МЕТОД ЗА ОЦЕНКА НА КИБЕРРИСКА В ТЕЛЕМЕДИЦИНАТА

ас. д-р. инж. **Петя Иванова Петрова**

Висше училище по телекомуникации и пощи, София

Резюме: *Развитието на телемедицината разширява използването на информационни и комуникационни технологии при дистанционни консултации, наблюдение на пациенти и обмен на медицински данни. Технологичната среда обединява крайни устройства, комуникационни мрежи, приложни платформи, облачни и сървърни ресурси, системи за управление на идентичности и достъп и свързани медицински устройства. Взаимодействието между тези компоненти формира специфичен киберрисков профил, при който локална техническа слабост може да повлияе върху сигурността на информацията и достъпността на услугата.*

В статията се предлага метод за количествена оценка на киберриска в телемедицина. Методът включва идентифициране на основните рискови компоненти, оценяване чрез нормализирани показатели, формиране на компонентен рисков вектор, претеглено агрегиране и корекция, която запазва влиянието на компонента с максимална рискова стойност. Въвежда се и параметър за критичност на телемедицинската услуга. Приложимостта на метода е проверена чрез три сценария с различен рисков профил и чрез повторна оценка след прилагане на защитна мярка. Резултатите показват ясно разграничаване на рисковите състояния и измеримо изменение на крайната оценка при промяна на техническите параметри.

Ключови думи: *телемедицина, киберриск, киберсигурност, информационни системи, комуникационни мрежи, медицински устройства, оценка на риска.*

METHOD FOR CYBER RISK ASSESSMENT IN TELEMEDICINE

Asst. Prof. Eng. **Petya Ivanova Petrova**, Ph.D

University of Telecommunications and Post, Sofia

Abstract: *The development of telemedicine expands the use of information and communication technologies for remote consultations, patient monitoring, and medical data exchange. The technological environment integrates endpoint devices, communication networks, application platforms, cloud and server resources, identity and access management systems, and connected medical devices. The interaction between these components creates a specific cyber-risk profile in which a local technical weakness may affect both information security and service availability.*

This paper proposes a method for quantitative cyber risk assessment in telemedicine. The method includes identification of the main risk components, assessment through normalized indicators, formation of a component risk vector, weighted aggregation, and a correction mechanism preserving the influence of the component with the highest risk value. A parameter representing the criticality of the telemedicine service is also introduced. The method is examined through three scenarios with different risk profiles and through reassessment after implementation of a protective measure. The results demonstrate differentiation between risk states and a measurable change in the final score when technical parameters are modified.

Keywords: *telemedicine, cyber risk, cybersecurity, information systems, communication networks, medical devices, risk assessment.*

Въведение

Телемедицината се утвърждава като технологична среда за дистанционно предоставяне на медицински услуги, обмен на медицинска информация и наблюдение на пациенти. Съвременните цифрови здравни системи включват организационни информационни системи, облачни услуги, мобилни и уеб приложения, програмни интерфейси и свързани медицински устройства [17], [18]. Подобна структура разширява технологичния периметър и увеличава зависимостта между компоненти, които могат да се намират както в инфраструктурата на лечебната организация, така и извън нея.

Особено значение има използването на лични устройства, домашни мрежи и медицинско оборудване в среда, която организацията не управлява непосредствено. NIST разглежда това като съществен източник на риск при telehealth и Hospital-at-Home реализации, тъй като компрометирани потребителски и IoT устройства могат да се превърнат в точки за достъп до здравни информационни ресурси [16]. Систематичните изследвания в областта също показват, че телемедицинските услуги са изложени на комбинирани рискове, свързани с удостоверяване, крайни устройства, комуникационна среда, приложения, медицински данни и свързани устройства [7], [12], [15].

Здравният сектор остава обект на интензивни кибератаки. ENISA идентифицира ransomware, нарушенията на данни и атаките срещу достъпността сред водещите заплахи за сектора [2]. Допълнителен технически риск произтича от медицинските и носимите устройства, при които защитата на комуникациите, актуалността на софтуера и достоверността на генерираните данни имат пряко значение за сигурността [1], [5].

