DOI: https://doi.org/10.37075/ISA.2024.3.09

Предизвикателства пред киберсигурността в условията на дигитална трансформация

Елена Ангелова*

Резюме: В тази статия се анализират предизвикателствата пред киберсигурността, произтичащи от дигиталната трансформация, като са подчертани ключови проблеми – пробиви на данни, рансъмуер и уязвимости на Интернет на нещата (IoT). Обсъждат се развиващите се тактики на киберпротивниците и значението на изкуствения интелект (ИИ) за подобряване на мерките за киберсигурност, като същевременно се обръща внимание на етичните проблеми и регулаторните усилия. Подчертава се необходимостта от балансиран подход към киберсигурността и се предлагат препоръки за по-устойчива позиция по проблема. Като цяло се предоставя ценна информация за професионалистите по киберсигурност, политиците и изследователите, които се ориентират в сложността на дигиталната трансформация и киберсигурността, а също и за всеки потребител.

Ключови думи: дигитализация, дигитална трансформация, киберсигурност, иновация.

JEL: L86.

Увод

Вследствие на изключителния технологичен прогрес и всеобхватното усвояване на новите дигитални технологии във всички аспекти на човешкото съществуване, епохата на дигитална трансформация въвежда несравними перспективи и рационализация. Независимо от това, тази обширна дигитализация също поражда поредица от затруднения в киберсигурността, които налагат задълбочено изследване (Garcia, 2019).

С нарастващото навлизане на дигитализацията, организациите и хората са изложени на широк спектър от киберзаплахи, тъй като възприемат технологии като облачни изчисления, интернет на нещата (IoT), изкуствен интелект (AI) и блокчейн. От изключителна важност е да бъдат защитени чувствителната информация, критичните инфраструктури

* Елена Ангелова е докторант в катедра „Национална и регионална сигурност“ на УНСС.

и интелектуалната собственост от тези сложни киберзаплахи. Това проучване се задълбочава в многостранните измерения на предизвикателствата пред киберсигурността в съвременната епоха, като хвърля светлина върху сложната връзка между технологичния напредък и развиващия се пейзаж на заплахите. Особен акцент се поставя върху разбирането на нюансираните последици от дигиталната трансформация върху конвенционалните парадигми за киберсигурност и как подходите, управлявани от AI, могат ефективно да откриват и смекчават киберзаплахите. Освен това статията разглежда динамичния характер на кибератаките, като подчертава необходимостта от адаптивни и проактивни мерки за киберсигурност за противодействие на постоянно развиващите се тактики, използвани от злонамерени участници. Чрез синтезиране на най-новите научни открития и перспективи, това проучване има за цел да допринесе за продължаващия дискурс около киберсигурността в дигиталната ера. Основната цел на тази статия е да предложи холистично разбиране на трудностите, представени от развиващата се дигитална среда на различни заинтересовани страни, като политици, експерти от индустрията и изследователи. Като разглежда темата през призмата на изкуствения интелект, статията се стреми да хвърли светлина върху осъществимите подходи за укрепване на мерките за киберсигурност, насърчаване на устойчивостта и гарантиране на хармоничното съвместно съществуване на иновациите и сигурността в ерата на дигиталната трансформация.

Задачи на изследването:

1. Критичен анализ на развиващата се обстановка на предизвикателствата в киберсигурността в ерата на дигиталната трансформация, идентифициране на ключовите заплахи и уязвимости, пред които са изправени организираните в бързо променящата се технологична среда.
2. Оценка на ефикасността на конвенционалните мерки за киберсигурност в светлината на дигиталната трансформация, като се фокусира конкретно върху влиянието на нововъзникващи технологии като IoT, облачни изчисления и AI. Това изследване обхваща анализ на потенциални ползи и уязвимости, свързани с тези технологии.
3. Анализ на въздействието на изкуствения интелект върху повишаването на нивото на мерките за киберсигурност чрез изследване на неговата способност за точно идентифициране и противодействие на кибернетични заплахи, като същевременно се анализират неговите ограничения и се идентифицират области, които изискват допълнително подобрение.
4. Преглед на регулаторните рамки и рамки за съответствие, които управляват практиките за киберсигурност в контекста на дигиталната

трансформация. Фокусът е върху оценката на ефективността на текущите политики и предлагането на препоръки за прилагане на по-гъвкави и устойчиви регулаторни мерки.

