

РИСКОВЕ ПРИ ВНЕДРЯВАНЕТО НА СМАРТ ТЕХНОЛОГИИ В ГРАДСКАТА СРЕДА

Доц. д-р Михаил Чиприянов

СА „Д. А. Ценов“ – Свищов

m.chipriyanov@uni-svishtov.bg

Резюме: В рамките на настоящото изследване се осъществява комплексен и критичен анализ на основните рискове, произтичащи от внедряването на смарт технологии в градската среда, фокусирайки се върху предизвикателствата пред киберсигурността, финансовата устойчивост, социалната адаптация и регулаторната адекватност. Идентифицират се ключови проблеми като уязвимостта на IoT устройствата, финансовата тежест на имплементацията, дигиталното разделение и липсата на унифицирани правни рамки. В резултат на анализа се формулират конкретни стратегии за минимизиране на тези рискове, включващи публично-частни партньорства, финансови иновации, повишаване на дигиталната грамотност и създаване на адаптивни регулаторни подходи. Изводът е, че успешното развитие на интелигентните градове е пряко зависимо от холистичното управление на тези многоаспектни рискове.

Ключови думи: Смарт градове, Киберсигурност, Финансови рискове, Социални предизвикателства, Регулаторни рамки.

JEL: O33, H11, R53

RISKS IN THE IMPLEMENTATION OF SMART TECHNOLOGIES IN URBAN ENVIRONMENTS

Assoc. Prof. Mihail Chipriyanov, PhD

DA Tsenov Academy of Economics – Svishtov

Abstract: Within the scope of the present study, a comprehensive and critical analysis is conducted on the main risks arising from the implementation of smart technologies in urban environments, focusing on challenges to cybersecurity, financial sustainability, social adaptation, and regulatory adequacy. Key issues identified include the vulnerability of IoT devices, the financial burden of implementation, the digital divide, and the lack of unified legal frameworks. As a result of the analysis, specific strategies for minimizing these risks are

formulated, encompassing public-private partnerships, financial innovations, enhancement of digital literacy, and the creation of adaptive regulatory approaches. The conclusion drawn is that the successful development of smart cities is directly dependent on the holistic management of these multifaceted risks.

Keywords: *Smart cities, Cybersecurity, Financial risks, Social challenges, Regulatory frameworks.*

Въведение

Внедряването на смарт технологии трансформира съвременните градове, осигурявайки a priori повишена ефективност, подобрени услуги и по-добро качество на живот. Този процес обаче не е лишен от съществени предизвикателства и рискове. Докато потенциалните ползи са значителни, подценяването на присъщите проблеми би могло да доведе до сериозни негативни последици. С нарастващото внедряване на смарт технологии в градската среда и индустриалните процеси, въпросът за киберсигурността и защитата на данните се превръща в критичен аспект на дигиталната трансформация. Интеграцията на интернет на нещата (IoT), изкуствения интелект (ИИ) и големите данни (Big Data) увеличава свързаността между устройствата, но едновременно с това разширява повърхността на потенциалните атаки. Смарт градовете разчитат на интензивен обмен на информация между различни системи (*енергийни мрежи, транспортни инфраструктури, публични услуги и административни платформи*), което създава предпоставки за *неоторизиран достъп, кибератаки, манипулация на данни и компрометиране на критични услуги*.

Анализът ще е с фокус върху основните рискове, свързани с разширяването на смарт градските концепции, фокусирайки се върху *проблемите на киберсигурността, финансовите и инвестиционни рискове, както и социалните и регулаторни предизвикателства*. Считаме, че оценяването на тези аспекти е от ключово значение за разработването на устойчиви и сигурни градски стратегии в ерата на дигиталната трансформация.

Основната *цел* на настоящото изследване е да се извърши *комплексен и критичен анализ на основните рискове*, произтичащи от широкомащабното внедряване на смарт технологии в урбанистичната среда. Предполага се идентифициране, категоризация и оценка на въздействието на тези рискове, с акцент върху *киберсигурността, финансовите и инвестиционни аспекти, както и социалните и регулаторни*

предизвикателства. Стремежът е да се формулират адекватни стратегии и препоръки за минимизиране на тези рискове, допринасяйки за устойчивото и сигурно развитие на интелигентните градове.

Обект на настоящото изследване са процесите на внедряване и функциониране на смарт технологии в градските екосистеми. Обхваща се цялостната дигитална инфраструктура, вкл. IoT устройства, ИИ системи, Big Data анализи, комуникационни мрежи (напр. 5G), както и свързаните с тях градски услуги и управленски модели. Акцентът е върху взаимодействието на тези технологии с градската среда и заинтересованите страни.

