приложения, които взаимодействат с блокчейна |

| | | |
|---|---|---|
| **5** | Специфична за блокчейн | Измерване на комплексността на операциите по сигурност на блокчейн |
| **6** | Специфична за блокчейн | Устойчивост на цензура като заплаха и възможност |
| **7** | Специфична за блокчейн | Подобряване на съществуващи процеси |
| **8** | Неспецифична за блокчейн | Развитие на способности в криптографията |
| **9** | Специфична за блокчейн | Изследване на алгоритми и протоколи за единодушие |
| **10** | Специфична за блокчейн | Извличане на полза от анонимност или неанонимност |
| **11** | Специфична за блокчейн | Реконструиране на организационни роли |
| **12** | Специфична за блокчейн | Преформулиране на цели на информационната сигурност |
| **13** | Неспецифична за блокчейн | Създаване и използване на подходящи контроли за сигурност |
| **14** | Специфична за блокчейн | Създаване на стабилни процеси за разработката на безопасен софтуер |
| **15** | Неспецифична за блокчейн | Управление на заплахи и защита от малуер и атаки |
| **16** | Специфична за блокчейн | Разбиране на последиците от закони и регулации |
| **17** | Специфична за блокчейн | Балансиране на сигурност, скалируемост и производителност |
| **18** | Неспецифична за блокчейн | Използване на методи и техники за оценка на риска |
| **19** | Неспецифична за блокчейн | Използване на стандарти, рамки и насоки |

## ОБОБЩЕНИЕ НА ГЛАВА 3

- Първо са идентифицирани 23 основни групи с аспекти за информационна сигурност, които са важни, съществени, критични или жизненоважни в сферата на блокчейн-технологиите. Някои от тях са уникални за блокчейни и свързани решения, например произход, прозрачност и алгоритми за единодушие. Други са приложими и за други технологии, например криптография, защита чрез контроли за информационна сигурност и анонимност. Във всички случаи аспектите имат специфични за блокчейн характеристики. Тази част отговаря на първия изследователски въпрос.

- Второ, значението на 23-те аспекта на информационната сигурност е определено за няколко категории организации и индивиди, в зависимост от вида на тяхното занимаване с блокчейн. Тази цел е постигната чрез извършване на сравнителен анализ с общо 621 отделни точки с данни.
- Като цяло резултатите от анализа показват, че уникалните характеристики на феномена блокчейн имат променливо значение от гледната точка на организации с различно взаимоотношение с блокчейните и свързаните с тях продуктови решения. Разкрива се, че организациите, които разработват, внедряват, поддържат или регулират такива технологии, трябва да имат задълбочени или напреднали компетенции относно тяхната сигурност. За разлика от тях, обикновените получатели (потребители) на такива технологии трябва да имат базисни компетенции. Този анализ отговаря на втория изследователски въпрос.
- На последно място, предложени са 19 управленски стратегии с релевантност за информационната сигурност, базирани на откритията, за да се помогне на организациите да постигнат целите си. Някои от тези стратегии са специфични за блокчейн, докато други вече се използват широко за други видове технологии. Специалистите по информационна сигурност и организационно управление могат да разширят тези стратегии в подробни задачи, приспособени към желания приложен сценарий на блокчейн или свързано продуктово решение.

# 4. ЗАКЛЮЧЕНИЕ

Дисертационният труд изследва сферата на блокчейн-технологиите от перспективата на теорията за информационна сигурност. Изследването цели да помогне на практици (и особено мениджъри) в сигурността като отговори подробно на два изследователски въпроса и след това предложи релевантни за информационната сигурност стратегии за повишаване на приложимостта (полезността) на блокчейн-технологиите.

**Изследователската стратегия** включва преглед и анализ на голям брой източници на информация (общо 148) чрез качествени методи. Основната цел е използването им за идентифициране на релевантни понятия и описване и обяснение на съществени аспекти и явления. Някои от източниците са използвани и за подпомагане на изготвянето на методологията и структурата на изследването.

**Основните приноси на изследването са:**

- Идентифициране на фундаментите на блокчейн-технологиите и обяснението им по кратък, точен и ясен начин.
- Обяснение на взаимоотношението между фундаментите на теорията за информационна сигурност и блокчейн-технологиите. Също така, определяне на *важността на информационната сигурност при блокчейн-технологиите за организации и индивиди*.
- Идентифициране на ключови аспекти на информационната сигурност, които са свързани с блокчейн-технологиите.
- Сравняване на степента на важност на информационната сигурност (компетенции) между категории организации и индивиди.
- Предлагане на управленски стратегии с широко приложение за повишаване на приложимостта на блокчейн-технологиите чрез методи, релевантни за информационната сигурност.

**Като цяло** изследването постига всяка от своите задачи, дефинирани в раздел *УВОД*. Разработката очертава полезна „обща картина“ на най-важните аспекти на информационната сигурност, свързани с блокчейн-технологиите, без несъществени подробности. Това очертание е основен принос както в областта на блокчейн, така и в сигурността. Специалистите и мениджърите по информационна сигурност могат да използват разработката като първостепенен източник за справка за информационна сигурност, когато организациите се намесват в сферата на блокчейн-технологиите**.**

# 5. ПУБЛИКАЦИИ

Авторът е написал пет публикации, свързани с изследването (виж таблица 12). Те са финализирани и приети за публикуване по време на писането на дисертационния труд. Три от тях са приети за публикуване в IEEE Conference Proceedings, след двойно-сляпо ревю от независими пиъри.

*Таблица 12. Специфики на публикациите към дисертационния труд.*

| No. | Издателство | Език | Година | Пиър ревю | Индексирана в | Представена на конференция | Фокус област | Тип |
|---|---|---|---|---|---|---|---|---|
| 1 | IEEE Conference Proceedings | Английски | 2020 | Двойно-сляпо | Scopus | ДА | Блокчейн + Информационна сигурност | Практическа насоченост |
| 2 | | | | | | | | |
| 3 | | | | | | | Информационна сигурност | |
| 4 | Научно-технически съюз по машиностроене "Индустрия - 4.0" | Български | 2020 | НЕ | Неприложимо | НЕ | Блокчейн + Информационна сигурност | Научна |
| 5 | | | | | | | | |

| | Заглавие на публикацията | Връзка с изследователската работа |
|---|---|---|
| 1 | Измерване на оптималната комплексност на информационната сигурност за операции в блокчейн | Разширява стратегия no. 5 от глава 3 на изследователската работа |
| 2 | Дефиниране и прилагане на цели на информационната сигурност за блокчейн-технологии | Разширява стратегия no. 12 и 13 от глава 3 на изследователската работа |
| 3 | Организационна оценка на зрелостта на информационната сигурност, базирана на ISO 27001 и ISO 27002 | Свързана с предмета на изследователската работа и стратегия no. 19 от глава 3 |
| 4 | Блокчейн-технологиите в контекста на целите на информационната сигурност | Проучва концепции от глава 1 - *Теоретична рамка* на изследователската работа |
| 5 | Ключови концепции от информационната сигурност, приложени при блокчейн-технологиите | Проучва концепции от глава 1 - *Теоретична рамка* на изследователската работа |