При телемедицината отделните технически фактори не действат независимо. Компрометирано крайно устройство може да доведе до неправомерно използване на

идентичност; недостатъчно защитен комуникационен канал може да позволи прихващане или изменение на данни; уязвим приложен интерфейс може да осигури достъп до свързани ресурси; а отказ на мрежова или сървърна инфраструктура може да прекъсне самата услуга. Поради това оценяването следва да обхваща както компонентното състояние, така и общото влияние на взаимосвързаните технически области.

Общите принципи за управление на риска и информационната сигурност са формулирани в ISO 31000, ISO/IEC 27001 и ISO/IEC 27005, а NIST CSF 2.0 предоставя рамка за идентифициране, защита, откриване, реагиране, възстановяване и управление на киберриска [8]–[10], [14]. Тези подходи формират методологична основа, но при конкретна телемедицинска среда е необходимо компонентите да бъдат представени чрез съпоставими количествени показатели и да бъде отчетено значението на критично висок локален риск.

Целта на изследването е да се разработи **метод за количествена оценка на киберриска в телемедицина**, чрез който основните технически рискови компоненти да бъдат идентифицирани, оценени и обединени в интегрална стойност, без критично висок компонентен риск да бъде скрит чрез усредняване.

За постигане на целта се поставят следните задачи: да се определят основните технически компоненти на телемедицинската среда; да се дефинират показатели за количественото им оценяване; да се разработи механизъм за агрегиране, отчитащ относителната значимост и максималната компонентна стойност; да се включи критичността на услугата; и да се провери поведението на метода чрез сценарийна експериментална проверка.

Допълнителна особеност на телемедицинската среда е динамичният характер на нейния технологичен контекст. Един и същ потребител може да използва различни устройства и мрежи, а една и съща услуга може да бъде предоставяна през различни приложни и облачни компоненти. Това означава, че киберрискът не следва да се възприема като постоянна характеристика на системата, а като величина, която се изменя при промяна на конфигурацията, начина на достъп, използваните устройства или състоянието на комуникационната инфраструктура. Тази постановка е съвместима с принципа за контекстно ориентирано управление на риска в ISO 31000 и ISO/IEC 27005 [8], [10].

От гледна точка на европейската регулаторна среда значението на киберсигурността в здравеопазването се засилва и от NIS2 и Европейското пространство

за здравни данни [3], [4]. В настоящото изследване тези актове не се използват като основа за математическото изчисление, а като контекст, който потвърждава необходимостта цифровите здравни услуги да бъдат разглеждани като критична информационна среда, в която сигурността на системите, мрежите и данните трябва да се управлява систематично.

Използването на количествена оценка има практическо предимство, защото позволява сравняване на различни конфигурации и проследяване на изменението на риска във времето. Ако резултатът е представен само чрез качествени категории, като „нисък“ или „висок“, трудно може да бъде измерен ефектът от конкретна техническа мярка. При числова стойност е възможно да се сравни състоянието преди и след актуализация, сегментация на мрежата, внедряване на многофакторно удостоверяване или промяна на конфигурацията на медицинско устройство. Това е една от причините в настоящото изследване компонентните оценки да се нормализират и да се обединяват в интегрална стойност.

1. Киберриск в телемедицинската среда

Телемедицинската услуга може да бъде разглеждана като разпределена информационно-комуникационна среда, в която взаимодействат потребител, крайно устройство, мрежова инфраструктура, приложна платформа и медицински информационен ресурс. Обобщеният комуникационен маршрут се представя чрез:

[U \ → D \ → N \ → A \ → S \ → H,]

където (U) е потребителят, (D) – крайното устройство, (N) – комуникационната среда, (A) – приложната платформа, (S) – системната/сървърната инфраструктура, а (H) – медицинският информационен ресурс.

Тази последователност не изчерпва всички възможни архитектури, но позволява да бъдат отделени техническите области, които формират рисковия профил. На тази основа в метода се използват седем компонента:

[\mathbf{R}=[R_I,R_D,R_N,R_A,R_M,R_{MD},R_S],]

където (R_I) е рискът при идентичността и достъпа; (R_D) – при крайните устройства; (R_N) – при комуникационната среда; (R_A) – при приложните компоненти; (R_M) – при медицинските данни; (R_{MD}) – при свързаните медицински устройства; (R_S) – при достъпността и непрекъсваемостта.