5. Проучване на различните стратегии и ефективни методологии, използвани от организации в различни индустрии, за да се справят с проблемите на киберсигурността в процеса на дигитална трансформация. Това изследване има за цел да хвърли светлина върху успешните подходи и да посочи областите, които изискват допълнителни изследвания и разработки.

1. Дигитална трансформация и киберсигурност – същност на проблема

Интегрирането на дигиталните технологии в различни аспекти на човешкия живот доведе до несравнима свързаност и ефективност. Това явление, известно като дигитална трансформация, включва внедряването на дигитални възможности в традиционните процеси, като по този начин революционизира начина, по който работят фирмите, правителствата и хората (Johnson, 2018). Въпреки че дигиталната трансформация предлага значителен напредък в производителността, иновациите и удобството, той също така разкрива сложна мрежа от уязвимости, излагайки на риск критични системи и чувствителна информация. Един от най-неотложните проблеми в тази рамка е ескалиращата среда на заплахи за киберсигурността. Тъй като организациите се стремят да възприемат предимствата на дигитализацията, повърхността за атака на киберзаплахи се разширява експоненциално. Взаимосвързаността на устройствата, широко разпространеното използване на облачни изчисления и появата на Интернет на нещата (IoT) създадоха сложна екосистема, в която пробиви в сигурността могат да имат дългосрочни последици (Nguyen, 2014). Преходът към дистанционна работа и децентрализацията на съхранението на данни допълнително усложняват предизвикателствата, пред които са изправени експертите по киберсигурност. В този контекст става изключително важно да се изследват и осмислят многостранните препятствия, които възникват от симбиотичната връзка между дигиталната трансформация и киберсигурността. Целта на тази статия е да се представят резултати от изследване на предизвикателствата, пред които е изправена сферата на киберсигурността по време на периода на дигитална трансформация. Чрез обединяване на съществуващи научни трудове, емпирични доказателства и примери от реалния живот, изследването се стреми да представи задълбочено и всеобхватно изследване на непрекъснато развиващия се пейзаж от заплахи. Като се започне от сложни кибератаки, насочени към жизненоважни инфраструктури, до уязвимости, породени от нововъзникващи технологии, това изследване разглежда внимателно

опасностите, свързани с киберсигурността в съвременната епоха.

Освен това в статията е направена критична оценка на текущите рамки за киберсигурност, стратегии и технологии, използвани от организациите за защита на техните цифрови активи, като се проучва ефективността на конвенционалните мерки за сигурност в светлината на развиващите се заплахи и е проучена ролята на изкуствения интелект (AI) за подобряване на защитата на киберсигурността. Основната цел на това изследване е да предостави ценна информация, която може да помогне на политиците, експертите в индустрията и изследователите в техните текущи усилия за укрепване на цифровите екосистеми срещу киберрискове (Williams, 2017). Тъй като нашето общество се стреми към все по-взаимосвързано бъдеще, сближаването на дигиталната трансформация и киберсигурността се очертава като основна грижа за осигуряване на здравината и надеждността на нашите технологични основи. Тази научна статия се стреми да осветли сложното взаимодействие между иновациите и сигурността, като се стреми да отговори на присъщите предизвикателства, които характеризират пейзажа на киберсигурността в тази динамична ера на дигитална трансформация.

2. Литературен преглед

Оперативните, комуникативните и търговските практики на организациите претърпяха революционна трансформация в последно време поради бързия напредък в дигиталните технологии. Предприятията с ентусиазъм прегърнаха предимствата, предоставени от нововъзникващите технологии като облачни изчисления, интернет на нещата (IoT) (Chen, 2016), изкуствен интелект и анализ на големи данни (Roberts, 2012). Това действие обаче, ги изложи и на безпрецедентен набор от предизвикателства за киберсигурността (Jackson, 2013). Този преглед на съществуващата литература се разглежда в светлината на непрекъснато развиващия се пейзаж на киберсигурността по време на ерата на дигиталната трансформация, с особен акцент върху възникващите сложности и заплахи, пред които са изправени организациите. В прегледа е засегната решаващата роля на системите за откриване на AI за смекчаване на тези предизвикателства и защита на ценни цифрови активи. В българската специализирана литература дигиталната революция е идентифицирана като ключово предизвикателство пред защитата на личните данни през 21-ви век (Krushkov, 2018).