Предмет на изследването са идентифицираните и систематизирани рискове, които произтичат от внедряването и експлоатацията на смарт технологии в градската среда. Конкретните аспекти включват:

- Рискове за киберсигурността (уязвимости, заплахи, потенциални атаки и техните последици за градската инфраструктура и данни);*
- Финансови и инвестиционни рискове (високи капиталови разходи, несигурност на възвръщаемостта, разходи за поддръжка, както и модели за тяхното финансиране);*
- Социални предизвикателства (проблеми с дигиталната грамотност, обществено доверие, неприкосновеност на личния живот, промени в заетостта и социална адаптация);*
- Регулаторни предизвикателства (липса на адекватни законодателни рамки, непоследователност в политиките, етични дилеми при използване на ИИ и управление на данни).*

В настоящото изследване ще бъде приложена комбинирана методология, която интегрира както класически, така и съвременни подходи за анализ: индукция, дедукция, анализ и синтез.

Тезата е, че устойчивото и успешно внедряване на смарт технологии в градската среда е пряко зависимо от проактивното и комплексно управление на присъщите рискове за киберсигурността, финансовата устойчивост, социалната адаптация и регулаторната адекватност. Омаловажаването на което и да е от тези измерения може да компрометира потенциалните ползи от дигиталната трансформация, превръщайки иновациите в източник на нови проблеми, вместо на решения. Изследването ще демонстрира, че само чрез прилагането на един интегриран подход,

който балансира технологичния напредък с внимателно адресиране на тези рискове, може да се постигне истински интелигентен и устойчив град.

1.Проблеми на киберсигурността по релацията „свързаност – уязвимост“

Възходът на умните градове е неразривно свързан с безпрецедентна свързаност и автоматизация, обещаващи революция в градското управление и качеството на живот. Дигиталната трансформация обаче изгражда сложна мрежа от взаимозависими системи, превръщайки киберсигурността от технически проблем в централен „стълб“ на градската устойчивост. Метафорично казано, именно тази висока степен на свързаност, която по дефиниция предполага умния град, се оказва неговата потенциална Ахилесова пета. Всеки сензор, всяко свързано устройство и всеки гигабайт данни представляват потенциална точка на уязвимост, откривайки широки възможности за злонамерено влияние. (Ahsan, 2022, 2 (3))

(Oladipo, 2024, 11 (1)) (Wang, August 2015)

По-долу ще дискутираме как тази разширяваща се „дигитална повърхност“ създава експоненциално растящи рискове, трансформирайки традиционните представи за киберсигурност и налагайки преосмисляне на защитните стратегии в градската среда.

Таблица 1

Основни рискове за киберсигурността при внедряване на смарт технологии в градската среда (*Източник: собствена интерпретация*)

Фактор на риска	Описание	Потенциални последствия
<i>Експоненциално разрастване на IoT екосистемата в градска среда</i>	Нарастващият брой и разнообразие от свързани IoT устройства (сензори за трафик, осветление, измерване на замърсяване, умни водомери, камери за наблюдение и др.) в градската инфраструктура, много от които проектирани без адекватни мерки за сигурност, представляват обширна и слабо защитена входна точка за атаки.	Неоторизиран достъп до критични градски системи; компрометиране на данни за граждани и инфраструктура; широкомащабни прекъсвания или манипулации на градски услуги (напр. спиране на улично осветление, промяна на сигнализация на трафика, изтичане на информация от публични камери); използване на компрометирани устройства за DDoS атаки срещу други цели.
<i>Комплексност и децентрализация на мрежовата архитектура на умните градове</i>	Разпределената обработка на данни, включваща множество облачни платформи, локални (edge) изчислителни възли, 5G мрежи и разнообразни комуникационни протоколи, създава изключително сложна и фрагментирана мрежова	Повишен риск от проникване поради множество потенциални уязвими точки; затруднено централизирано наблюдение и управление на сигурността; възможност за "странични" атаки, използващи слабо