Подобно компонентно разделяне е съвместимо с установените в литературата рискови области при telehealth, включващи удостоверяване, устройства, комуникации, приложения, защита на данните и медицинско оборудване [7], [12], [16]. То съответства

и на техническите категории, използвани в актуалните ръководства за цифрови здравни информационни системи [17], [18].

Таблица 1

Рискови компоненти и показатели

Компонент	Основни показатели за оценяване
(R_I)	многофакторно удостоверяване; управление на идентичности; права и роли; защита на сесии; привилегирован достъп
(R_D)	актуалност на софтуера; защита срещу зловреден код; локално криптиране; контрол на достъпа; управляемост на устройството
(R_N)	криптографска защита; сигурност на протоколите; сегментация; защита от прихващане; устойчивост на прекъсване
(R_A)	уязвимости; входна валидация; защита на API; управление на сесии; актуалност на компонентите
(R_M)	контрол на достъпа; криптиране; целостта; архивиране и възстановяване; проследимост
(R_{MD})	актуалност на firmware; сигурност на интерфейсите; удостоверяване; защита от промяна; достоверност на данните
(R_S)	резервираност; устойчивост на комуникациите; възстановяване; резервни ресурси; външни зависимости

Представената в Таблица 1 структура показва, че оценката обхваща целия основен технологичен маршрут на телемедицинската услуга – от идентификацията на потребителя и използваното крайно устройство до комуникационната среда, приложните компоненти, медицинските данни, свързаните медицински устройства и непрекъсваемостта на услугата. По този начин се осигурява компонентно покритие на основните технически области, в които може да възникне или да се развие киберриск. Таблицата показва също, че всеки компонент може да бъде свързан с конкретни и проверими показатели, което създава основа за последващото им количествено оценяване и нормализиране.

Компонентите са взаимозависими. Например компрометирано крайно устройство може да доведе до компрометиране на идентичност и последващ неправомерен достъп до медицински данни:

$$[R\_D \setminus \rightarrow R\_I \setminus \rightarrow R\_M.]$$

По аналогичен начин нарушение на комуникационната среда може да повлияе върху приложна сесия и впоследствие върху достъпността:

$$[R\_N \setminus \rightarrow R\_A \setminus \rightarrow R\_S.]$$

Затова компонентният вектор не се използва само като списък от независими оценки, а като вход към интегрална процедура за оценяване.

1.1. Избор на компонентната структура

Изборът на седем компонента е направен така, че да покрива основните технически точки на взаимодействие в телемедицинската услуга, без оценката да се

раздробява до прекомерно голям брой показатели. Компонентите са достатъчно общи, за да бъдат приложими към различни типове телемедицински услуги, но и достатъчно конкретни, за да бъдат свързани с измерими технически характеристики.

Компонентът за идентичност и достъп е отделен самостоятелно, защото дистанционната услуга зависи от надеждното установяване на участниците и правилното разпределение на права. Крайното устройство също е отделен компонент, тъй като в телемедицината значителна част от устройствата могат да бъдат извън централизираното управление на организацията. Комуникационната среда се разглежда самостоятелно поради двойното ѝ влияние върху поверителността и достъпността. Приложните компоненти и медицинските данни са разделени, защото уязвимостта на приложение и компрометирането на данните са различни технически състояния и изискват различни мерки. Свързаните медицински устройства са самостоятелен компонент поради специфичния им firmware, интерфейси и ограничения за актуализация [5], [16]. Накрая, достъпността и непрекъсваемостта се отделят като компонент, тъй като при телемедицината отказът на цифрова услуга може непосредствено да прекъсне медицинското взаимодействие.

Подобна компонентна логика е близка до рисковите области, идентифицирани в систематичния обзор на Houser et al. [7] и в модела за security evaluation на Kim et al. [12]. Разликата е, че настоящият метод не използва компонентите единствено като категории за описание на заплахите, а ги превръща в нормализирани количествени входове за последващо агрегиране.