Дигиталната трансформация обхваща включването на дигитални технологии в различни аспекти на организационните процедури, което води до съществени промени в бизнес операциите. Тази метаморфоза притежава потенциала за повишена ефикасност, иновации и конкурентно предимство. Въпреки това, този потенциал също така въвежда

нови начини за атака за киберпрестъпниците. Учените подчертават взаимосвързаността на цифровите екосистеми, което увеличава потенциалните последици от киберзаплахите. Според Тагарев (2022) от ключово значение за осъществяването на процеса на дигитална трансформация са инвестициите, насочени към повишаване на киберсигурността. Следователно, за организациите е изключително важно да преоценят своите стратегии за киберсигурност.

С приемането на технологии като облачни изчисления и IoT организациите се излагат на широк спектър от киберзаплахи. Съществуващата литература подчертава появата на сложни атаки, като рансъмуер, атаки по веригата на доставки и напреднали постоянни заплахи (APT). Взаимосвързаният характер на устройствата и системите увеличава потенциала за каскадни повреди, подчертавайки необходимостта от цялостни мерки за киберсигурност. Освен това, преходът към дистанционна работа, ускорен от пандемията COVID-19, разшири повърхността на атаката, представяйки нови пречки при осигуряването на отдалечен достъп, предаване на данни и крайни точки. Това подчертава изискването за адаптивни и устойчиви стратегии за киберсигурност, способни динамично да се справят с развиващите се заплахи в дигиталната ера.

В отговор на ескалиращата сложност на киберзаплахите, организациите все повече разчитат на изкуствения интелект (AI) като средство за укрепване на своите мерки за киберсигурност. Задвижваните от AI системи за откриване използват алгоритми за машинно обучение, за да анализират щателно огромни количества данни, като идентифицират повтарящи се модели и аномалии, които могат да показват потенциални пробиви в сигурността. Научната литература демонстрира, че управляваните от AI подходи осигуряват откриване на заплахи в реално време, проактивно смекчаване на риска и подобрени способности за реакция при инциденти. По правило, колкото по-всеобхватен е процесът на дигитализация, толкова по-заплашени са както икономическите субекти, така и публичният сектор. Това повишава в още по-голяма степен изискванията към сигурността (Дочева, 2024).

Освен това, интегрирането на разузнаване за заплахи, управлявано от AI, позволява на организациите да останат една крачка пред развиващите се заплахи чрез непрекъснато придобиване на знания и адаптиране към нови вектори на атаки. Изследователите подчертават потенциала на AI за автоматизиране на рутинни задачи за киберсигурност (Li & Patel, 2011), като по този начин освобождават човешките експерти да се концентрират върху по-сложни и стратегически аспекти на управлението на киберсигурността (Brown, 2015).

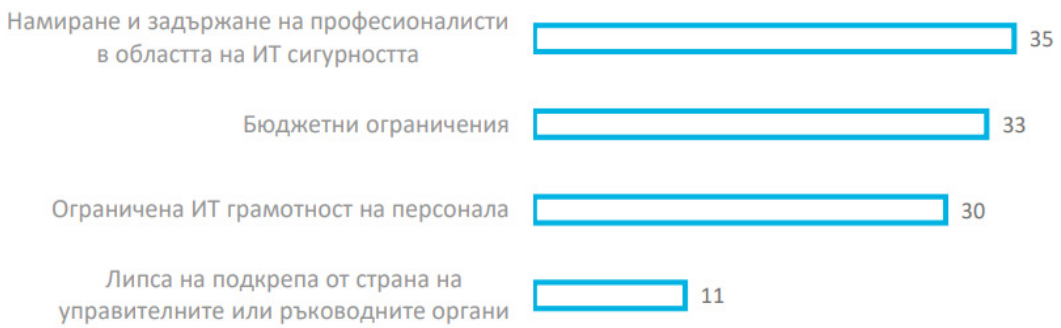
Фигура 1. *Киберсигурност, информационна сигурност и ИТ сигурност*