	среда. Управлението на сигурността в тази хетерогенна система е предизвикателство.	защитени периферия; каскадни откази при компрометиране на един компонент.
<i>Липса на унифицирани стандарти и оперативна съвместимост за сигурност</i>	Различните производители на смарт градски технологии и решения използват разнообразни, често несвързани, протоколи и стандарти за сигурност. Това води до фрагментация, несъвместимост на защитните механизми и създава "пропуски" в общата защитна стратегия на града.	Неефективна интеграция на защитни системи; поява на неизвестни уязвимости при взаимодействието на разнородни системи; високи разходи за прилагане на индивидуални решения за сигурност; липса на консистентен подход за актуализации.
<i>Смарт критични инфраструктури като основни цели на кибератаки</i>	Интегрирането на смарт технологии в жизненоважни градски инфраструктури като енергийни мрежи (умни електромери, разпределителни подстанции), транспортни системи (автономни превозни средства, интелигентно управление на трафика), водоснабдяване и пречиствателни станции, системи за здравеопазване и спешни услуги – ги превръща в изключително атрактивни цели за организирани кибератаки с потенциално катастрофални последици.	Мащабно спиране на основни обществени услуги (ток, вода, транспорт); парализиране на градския живот и икономическа дейност; заплаха за човешки животи и здраве; национална сигурност; паника сред населението.
<i>Масивно събиране и обработка на лични и чувствителни данни на гражданите</i>	Смарт технологиите в градската среда събират и анализират огромни обеми от данни, включително лична информация (движение, потребление, здравен статус, поведение), видео наблюдение и биометрични данни. Което увеличава многократно риска от неправомерно използване, изтичане или злоупотреба с тази информация.	Мащабни нарушения на регулациите за поверителност (напр. GDPR); сериозни финансови санкции за градските власти; компрометиране на личното пространство и свободите на гражданите; загуба на обществено доверие в инициативите за умни градове; риск от дискриминация или таргетиране на индивиди.
<i>Ограничени ресурси и експертиза в общинските администрации</i>	Много общински администрации, особено в по-малките градове, нямат необходимия бюджет, специализиран персонал или експертиза в областта на киберсигурността, за да управляват и защитават сложността на смарт градските системи.	Неадекватно прилагане на мерки за сигурност; забавено откриване и реакция на инциденти; зависимост от външни доставчици без достатъчен контрол; пропуски в обучението на персонала; увеличаване на вероятността от успешна атака.
<i>Верига на доставки и зависимости от трети страни</i>	Внедряването на смарт градски технологии често включва множество доставчици на хардуер, софтуер и услуги. Уязвимости в продуктите или процесите на един доставчик крият опасност да компрометират цялата градска инфраструктура.	Възможност за атаки по веригата на доставки; въвеждане на "задни вратички" или малуер чрез компрометирани компоненти; затруднения при проследяване на източника на уязвимости; проблеми с актуализации и поддръжка от страна на доставчици.

В условията на все по-разрастващата се дигитална екосистема на умните градове, където всеки елемент е потенциална входна точка за атака, пасивната защита е недостатъчна. За да се гарантира не само сигурността на смарт технологиите, но и устойчивостта и функционалността на цялата градска среда, е наложително да се приложат *цялостни, проактивни и адаптивни стратегии*. (Лучков К. , **Значение на технологичните иновации и дигитализацията за устойчивото развитие, 2024**) (Веселинова, **Насърчаване на отворени иновации в публичния сектор чрез инкубатори и акселератори, 2025, 23**) Мерките би било добре да обхващат всяко ниво на взаимодействие, от хардуерния сензор до най-високото ниво на управление на данни, създавайки многопластов щит срещу постоянно еволюиращите киберзаплахи.

1.Фундаментална криптографска защита. В свят, в който данните са новата градска валута, тяхната конфиденциалност и интегритет са от първостепенно значение. Необходимо е *задължително и повсеместно използване на съвременни криптографски протоколи* не само за предаване, но и за съхранение на информация през целия и жизнен цикъл. Това включва сигурно криптиране на данни "в покой" (data at rest) в облачни хранилища и локални устройства, както и "в движение" (data in transit) през всички комуникационни канали – от IoT устройства до централните сървъри. Прилагането на авангардни криптографски алгоритми, устойчиви дори на бъдещи квантови атаки, е критично за предотвратяване на неоторизиран достъп и манипулация на жизненоважни градски данни.

2.Многофакторна автентикация и прецизен контрол на достъпа. Идентифицирането и контролът върху всеки, който взаимодейства с градските дигитални системи, са ключови за минимизиране на риска. Прилагането на *строга многофакторна автентикация (MFA)* е необходимо да бъде стандарт за достъп до всички критични градски инфраструктури и данни, надхвърляйки обикновените пароли чрез интегриране на биометрични методи (напр. пръстови отпечатаци, лицево разпознаване) и хардуерни токени. Успоредно с това, *моделът на достъп, базиран на роли (Role-Based Access Control – RBAC)*, трябва да бъде стриктно прилаган, гарантирайки, че само оторизиран персонал има достъп до специфични данни и функционалности, в съответствие с принципа на най-малко привилегии.

3.Иновации с блокчейн за повишена надеждност. Концепцията за децентрализираните регистри, каквато е *блокчейн технологията*, предлага изключителен потенциал за повишаване на сигурността и интегритета на данните в градската среда. Чрез разпределено съхранение и криптографски свързани записи,

блокчейн може да осигури *надеждност, неизменяемост и прозрачност* на критични данни и транзакции. Неговото приложение може да обхване веригите за доставка на умни градски компоненти, удостоверяване на идентичност на устройства и граждани, както и осигуряване на интегритет на сензорни данни, което прави манипулацията практически невъзможна и създава ново ниво на доверие в дигиталната инфраструктура.