1.2. Източници на данни за оценяването

За практическото приложение на метода е важно компонентните стойности да се основават на проверими данни. За R_I могат да се използват настройки за MFA, роли, привилегировани акаунти и регистри за удостоверяване. За R_D източници могат да бъдат данни от endpoint management, EDR/антивирусни системи, статус на актуализациите и криптиране на устройствата. За R_N могат да се използват конфигурации на защитни стени, VPN, TLS, сегментация, логове и показатели за наличност.

Оценката на R_A може да използва резултати от vulnerability scanning, penetration testing, анализ на API и управление на версии. За R_M могат да бъдат използвани настройки за криптиране, контрол на достъпа, журнализация, резервни копия и тестове за възстановяване. При R_{MD} са приложими данни за firmware, поддържани протоколи, удостоверяване, налични актуализации и механизми за контрол на целостта.

R_S може да се основава на резервираност, RTO/RPO, резултати от тестове за възстановяване и измерена наличност.

Тази връзка между показател и техническо доказателство е необходима, за да не се превърне количественият резултат в субективна числова оценка. WHO/Europe също поставя акцент върху оценяване на цифровите здравни системи чрез структурирани контролни области и доказателства [17], [18].

1.3. Технически зависимости и възможни направления на компрометиране

Компонентното разделяне не означава, че атаката се развива само в рамките на една област. В реална среда въздействието често преминава през последователност от компоненти. Компрометирането на идентичност може да започне от крайно устройство, да премине през приложния слой и да достигне до медицинските данни. По аналогичен начин уязвим медицински уред може да се превърне във входна точка към локална мрежа или към облачна услуга, ако интерфейсите и механизмите за удостоверяване са недостатъчно защитени.

От тази гледна точка компонентният вектор може да бъде използван не само като количествено представяне, но и като карта на възможните направления на развитие на инцидент. Ако R_D и R_I са едновременно високи, това може да показва повишен риск от кражба на идентификационни данни чрез компрометирано устройство. Ако R_N, R_A и R_S са високи, по-вероятен е сценарий, при който комуникационна или приложна слабост води до прекъсване на услугата.

Тази интерпретация е полезна при планиране на защитните мерки, защото показва, че редуцирането на един компонент може да има положителен ефект върху няколко възможни вериги на компрометиране. Например внедряване на многофакторно удостоверяване намалява R_I, но едновременно ограничава част от последствията от компрометирано устройство. Сегментацията и криптографската защита на комуникациите могат да повлияят върху R_N, но и да ограничат разпространението към приложните и медицинските ресурси.

Методът не моделира експлицитно вероятностите на всяка възможна атакуваща верига. Подобно разширение би изисквало графов модел или attack graph и би увеличило значително сложността. В настоящата разработка зависимостите се използват за интерпретация и приоритизация, докато количественото ядро остава компактно и приложимо.

2. Метод за оценка на киберриска

Предложеният метод се реализира чрез шест последователни стъпки:

[S_1\ → S_2\ → S_3\ → S_4\ → S_5\ → S_6.]

Таблица 2

Последователност на метода

Стъпка	Действие	Резултат
(S_1)	определяне на обхвата и вида на телемедицинската услуга	техническа конфигурация
(S_2)	определяне на приложимите рискови компоненти	компонентен набор
(S_3)	оценяване и нормализиране на показателите	(x_{ij}\in[0,1])
(S_4)	изчисляване на компонентните оценки	(R_i)
(S_5)	агрегиране и отчитане на критичността	(R_F) и рисково ниво
(S_6)	определяне на компонентния принос	приоритет за въздействие

Таблица 2 показва, че предложеният метод има ясно определена последователност от входно описание на телемедицинската услуга до формиране на крайна рискова оценка и определяне на приоритетите за въздействие. Всяка стъпка генерира резултат, който се използва като вход за следващата, поради което методът може да бъде възпроизвеждан при различни технически конфигурации. Последователността показва също, че крайната стойност на киберриска не се формира чрез еднократна експертна преценка, а чрез структурирана процедура за определяне, нормализиране, агрегиране и интерпретиране на компонентните рискове.