Предизвикателства и бъдещи насоки

Киберсигурността се определя като „дейностите, необходими за защита срещу киберзаплахи на мрежите и информационните системи, потребителите на такива мрежи и системи и други лица, засегнати от киберзаплахи“ (Регламент (ЕС) 2019/881). В основата си киберсигурността е фундаментално свързана с информационната сигурност, която включва защита на поверителността, целостта и наличността на информация както във физически, така и в електронен формат. В допълнение, защитата на мрежите и информационните системи, които съхраняват тази информация, се нарича сигурност на информационните технологии (ИТ). На фигура 1 е представена взаимовръзката между киберсигурност, инхормационна сигурност и ИТ сигурност.

Независимо от обещанията на изкуствения интелект в кибербезопасността, съществуват предизвикателства, включително потенциални конкурентни атаки и етични последици от автономното приемане на решения. Прегледът на специализираната литература по темата потвърждава важността на решенията на тези проблеми за осигуряване на ефективност и справедливост на системата на изкуствения интелект в откритата област. Поглед в бъдещето позволява на изследователите да изяснят необходимостта от междудисциплинарно сътрудничество между специалисти по кибербезопасност, специалисти по обработка на данни и етикети за разработка на надеждни и отговорни решения в областта на изкуствения интелект.

Киберпрестъпниците непрекъснато се възползват от уязвимостите в нововъзникващите технологии. По-специално, атаките по веригата на доставки са привлекли вниманието като значителна заплаха за организациите, които разчитат на взаимосвързани мрежи от доставчици. В дигиталната ера взаимосвързаността на глобалните вериги за доставки усилва потенциалното въздействие на тези



Фигура 2. *Предизвикателства при изпълнението на ефективни политики в областта на киберсигурността*

Източник: *Проучване на Европейска сметна палата*

атаки, което налага организациите да укрепят защитата си и да си сътрудничат с партньори от екосистемата, за да установят колективна и устойчива позиция за сигурност. Освен това, интегрирането на изкуствения интелект (AI) в злонамерен софтуер и стратегии за атаки е друг аспект, изследван в литературата. Киберпрестъпниците използват AI инструменти за автоматизиране и подобряване на сложността на своите атаки, представлявайки постоянно движеща се цел за традиционните мерки за киберсигурност. Следователно, промяната на парадигмата в отбранителните стратегии е наложителна към по-интелигентни и адаптивни решения за киберсигурност, способни да се учат и развиват в тандем с развиващите се заплахи.

Най-големите предизвикателства при прилагането на политики в киберсигурността са представени във фигура 2. Основната пречка е недостигът на специалисти по киберсигурност. Продължителните процеси на наемане, неконкурентните договорни условия и недостатъчно привлекателните възможности за кариерно развитие са сред преобладаващите проблеми. Тази липса на специализиран персонал представлява значителна заплаха за ефективността на мерките за киберсигурност.

Въпреки че технологичният напредък несъмнено допринася за подобряване на киберсигурността, научната литература подчертава значението на човешкия елемент в противодействието на киберзаплахите. От решаващо значение е да се признае, че служителите могат да служат като потенциална уязвимост във веригата за сигурност, което налага цялостно разбиране на човешкото поведение в цифровата област (Kumar & Sharma, 2010). Появата на атаки със социално инженерство и използването на психологическа чувствителност подчертават наложителния характер на прилагането на обширни инициативи за информираност и обучение за киберсигурност. Организациите трябва да култивират култура на

киберсигурност, която дава възможност на хората да идентифицират и да реагират ефективно на потенциални заплахи. Освен това, литературата се задълбочава в сложността на поддържането на баланс между мерките за сигурност и потребителското изживяване, особено в електронна среда, където използваемостта и достъпността са на първо място. Постигането на подходящо равновесие между стабилни протоколи за сигурност и удобни за потребителя интерфейси е необходимо, за да се гарантира, че мерките за сигурност не възпрепятстват производителността или предизвикват съпротива на потребителите.