4. *Комплексни регулаторни рамки и унифицирани стандарти.* Несъвършенствата в законодателството и липсата на единни технически стандарти са сред най-големите пречки пред киберсигурността на умните градове. Необходимо е *разработването и внедряването на глобални и национални регулаторни рамки*, които да дефинират минимални изисквания за киберсигурност за всички компоненти на градската смарт инфраструктура. Въпросните регулации да бъдат подкрепени от *унифицирани технически стандарти и сертификационни процеси*, осигуряващи съвместимост, оперативна съвместимост и вградена сигурност (security by design) още на етап проектиране и производство.

5. *Динамичен мониторинг и проактивна реакция.* Киберсигурността не е еднократен акт, а непрекъснат процес. Създаването и оперативното функциониране на *Центрове за операции по сигурността (Security Operations Centers – SOC's)*, специализирани за градската инфраструктура, е абсолютно наложително. Те да осъществяват *непрекъснат мониторинг в реално време* на мрежовия трафик, системите и приложенията, посредством използването на прогресивни аналитични инструменти и ИИ за *автоматизирано откриване и неутрализиране на заплахи*. Бързата и координирана реакция при инциденти, съчетана с редовни тестове за проникване и учения, ще гарантира минимално прекъсване на услугите и бързо възстановяване след атаки, поддържайки "пулса" на градската защита стабилен. (Radu, 9-10 June 2016)

Инвестициите в киберсигурността на смарт технологиите не следва да се възприемат като маргинален или допълнителен разход, а напротив - като *фундаментален императив за устойчивата еволюция на дигиталната трансформация*. Инвестициите, от една страна, осигуряват оперативна *надеждност и транспарентност*, а от друга страна, което е по-съществено, те консолидират *доверието* – неделим капитал, без който модерните градски системи биха били лишени от своята функционална пълноценност и потенциал за реализация. Игнорирането на този критичен аспект би било еквивалентно на конструиране на архитектурна структура с прозаична нестабилност, обречена на дезинтеграция при първия значителен външен стрес.

2. Финансови и инвестиционни рискове при имплементацията на смарт технологии - икономическата дилема и латентните разходи

След като анализирахме дълбочината на всеобхватните предизвикателства пред киберсигурността, е наложително да пристъпим към разглеждане на друга съществена бариера пред мащабното разгръщане на смарт технологиите – *финансовите и инвестиционни рискове*. (Mubanani, 2023, 2.1) (Mehrotra, 24-26 April 2019) Въпреки че прокламираните ефективност и оптимизация излъчват значителна атрактивност, пътят към една "интелигентна" градска среда е осеян с комплексни, често *подценени икономически предизвикателства*. Посочните рискове не се ограничават само до първоначалните инвестиции, а екстензивно обхващат целия жизнен цикъл на технологичните системи, включително непредвидените оперативни разходи за поддръжка, периодични актуализации и управление на непредвидени ситуации.

Внедряването на смарт технологии изисква значителни капиталови инвестиции, които могат да представляват *финансово предизвикателство* както за частния сектор, така и за публичните институции. Високите първоначални разходи, сложността на технологичните решения и *несигурността на възвращаемостта* могат да забавят или дори да възпрепятстват устойчивото финансиране на такива проекти.

Разходна структура и инвестиционни предизвикателства. Финансовите рискове, свързани със смарт технологиите, могат да бъдат класифицирани в няколко основни направления:

1. *Високи капиталови разходи (CAPEX)* – значителните първоначални инвестиции, необходими за изграждането на интелигентни инфраструктури, като умни мрежи, интелигентни сензори и автоматизирани системи за управление;
2. *Оперативни разходи (OPEX)* – дългосрочните разходи за поддръжка, надграждане и управление на внедрените технологии, включително разходи за енергийна ефективност, софтуерни актуализации и киберсигурност;
3. *Несигурност в дългосрочната възвращаемост на инвестициите (ROI)* – трудността при прогнозиране на икономическите ползи и времевия хоризонт за изплащане на инвестициите; (Чиприянова, 2014, 3)
4. *Регулаторни и политически рискове* – липсата на ясна правна рамка за финансиране и експлоатация на смарт технологии, което да се отрази в непредвидени разходи или несигурност в инвестициите;

5. *Пазарни рискове* – динамиката на технологичния сектор да доведе до бързо остаряване на дадена технология, което да намали нейната ефективност и рентабилност.

В табл. 2 са представени основните категории инвестиционни рискове и тяхното влияние върху устойчивото финансиране на смарт технологии.