2.1. Входни и изходни данни на метода

Методът използва четири основни групи входни данни: описание на телемедицинската услуга; нормализирани стойности на техническите показатели; тегловни коефициенти на компонентите; и критичност на услугата. На изхода се получават компонентен рисков вектор, техническа интегрална стойност, крайна стойност на риска и приоритети за последващо въздействие. Формално входът може да бъде представен като множеството:

[\mathcal{I}={X,W,\lambda,\beta,C_T}],

където X съдържа нормализираните показатели, W – теглата, λ – чувствителността към максималния компонент, β – силата на контекстната корекция, а C_T – критичността на услугата. Изходът е:

[\mathcal{O}={\mathbf{R},R_B,R_T,R_F,P}].

Тази формализация ясно отделя процедурата по събиране на технически данни от изчислителното ядро.

2.2. Нормализиране на показателите

Всеки показател (x_{ij}) се оценява по петстепенна скала, ориентирана в посока на риска – по-високата стойност означава по-неблагоприятно състояние:

Ниво	Стойност
пренебрежим/липсващ риск	0.00
нисък	0.25
среден	0.50
висок	0.75
критичен	1.00

Използването на нулева долна граница осигурява съответствие с дефинирания интервал ([0,1]). След агрегиране на няколко показателя компонентната стойност може да приема и междинни стойности, например 0.20, 0.40 или 0.60.

За компонент (R_i), описан чрез (m_i) показатели, оценката е:

[R_i=\frac{\sum_{j=1}^{m_i}a_{ij}x_{ij}}{\sum_{j=1}^{m_i}a_{ij}}],

където (a_{ij}\ge0) е теглото на показател (j). При липса на емпирично основание за диференциране се използват равни тегла. Получава се:

[R_i\in[0,1]].

При определяне на теглата е важно да се избегне смесването на две различни понятия – вероятност за неблагоприятно състояние и значимост на компонента за услугата. В настоящия метод компонентната стойност R_i представя оценените рисково състояние, а w_i представя относителната значимост на компонента. Това разделение позволява еднаква компонентна стойност да има различно влияние в зависимост от конкретната телемедицинска архитектура.

При практическо внедряване теглата могат да бъдат определяни по няколко начина. Експертният подход е приложим, когато липсва достатъчно историческа информация. AHP може да се използва за систематизиране на експертните сравнения, както е показано и в съвременни анализи на телемедицински платформи [15]. При наличие на данни за инциденти и откази могат да се използват статистически оценки. Възможен е и хибриден подход, при който началните тегла се определят експертно и впоследствие се калибрират с натрупването на наблюдения.

2.3. Агрегиране на компонентния риск

За компонентите се определят тегла (w_i), като:

[w_i\ge0,\qquad \sum_{i=1}^{n}w_i=1.]

При липса на калибрирани данни може да се използва равномерно разпределение (w_i=1/n). При конкретно практическо приложение теглата следва да бъдат определяни

според зависимостта на услугата от съответния компонент. Подобно разграничаване на значимостта е съвместимо с принципите за контекстно ориентирана оценка на риска [8], [10].

Базовата интегрална стойност се изчислява чрез:

[R_B=\sum_{i=1}^{n}w_iR_i.]

Претеглената средна стойност представя общото състояние, но може да намали влиянието на единичен критичен компонент. Поради това се въвежда:

[R_{\max}=\max(R_i),]

а техническата оценка се определя чрез:

[R_T=(1-\lambda)R_B+\lambda R_{\max}\qquad 0\le\lambda\le1].

Параметърът (\lambda) контролира влиянието на максималната компонентна стойност. При (\lambda=0) методът се свежда до стандартно претеглено агрегиране. При по-висока стойност влиянието на локално критичния компонент нараства.

2.4. Отчитане на критичността на услугата

При еднакво техническо състояние последствията от прекъсване могат да бъдат различни при планова видеоконсултация и при непрекъснат дистанционен мониторинг. Затова се въвежда коефициент:

[C_T\in[0,1]],

който представя критичността на конкретната телемедицинска услуга. (C_T) не е технически риск и не дублира (R_S): (R_S) оценява вероятността и техническите предпоставки за недостъпност, докато (C_T) представя значимостта на услугата при такова нарушение.