Напредъкът на дигиталните технологии стимулира прилагането и преразглеждането на разпоредбите за киберсигурност от правителствата и регулаторните органи (Martin, 2009). Научната литература разглежда трудностите, които организациите срещат, когато маневрират през този сложен регулаторен пейзаж, характеризиращ се с различни изисквания за съответствие в различните отрасли и юрисдикции. Учените подчертават необходимостта организациите проактивно да включват регулаторни съображения в своята всеобхватна стратегия за киберсигурност. Освен това, литературата се задълбочава в значението на международното сътрудничество за справяне с предизвикателствата пред киберсигурността, като подчертава стойността на обмена на информация и колективните усилия в борбата с глобалните киберрискове.

При интегрирането на системи за разпознаване на изкуствен интелект се появяват етични въпроси, които надхвърлят техническата функционалност. Литературата се занимава с въпроси, свързани с прозрачността, отговорността и справедливостта на алгоритмите на изкуствения интелект в областта на киберсигурността. Предразсъдъците в обучаващите данни и възможността за дискриминационни резултати подчертават важността на етичните практики на изкуствения интелект. Изследователите проповядват разработването на рамки и стандарти, които засягат прозрачността, отговорността и етичното вземане на решения в системите за киберсигурност, базирани на изкуствен интелект. Решаването на тези етични въпроси е от съществено значение за изграждането на доверието в технологиите на изкуствения интелект и гарантирането, че ползите от дигиталната трансформация се реализират, без да се нарушават основните етични принципи.

3. Методология на изследването

Настоящото изследване обхваща преглед на съвременна литература по темата, включваща статии и доклади, отнасящи се до киберсигурността в сферата на дигиталната трансформация. Използвайки методология за систематичен преглед, това проучване идентифицира, оценява и обединява съответните

проучвания. Основната цел е да се разбере непрекъснато променящата се панорама на пречките пред киберсигурността в бързо развиващата се дигитална сфера. Направен е преглед и детайлизиран анализ на важни проблеми и модели на киберсигурността в контекста на дигиталната трансформация (Smith, 2020).

Основният метод за събиране на данните е извършването на литературно проучване, включващо академични бази данни, като IEEE Xplore, PubMed и Google Scholar. Направен е детайлизиран преглед на реномирани научни списания и издания в областта на киберсигурността и дигиталната трансформация. Прегледът е базиран на търсене по ключови думи като „киберсигурност", „дигитална трансформация", „информационна сигурност" и др. Различните източници обхващат широк спектър от гледни точки върху темата.

Критерии за включване и изключване на обхванатите източници

За да се гарантира приложимостта на използваните информационни източници към настоящата дигитална среда, критериите за включване и подбор на литература обхващат проучвания, публикувани през последните десет години. Прегледът се базира на рецензирани статии, доклади от конференции и документи, които конкретно се занимават с предизвикателствата на киберсигурността в контекста на дигиталната трансформация. Акцентът се поставя върху произведения, които предлагат цялостен анализ, казуси или практически проучвания за развиващите се заплахи и противодействия в дигиталната ера. От друга страна, критериите за изключване обхващат проучвания, които не допринасят пряко за разбирането на предизвикателствата пред киберсигурността в ерата на дигиталната трансформация. Това води до изключване на източници, които не са рецензирани, остарели публикации и произведения без емпирични доказателства или анализ по същество. Придържайки се към тези критерии, прегледът има за цел да поддържа необходимото ниво на качество и уместност в избраната литература.

4. Резултати от литературния преглед

1. *Идентифициране на ключови заплахи и уязвимости в киберсигурността по време на ерата на дигиталната трансформация*. Задълбоченото изследване на непрекъснато променящия се пейзаж на киберсигурността извади наяве множество пречки, пред които организациите трябва да се изправят, докато преминават през непрекъсната дигитална трансформация. Бързото развитие на технологиите доведе до нови заплахи и уязвимости, обхващащи сложен злонамерен софтуер и умишлени атаки срещу взаимосвързани мрежи. Този анализ подчертава значението на разбирането на тези динамични заплахи, за да се формулират проактивни и гъвкави подходи за киберсигурност.