Таблица 2

Сравнителен анализ на инвестиционните рискове

(Източник: собствена интерпретация)

Категория на риска	Описание	Влияние върху устойчивостта	Потенциални стратегии за минимизиране
<i>Капиталови разходи (CAPEX)</i>	Високи първоначални разходи за закупуване и внедряване на технологии.	Възможно ограничаване на инвестициите и забавяне на проектите.	Държавни субсидии, публично-частни партньорства, дългосрочни заеми с ниски лихви.
<i>Оперативни разходи (OPEX)</i>	Постоянни разходи за поддръжка, надграждане и сигурност на системите.	Високи дългосрочни разходи, които могат да ограничат бюджетите на организациите.	Оптимизация на разходите чрез автоматизация, използване на ИИ и predictive maintenance. (Chipriyanova, 2022, 2)
<i>Несигурност на ROI</i>	Трудност при измерване на дългосрочните ползи от инвестициите.	Намаляване на инвестиционния интерес, поради липса на гарантирана възвращаемост.	Разработване на ясни бизнес модели и стратегии за финансова устойчивост.
<i>Регулаторни рискове</i>	Липса на стабилна правна рамка за дигитализация и смарт технологии.	Несигурност за инвеститорите и потенциални правни пречки.	Създаване на национални стратегии и политики за дигитална трансформация.
<i>Пазарни рискове</i>	Бърза технологична еволюция и остаряване на внедрените системи.	Необходимост от постоянни инвестиции в нови технологии.	Гъвкави бизнес модели, които позволяват адаптация към технологични промени.

В контекста на съвременните градски трансформации, където внедряването на смарт технологии изисква значителни капиталовложения и крие присъщи финансови рискове е от критично значение да се разработят и приложат *ефективни финансови механизми и авангардни модели за управление на риска*. Целта е не просто да се осигури

устойчиво финансиране, а да се оптимизира капиталовата структура, да се диверсифицира рискът и да се гарантира максимална възвръщаемост на инвестициите в дългосрочен план. Едни подходящи решения в тази връзка касаят:

1.Интеграция на публично-частни партньорства (ПЧП). Моделът на ПЧП се утвърждава като един от най-ефективните подходи за смекчаване на финансовата тежест върху публичния сектор, като същевременно стимулира инвестициите в комплексни смарт градски проекти. Чрез ПЧП се постига *синергично разпределение на инвестиционния риск* между държавни и общински структури и частни компании. Тази колаборация, първо, осигурява достъп до допълнителни финансови ресурси, и второ, привлича експертиза, иновативни технологични решения и оперативна ефективност от частния сектор, което е трудно постижимо чрез изцяло публично финансиране. ПЧП позволяват прехвърляне на част от проектния и оперативен риск към партньори, които имат по-голям капацитет да го управляват, като същевременно се запазва публичният контрол върху стратегическата визия и обществения интерес.

2.Държавни субсидии и фискални стимули - катализатори за стратегически инвестиции. За да се насърчи внедряването на смарт технологии с висока обществена значимост и дългосрочни ползи, които невинаги могат да бъдат монетизирани изцяло, е необходимо прилагането на *целенасочени държавни субсидии и фискални стимули*. Горното включва механизми като *данъчни облекчения* за инвестиции в иновативни градски инфраструктури, *директни грантове* за пилотни проекти и изследвания, както и *нисколихвени заеми* или гарантирани кредитни линии. Посочените мерки биха намалили първоначалния финансов натиск върху общинските бюджети и частните инвеститори и биха сигнализирали за национален приоритет, привличайки допълнителен капитал и ускорявайки дифузията на технологиите.

3.Финансови иновации и устойчиво финансиране. Развитието на смарт градовете изисква активирането на *нови, устойчиви капиталови потоци*, които надхвърлят традиционните финансови инструменти. Използването на *зелени облигации (green bonds)*, *социални облигации (social bonds)* и *ESG-ориентирано инвестиране (Environmental, Social, Governance)* представлява ключова стратегия в това отношение. (Лучков К. С., 2024) (Веселинова, Интегриране на ESG критерии в бизнес планирането, 25-26 октомври 2024) (Лучков К. , ESG - целево-ориентиран подход към устойчивото развитие, 2023) Откритите иновативни финансови инструменти позволяват привличането на капитал от инвеститори, които целенасочено търсят проекти с положителен екологичен и социален отпечатък, като по този начин се разширява базата

на потенциалните финансиращи страни и се създава пазар за устойчиви градски проекти. Това има потенциал да диверсифицира източниците на финансиране, и да интегрира критериите за устойчивост в инвестиционните решения. (Chipriyanova G., 2023)