За да се запази крайният резултат в интервала ([0,1]), без последващо изкуствено ограничаване, се използва ограничена корекция:

[\boxed{R_F=R_T+\beta C_T(1-R_T)}]

при:

[0\le\beta\le1].

Тази зависимост гарантира:

[R_T\le R_F\le1]

Когато (C_T=0), крайният риск е равен на техническата оценка. Когато критичността нараства, корекцията се увеличава пропорционално на оставащото разстояние до горната граница 1. По този начин не се допуска стойност над 1 и не е необходим оператор (\min). Крайният резултат се класифицира в пет нива:

Интервал на (R_F)	Ниво
(0.00\le R_F<0.20)	много ниско
(0.20\le R_F<0.40)	ниско
(0.40\le R_F<0.60)	средно
(0.60\le R_F<0.80)	високо
(0.80\le R_F\le1.00)	много високо

За приоритизиране може да се използва компонентният принос:

[P_i=w_iR_i.]

Той не замества анализа на (R_{\max}), а служи за подреждане на областите според приноса им към базовата оценка. При наличие на критичен компонент той се разглежда отделно независимо от стойността на (P_i).

За практическото определяне на C_T може да се използва предварително дефинирана скала, например 0.25 за планова услуга без непрекъсната зависимост, 0.50 за услуга със средна времева чувствителност, 0.75 за услуга с висока зависимост от непрекъснатостта и 1.00 за критична услуга, при която прекъсването може да има непосредствено значение за наблюдението. Тези стойности следва да бъдат адаптирани спрямо конкретната организационна и клинична среда и не се приемат като универсална нормативна класификация.

Ограничената форма на корекцията има и интерпретационно предимство. Ако техническият риск вече е много висок, например R_T=0.95, критичността не трябва да изведе резултата над допустимата горна граница. Формулата увеличава риска само в оставащото пространство до 1, което осигурява плавно насищане.

2.5. Проверки за консистентност на входните оценки

Преди изчисляване на интегралната стойност е необходимо да бъдат приложени проверки за консистентност. Първо, всички показатели трябва да бъдат ориентирани в една и съща посока на риска. Ако даден показател описва „ниво на защита“, той трябва да бъде преобразуван така, че по-високата стойност да означава по-висок риск. Второ, не трябва един и същ технически фактор да бъде включван едновременно в два компонента без ясно разграничение, защото това би довело до двойно отчитане.

Трето, липсваща информация не следва автоматично да се интерпретира като нисък риск. При практическо приложение може да се използва отделен статус „неоценено“ или консервативна стойност, докато бъде получено техническо доказателство. Това е особено важно при външни доставчици и медицински устройства, за които организацията може да не разполага с пълна информация за конфигурацията.

Четвърто, теглата трябва да бъдат нормализирани така, че сумата им да е единица. Ако част от компонентите не са приложими, теглата на останалите следва да бъдат

преизчислени, а не просто да се оставят непроменени. По този начин интегралната стойност остава съпоставима между различни конфигурации.

Тези проверки не променят математическата формула, но са необходими за надеждното практическо прилагане на метода.

3. Експериментална проверка и анализ

3.1. Критерии за интерпретация на експеримента

Проверката е насочена към три свойства на метода. Първото е **монотонност** – при равни други условия увеличаването на компонентния риск не трябва да води до намаляване на крайната стойност. Второто е **чувствителност към локален максимум** – критично висок компонент трябва да има по-голямо влияние от обикновено усредняване. Третото е **реакция при защитна мярка** – намаляването на съществен технически риск трябва да бъде отразено чрез измеримо намаляване на R_F.

Тези критерии не доказват емпирична точност спрямо реална честота на инциденти, но позволяват да се провери вътрешната математическа последователност на метода.

3.2. Експериментални сценарии

Сценарий 1 може да се разглежда като контролна конфигурация. Повечето компонентни стойности са ниски и само крайното устройство е по-рисково. Полученият нисък общ риск показва, че методът не надценява единична умерена слабост.