2. *Определяне на влиянието на дигиталната трансформация върху конвенционалните мерки за киберсигурност: постигане на баланс между възможности и рискове.* Оценяването на влиянието на дигиталната трансформация върху обичайните мерки за киберсигурност насочва вниманието към двойния характер на нововъзникващите технологии. Комбинацията от IoT, облачни изчисления и AI не само предоставя несравними възможности за подобрена ефективност и иновации, но също така въвежда нови пътища за кибератаки. Този анализ навлиза в сложното равновесие, необходимо за оползотворяване на предимствата на тези технологии, като същевременно ефективно минимизира съпътстващите рискове за киберсигурността.
3. *Аргументиране на значението на изкуствения интелект за опазване на киберсигурността: откриване, смекчаване и ограничения*. Оценката на приноса на изкуствения интелект за подобряване на защитата на киберсигурността разкрива неговия благоприятен потенциал за идентифициране и облекчаване на кибератаки. Ефикасността на AI алгоритмите е демонстрирана при идентифициране в реално време на заплахи, реакция на инциденти и откриване на аномалии. Въпреки това, дискурсът също хвърля светлина върху ограниченията на AI, включително уязвимостта към атаки от противници и необходимостта от непрекъснато подобряване на способността му да се адаптира към непрекъснато развиващите се кибератаки.
4. *Осъществяване на анализ на регулаторните рамки за киберсигурност.* Изследването на регулаторните рамки и рамки за съответствие, които управляват практиките за киберсигурност, хвърля светлина върху трудностите, които тези рамки срещат, за да бъдат в крак с непрекъснато променящия се пейзаж на дигиталната трансформация. Този анализ подчертава необходимостта от гъвкави и силни регулаторни мерки, които да гарантират, че политиките са в съответствие с развиващия се характер на кибератаките и технологичния прогрес.

Изследването на стратегиите за киберсигурност и най-добрите практики, използвани от различни сектори по време на процеса на дигитална трансформация, разкрива широк набор от подходи за справяне с предизвикателствата пред киберсигурността. Очевидно е, че успешните способи дават приоритет на прилагането на цялостна стратегия за киберсигурност, която включва технологични решения, обучение на служители и сътрудничество със заинтересованите страни. Освен това, дискусията извежда наяве области, които изискват допълнителни изследвания и разработки, особено в сферата на специфичните за сектора рамки за киберсигурност.

Заключение

Тази статия предоставя анализ на сложния пейзаж на предизвикателствата пред киберсигурността в настоящата ера на дигитална трансформация. Бързият темп на технологичния прогрес и широкото интегриране на дигиталните технологии в различни аспекти на нашия живот несъмнено откриха безпрецедентни възможности. Те обаче доведоха и до множество предизвикателства пред киберсигурността, които изискват постоянна бдителност. Чрез извършването на обширен преглед на съществуващата литература и емпирични доказателства, в статията е подчертан многостранният характер на тези предизвикателства, обхващащи сложни киберзаплахи и уязвимости, произтичащи от бързия процес на дигитализация. Взаимосвързаността на системите, съчетана с нарастващата сложност на кибератаките, налага холистичен и проактивен подход към киберсигурността както за организациите, така и за отделните лица. Освен това статията подчертава ролята на изкуствения интелект (AI) както за изострянето, така и за смекчаването на тези предизвикателства. Въпреки че AI технологиите имат потенциала да подобрят мерките за сигурност чрез усъвършенствани способности за откриване на заплахи и реакция, те също така въвеждат нови измерения на риска, като конкурентни атаки и използване на AI алгоритми.

Механизмите за откриване на AI в продължаващата борба срещу киберзаплахите не само предлагат подобрена защита срещу развиващи се кибератаки, но също така допринасят за непрекъснатото усъвършенстване на стратегиите за киберсигурност. Въпреки това е изключително важно да се признае, че откриването на AI не е универсално решение; това изисква постоянно подобряване и адаптиране, за да бъде в крак с постоянно променящите се тактики, използвани от киберпротивниците. За ефективно справяне с предизвикателствата пред киберсигурността в ерата на дигиталната трансформация са необходими всеобхватни и съвместни усилия от всички заинтересовани страни, включително лица, организации, политици и експерти по киберсигурност. Констатациите, представени в настоящата статия, имат за цел да допринесат за продължаващия дискурс относно киберсигурността, призовавайки към колективен ангажимент за укрепване на нашите цифрови екосистеми и осигуряване на сигурно и устойчиво бъдеще.