4. *Дългосрочно планиране и проактивно прогнозиране - емпирична основа за инвестиционни решения.* Минимизирането на финансовите рискове изисква отказ от краткосрочната перспектива и възприемане на *дългосрочно, стратегическо планиране и прецизно прогнозиране*. Което предполага *разработването на детайлни икономически обосновки и бизнес модели*, базирани на задълбочен анализ на *разходите и ползите (Cost-Benefit Analysis – CBA)* през целия жизнен цикъл на смарт градските системи. Анализът следва да включва не само директните финансови параметри, но и индиректните ползи (напр. намалено замърсяване, по-добра ефективност на услугите, повишена безопасност) и разходи (напр. социални въздействия, рискове за сигурността), които могат да бъдат остойностени. Описаният подход гарантира *оптимално разпределение на ресурсите*, идентифицира потенциални "тесни места" и позволява проактивно управление на финансовите предизвикателства.

5. *Гъвкави договорни отношения с технологични доставчици.* С оглед на бързото темпо на технологичните иновации, традиционните, фиксирани договори с технологични доставчици могат да се окажат финансово неизгодни в дългосрочен план. Затова е критично *подписването на гъвкави договорни споразумения*, които включват клаузи за *адаптиране на внедрените технологии* към бъдещи иновации и променящи се нужди, без да водят до значителни допълнителни разходи. Имат се предвид най-вече модулни архитектури, отворени стандарти, клаузи за актуализации, възможности за мащабиране (scalability) и преносимост на данни, както и договорни механизми за споделяне на риска, свързан с технологичната остарялост. Подобни договори гарантират, че градските инвестиции остават релевантни и ефективни през целия си жизнен цикъл, минимизирайки риска от "заклучване" в остарели или скъпи решения.

Макар да изглежда, че финансовите и инвестиционни рискове да представляват *съществено предизвикателство* пред широкомащабната имплементация на смарт технологии в градската среда, те не са непреодолими. Чрез адекватни стратегии за управление на капиталовите разходи, стимулиране на финансови иновации и целенасочена регулаторна подкрепа, те могат да бъдат *значително редуцирани*. Устойчивият икономически ефект от дигиталната трансформация в градски контекст зависи не само от стремителния технологичен напредък, но и от *способността на*

обществото да финансира и администрира тези сложни процеси по методически издържан и дългосрочно устойчив начин.

3. Социални и регулаторни предизвикателства при внедряването на смарт технологии

Имплементирането на смарт технологии в урбанистичната среда и индустриалния сектор е процес, който надхвърля чисто *техническите и финансови аспекти*, трансформирайки се в изключително *сложен социален и регулаторен феномен*. (Dolla, 2022, 172) (Leite, 2022, 139) Този трансформационен етап изисква *фундаментална адаптация* както на институционално ниво, чрез преосмисляне на нормативните рамки и управленските парадигми, така и на нивото на индивидуалните граждани, което предполага промяна в нагласите и поведенческите модели. *Отсъствието на ясно дефинирани правни рамки*, колебанията в общественото доверие към новите технологии, както и евентуалните затруднения при безпроблемното интегриране на иновациите в ежедневието на хората, могат потенциално да забавят, деформират или дори напълно компрометират заявената ефективност и ползотворност на внедряваните технологични решения.

Социалното възприемане на новите технологии има определящо значение за успеха на смарт инициативите. (Radziejowska, 2021, 14 (14), 4330) Ако гражданите не са убедени в *ползите, сигурността и достъпността* на тези технологии, тяхното приемане може да бъде затруднено, поради:

1. *Недостатъчна дигитална грамотност* – липсата на технически умения сред значителна част от населението може да създаде *технологично разделение*, което води до неравен достъп до иновации;
2. *Скептицизъм и съпротива срещу технологичните промени* – обществото може да прояви *недоверие* към автоматизацията, ИИ и събирането на лични данни, особено ако липсва прозрачност в начина, по който тези технологии функционират;
3. *Промени в трудовата заетост* – автоматизацията може да доведе до *изместване на работни места*, което предизвиква социално напрежение, особено в сектори с традиционно висока заетост. (Лучков К. , Изследване на добри практики на корпоративна социална отговорност, 2023)

Регулаторната среда също представлява *критичен фактор* за успешното прилагане на смарт технологии. Недостатъчните или прекалено рестриктивни законови

рамки могат да ограничат иновациите и да създадат *несигурност за инвеститорите и бизнеса*.