За проверка и доказване на функционалната работоспособност на предложения метод се приемат три експериментални сценария, формирани така, че да представят последователно различни състояния на телемедицинската среда – нисък, повишен и критичен рисков профил. Използването на три различими конфигурации позволява да се проследи поведението на метода при изменение както на отделните компонентни оценки, така и на максималния компонентен риск и критичността на услугата. Сценариите са подбрани така, че да проверят способността на метода да разграничава различни рискови състояния, чувствителността му към локално висок компонентен риск и реакцията на крайната оценка при промяна на техническите параметри. По този начин експерименталната проверка е насочена към установяване на функционалната работоспособност и вътрешната математическа последователност на метода, а не към доказване на статистическа или прогностична точност спрямо реални клинични инциденти.

За сравнимост се използват равни тегла:

[w_i=\frac{1}{7}].

Приема се:

[\lambda=0.30,\qquad \beta=0.20].

Тези стойности са **експериментални параметри**, избрани за демонстриране на поведението на метода, а не универсални константи.

Таблица 3

Входни стойности

Компонент	**Сценарий 1**	**Сценарий 2**	**Сценарий 3**
(R_I)	0.2	0.4	0.6
(R_D)	0.4	0.6	0.8
(R_N)	0.2	0.8	0.8
(R_A)	0.2	0.4	0.6
(R_M)	0.2	0.6	0.8
(R_{MD})	0.2	0.6	1
(R_S)	0.2	0.6	0.8
(C_T)	0.25	0.75	1

Данните в Таблица 3 показват целенасочено нарастване на рисковия профил между трите експериментални конфигурации. При Сценарий 1 преобладават ниски компонентни стойности, като единственото по-изразено отклонение е при крайното устройство. Тази конфигурация служи като базово състояние, чрез което се проверява дали методът формира ниска крайна оценка при ограничено наличие на технически слабости. При Сценарий 2 стойностите на няколко компонента се увеличават, като комуникационният риск достига 0.80. По този начин се създава ясно изразен локален максимум, който позволява да бъде проверено дали включването на R_max предотвратява прекомерното изглаждане на значим технически риск при изчисляването на интегралната стойност. Сценарий 3 представя най-неблагоприятната конфигурация. При него рискът на свързаното медицинско устройство достига максимална стойност 1.00, няколко други компонента са със стойност 0.80, а критичността на услугата е C_T=1.00. Тази конфигурация позволява да се провери поведението на метода в близост до горната граница на рисковата скала и да се установи дали контекстната корекция увеличава оценката, без крайният резултат да излиза извън интервала [0,1]. Следователно Таблица 3 представя три контролирани рискови конфигурации, чрез които последователно се проверява реакцията на метода при изменение на компонентния риск, локалния максимум и критичността на телемедицинската услуга.

За Сценарий 2:

[\mathbf{X}_{R2}=[0.40,0.60,0.80,0.40,0.60,0.60,0.60]].

Базовата стойност е:

[R_B=\frac{0.40+0.60+0.80+0.40+0.60+0.60+0.60}{7}\approx0.571].

При (R_{\max}=0.80) и (\lambda=0.30):

[R_T=0.70(0.571)+0.30(0.80)\approx0.640].

При (C_T=0.75) и (\beta=0.20):

[R_F=0.640+0.20(0.75)(1-0.640)\approx0.694].

Получената стойност съответства на високо ниво на киберриск.

Таблица 4

Резултати от експерименталната проверка

Сценарий	(R_B)	(R_{\max})	(R_T)	(C_T)	(R_F)	ниво
1	0.229	0.4	0.28	0.25	0.32	ниско
2	0.571	0.8	0.64	0.75	0.69	високо
3	0.771	1	0.84	1	0.87	много високо