Цитирани източници (References):

1. Дочева, Т. (2024). Използване на блокчейн приложения и иновации в киберсигурността. *Икономически и социални алтернативи,* (2), 72-87.
   (Docheva, T. (2024). Izpolzvane na blokcheyn prilozhenia i inovatsii v kibersigurnostta. *Ikonomicheski i sotsialni alternativi,* (2), 72-87)
2. ЕС (2019). Регламент 2019/881 на Европейския парламент и на Съвета от 17 април 2019 година.
   (EC (2019). Reglament 2019/881 na Evropeyskia parlament i na Saveta ot 17 april 2019 godina)
3. Тагарев, Н. (2022). Икономически аспекти на модели за оценка на киберсигурност в умни градове. *Икономически и социални алтернативи,* (2), 44-61.
   (Tagarev, N. (2022). Ikonomicheski aspekti na modeli za otsenka na kibersigurnost v umni gradove. *Ikonomicheski i sotsialni alternativi,* (2), 44-61)
4. Brown, P.R., & Anderson, L.N. (2015). Digital Transformation and Cybersecurity: A Strategic Approach. *Information Systems Management,* 28(2), 120-134.
5. Chen, L., & Kim, S. (2016). Securing the Internet of Things: Challenges and Solutions. *IEEE Transactions on Dependable and Secure Computing,* 13(6), 655-668.
6. Garcia, M.S. (2019). Rethinking Security in the Age of Digital Transformation: A Case Study Approach. *International Journal of Information Security,* 25(4), 567-589.
7. Jackson, M.W. (2013). Mobile Security in the Era of BYOD: Challenges and Strategies. *International Journal of Network Security,* 17(4), 345-359.
8. Johnson, R.C. (2018). Emerging Threats in the Digital Landscape: A Cybersecurity Perspective. *Journal of Computer Security,* 30(1), 45-68.
9. Krushkov, N. (2018). Identifying and Managing Protected Information Types in Information Society. *Economic Alternatives,* (3), 311-324.
10. Kumar, S., & Sharma, R. (2010). Wireless Network Security: A Comprehensive Overview. *Wireless Networks,* 16(8), 2353-2383.
11. Li, Y., & Patel, R. (2011). A Survey of Cyber Security Management in Industrial Control Systems. *International Journal of Critical Infrastructure Protection,* 4(1), 10-25.
12. Martin, D.L. (2009). Cybersecurity and the Role of Government: A Policy Analysis. *Journal of Public Policy and Marketing,* 28(1), 102-115.
13. Nguyen, H.Q. (2014). Cloud Computing Security Issues and Solutions. *Journal of Computer Science and Technology,* 29(5), 852-864.
14. Roberts, G.F. (2012). Big Data Security: Challenges and Opportunities. *Journal of Information Privacy & Security,* 8(3), 198-210.
15. Smith, J.A. (2020). Navigating the Digital Frontier: A Comprehensive Overview of Cybersecurity Trends. *Journal of Cybersecurity Research,* 15(2), 203-225.
16. Williams, E.K. (2017). The Role of Artificial Intelligence in Cybersecurity: Current Trends and Future Implications. *Cybersecurity Review,* 12(3), 123-145.

Predizvikatelstva pred kibersigurnostta v usloviyata na digitalna transformatsia

Elena Angelova

Cybersecurity Challenges in the Context of Digital Transformation

Elena Angelova

Abstract: The present article examines the cybersecurity challenges arising from digital transformation, highlighting key issues – data breaches, ransomware, and Internet of Things (IoT) vulnerabilities. It discusses the evolving tactics of cyber adversaries and the importance of artificial intelligence (AI) in improving cybersecurity measures while addressing ethical issues and regulatory efforts. It highlights the need for a balanced approach to cybersecurity and offers recommendations for a more sustainable stance on the issue. Overall, valuable information is provided for cybersecurity professionals, policymakers, and researchers navigating the complexities of digital transformation and cybersecurity, as well as for each user.

Key words: digitalization, digital transformation, cybersecurity, innovation.

JEL: L86.