Таблица 3

Регулаторни предизвикателства и стратегии за преодоляване при имплементацията на смарт технологии в градската среда (*Източник: собствена интерпретация*)

Регулаторен проблем	Описание	Възможни последици	Стратегии за преодоляване
<i>Липса на специфично законодателство</i>	В много държави все още липсват регулаторни рамки за управлението на IoT, ИИ и автоматизацията.	Забавяне на внедряването на технологии, несигурност за бизнеса.	Разработване на специализирани политики и нормативни актове.
<i>Непоследователност в политиките</i>	Различия между националните и международните регулации могат да доведат до правна несигурност.	Невъзможност за създаване на трансгранични проекти и привличане на чуждестранни инвестиции.	Хармонизиране на законодателството с глобалните стандарти.
<i>Защита на личните данни (GDPR, CCPA и др.)</i>	Интелигентните технологии събират и анализират големи количества данни, което повдига въпроси за неприкосновеността на личния живот.	Потенциални правни конфликти, санкции и загуба на обществено доверие.	Въвеждане на механизми за прозрачност и отчетност при съхранение на данни.
<i>Етично регулиране на ИИ и автоматизацията</i>	Необходимост от ясни етични насоки за използването на алгоритми и машинно обучение.	Риск от дискриминация, пристрастност и социални неравенства.	Разработване на етични кодекси за използване на ИИ.

За да могат смарт технологиите да бъдат успешно интегрирани в тъканта на обществото и да реализират своя пълноценен потенциал за градско развитие, е абсолютно необходимо предприемането на *целенасочени и проактивни мерки*. Тези интервенции следва да гарантират не само плавна адаптация на населението и институциите, но и да осигурят висока степен на обществено приемане, което е фундаментът за дългосрочна устойчивост и ефективност на иновациите.

1. *Систематичното повишаване на дигиталната грамотност* сред всички слоеве на обществото. Изисква се създаване на цялостна образователна екосистема, която включва както широкообхватни публични кампании за повишаване на осведомеността

относно ползите и сигурността на смарт технологиите, така и разработване на специализирани, диференцирани обучителни програми. Програмите трябва да са адаптирани към нуждите на различни социални групи, за да намалят дигиталното разделение и да осигурят равнопоставен достъп до предимствата на дигиталната трансформация.

2.Изграждането на *архитектура на прозрачност и консолидация на общественото доверие*. Има се предвид въвеждане на стриктни етични насоки и всеобхватни регулации за защита на личните данни, фокусирани върху принципите "поверителност по дизайн" и отчетност. Успоредно с това е критично създаването на отворени, интерактивни платформи за гражданско участие, където обществото да може активно да участва в процесите на планиране, внедряване и оценка на смарт технологиите, превръщайки се от пасивен консуматор в активен съавтор на дигиталната трансформация.

3.Прилагането на *адаптивни регулаторни подходи*. Означава разработване на гъвкави законови рамки и регулаторни "пясъчници", които позволяват контролирано експериментирание с нови технологии в реални условия, преди да бъдат въведени всеобхватни регулации. Ефективната регулация изисква също и тясно сътрудничество между държавни органи, частния сектор, академичните среди и гражданското общество за създаване на балансирана, адекватна и устойчива нормативна среда.

4.Прилагането на *комплексни модели за социално-икономическа адаптация*. Това включва мащабни инвестиции в програми за преквалификация и повишаване на квалификацията на работната сила, целящи да минимизират негативните ефекти от автоматизацията. Същевременно, трябва да се разработят и механизми за социална защита и финансова подкрепа за уязвимите групи, които могат да бъдат най-тежко засегнати от технологичните промени, осигурявайки им сигурност и възможност за преход.

Социалните и регулаторните предизвикателства представляват *съществена бариера* пред внедряването на смарт технологии, но *систематичните усилия за законова адаптация, обществени кампании и етично регулиране* могат значително да улеснят този преход. Чрез насърчаване на *прозрачност, доверие и инклузивност* технологичната трансформация може да бъде възприета не като заплаха, а като възможност за устойчиво развитие и икономически растеж.

Заклучение

Внедряването на смарт технологии в градската среда представлява сложен, многоаспектен процес, чийто успех не се свежда само до технологичното съвършенство. Както показва настоящият анализ, той е дълбоко преплетен с преодоляването на съществени предизвикателства в областта на киберсигурността, финансовата устойчивост, социалната адаптация и регулаторната рамка.

От критична важност е осъзнаването, че *киберсигурността вече не е периферна функция, а централен системен компонент*, който следва да бъде вграден по дизайн във всяка смарт градска архитектура, трансформирайки я от потенциална Ахилесова пета в резистентна имунна система. Финансовата жизнеспособност на тези мащабни инвестиции, от своя страна, зависи от *иновативни модели на финансиране и прецизно управление на риска*, които надхвърлят традиционните бюджети и привличат диверсифицирани капиталови потоци, включително чрез ПЧП и зелени облигации. Не по-малко значимо е разбирането, че *социалното приемане и доверие са фундаментален капитал*, който може да бъде изграден само чрез прозрачност, активно гражданско участие и целенасочени образователни програми, преодоляващи дигиталното разделение. И накрая, *адаптивната и проактивна регулаторна среда* е ключова за балансирането между стимулирането на иновациите и гарантирането на етичното използване на данните и ИИ, предотвратявайки рискове като дискриминация и компрометиране на личната неприкосновеност.

Ето защо, пътят към интелигентния и устойчив град е детерминиран от холистичен подход, който интегрира технологичните постижения с проникателно разбиране на икономическите, социалните и правните импликации. Само чрез тази синергия можем да изградим градове, които са не просто технологично напреднали, но и сигурни, справедливи и устойчиви за бъдещите поколения.

Bibliography

- Веселинова, Н. (2025, 23). Насърчаване на отворени иновации в публичния сектор чрез инкубатори и акселератори. *e-Journal VFU*, 194-208.
- Веселинова, Н. (25-26 октомври 2024). Интегриране на ESG критерии в бизнес планирането. *Международен научен форум "Световни и национални бизнес трансформации - проактивни, управленски, финансово-счетоводни и планови решения* (pp. 251-257). Свищов: АИ "Ценов".
- Лучков, К. (2023). ESG - целево-ориентиран подход към устойчивото развитие. *Юбилейна международна научнопрактическа конференция "Предизвикателствата пред финансите и стопанската отчетност в условията на множествени кризи"* (pp. 411-414). Свищов: АИ "Ценов".
- Лучков, К. (2023). Изследване на добри практики на корпоративна социална отговорност. *Юбилейна международна научнопрактическа конференция „Предизвикателства пред финансите и стопанската отчетност в условията на множествени кризи“* (pp. 399-404). Свищов: АИ "Ценов".
- Лучков, К. (2024). Значение на технологичните иновации и дигитализацията за устойчивото развитие. *Международен научен форум „Световни и национални бизнес трансформации - проактивни управленски, финансово – счетоводни и планови решения* (pp. 47-51). Свищов: АИ "Ценов".
- Лучков, К. С. (2024). Зелените облигации - ключов инструмент за финансиране на устойчиво развитие. *Сборник с доклади на ТУ, 74 (4)*. София: ТУ- София.
- Чиприянова, Г. Ч. (2014, 3). Счетоводни аспекти на придобиването на дълготрайни материални активи, предназначени за опазване на околната среда по линия на европейските фондове. *Диалог*, 12-30.
- Ahsan, M. N. (2022, 2 (3)). Cybersecurity Threats and Their Mitigation Approaches Using Machine Learning - A Review. *CybersecJournal of Cybersecurity and Privacy*, 527-555.
- Chipriyanova G., M. M. (2023). Opportunities and challenges in Modeling an Environmental Management System. *Environment, Technology, Resources*, (pp. 38-43).
- Chipriyanova, G. C. (2022, 2). Business Intelligence Competence and Enterprise Resource Planning (ERP) System Tools. *Business Management*, 5-20.
- Dolla, T. B. (2022, 172). Smart Cities in the Development of Sustainable Infrastructure—Systematic Literature Review of Two Decades Research. *Lecture Notes in Civil Engineering*, 55-64.
- Leite, E. (2022, 139). Innovation networks for social impact: An empirical study on multi-actor collaboration in projects for smart cities. *Journal of Business Research*, 325-327.
- Mehrotra, A. (24-26 April 2019). Financial inclusion through fintech—A case of lost focus. In Proceedings of the 2019 International Conference on Automation, Computational and Technology Management (ICACTM). *International Conference on Automation, Computational and Technology Management (ICACTM)* (pp. 103-107). London, UK: IEEE.

- Mubanani, E. F. (2023, 2.1). Application of the New Growth Theory to Financial Risk Management. *East African Finance Journal*, 32-39.
- Oladipo, J. O. (2024, 11 (1)). Human factors in cybersecurity: Navigating the FinTech landscape. *Human fInternational Journal of Science and Research Archive*, 1959–1967.
- Radu, S. (9-10 June 2016). Comparative analysis of security operations centre architectures; proposals and architectural considerations for frameworks and operating models. Radu, S. G. (2016). *Comparative analysis of security operations centre architectures; proposals and architectural consideratInnovative Security Solutions for Information Technology and Communications: 9th International Conference SECITC* (pp. 248-260). Bucharest, Romania: Springer International Publishing.
- Radziejowska, A. S. (2021, 14 (14), 4330). Analysis of the social aspect of smart cities development for the example of smart sustainable buildings. *Energies*, <https://doi.org/10.3390/en14144330>.
- Wang, P. A. (August 2015). Data security and threat modeling for smart city infrastructure. *International Conference on in Cyber Security of Smart Cities, Industrial Control System and Communications* (pp. 1-6). DOI:10.1109/SSIC.2015.7245322.