Резултатите в Таблица 4 потвърждават функционалната работоспособност на предложения метод в рамките на зададените експериментални условия. За трите последователно усложняващи се конфигурации се получават крайни стойности R_F=0.316, R_F=0.694 и R_F=0.872, които ги класифицират съответно като ниско, високо и много високо рисково състояние. Получената градация съответства на предварително зададеното изменение на компонентните стойности и показва, че методът разграничава рискови конфигурации с различна техническа тежест. Резултатите показват и ефекта от включването на максималния компонентен риск. При Сценарий 2 базовата стойност R_B=0.571 се увеличава до техническа оценка R_T=0.640 при R_max=0.80. Това означава, че високата стойност на комуникационния риск запазва съществено влияние върху общата оценка и не се неутрализира чрез усредняване с останалите компоненти. При Сценарий 3 техническата оценка достига R_T=0.840, а след отчитане на максималната критичност на услугата крайната стойност се увеличава до R_F=0.872. Резултатът остава под горната граница 1.00, което потвърждава коректното действие на ограничената контекстна корекция. Следователно трите сценария показват, че методът изпълнява основните функционални изисквания, заложени при неговото разработване: реагира монотонно при увеличаване на компонентния риск, запазва влиянието на локално критичен компонент, отчита критичността на телемедицинската услуга и формира различими крайни рискови нива.

За проверка на реакцията при защитна мярка се приема, че при Сценарий 2 комуникационният риск се намалява:

[R_N:0.80\ \rightarrow0.40].

Новият вектор е:

$$\mathbf{X}'_{R2}=[0.40,0.60,0.40,0.40,0.60,0.60,0.60]].$$

Получава се:

$$R'_B\approx0.514,\qquad R'_{\max}=0.60,\qquad R'_T\approx0.540]$$

и:

$$R'_F=0.540+0.20(0.75)(1-0.540)\approx0.609].$$

След прилагането на мярката крайната стойност се намалява от 0.694 до 0.609, т.е. приблизително с 12.2%. Рискът остава в категория „висок“, което е логично, тъй като останалите компонентни стойности не са променени. Повторната оценка представлява допълнителна функционална проверка на метода: при промяна само на един съществен технически параметър – комуникационния риск – крайната стойност се изменя в очакваната посока. Това показва, че методът е чувствителен към реално изменение на техническото състояние и може количествено да отразява ефекта от приложена защитна мярка. Същевременно запазването на категорията „висок риск“ показва, че подобрението на един компонент не се интерпретира като автоматично отстраняване на общия риск, тъй като останалите непроменени компонентни стойности продължават да участват във формирането на крайния резултат. Така методът позволява да се оценява както ефектът от предприетото въздействие, така и остатъчният риск след неговото прилагане.

Чувствителността към максималния компонент се определя от структурата на (R_T). За компонент, който не е максимален:

$$\frac{\partial R_T}{\partial R_k}=(1-\lambda)w_k],$$

а за уникалния максимален компонент:

$$\frac{\partial R_T}{\partial R_{\max}}=(1-\lambda)w_{\max}+\lambda].$$

При $(w_i=1/7)$ и $(\lambda=0.30)$ непосредственото влияние е съответно 0.10 и 0.40. Следователно в използваната експериментална конфигурация промяна в максималния компонент има по-силно влияние върху техническата оценка. При равни максимални стойности функцията $(\max)$ не е диференцируема в класически смисъл; тогава анализът следва да се извършва по отделните възможни активни максимални компоненти.

Методът има няколко ограничения. Точността му зависи от качеството на входните оценки и от начина на определяне на теглата. Параметрите (λ), (β) и (C_T) трябва да бъдат калибрирани спрямо конкретната среда, а експерименталните стойности в настоящото изследване не следва да се приемат като универсални. При реално приложение оценките трябва да се основават на проверими технически данни – конфигурации, логове, резултати от сканиране за уязвимости, информация за актуализации, контрол на достъпа, мрежови настройки и показатели за непрекъсваемост.

Това е в съответствие с принципите за контекстно и доказателствено ориентирана оценка на риска [8], [10], [14].

В сравнение с общите рамки за управление на риска, предложението е насочено към конкретна телемедицинска компонентна структура и към количествено запазване на влиянието на локално критичен компонент. Съществуващи изследвания разглеждат модели за security evaluation на telemedicine systems и AHP-базирани оценки на телемедицински платформи [12], [15]. Настоящият метод се отличава с комбинирането на компонентен вектор, максимална компонентна корекция и отделен параметър за критичност на услугата в една последователна процедура.

3.3. Практическа приложимост

Практическото приложение на метода може да бъде реализирано периодично или при настъпване на съществена промяна в инфраструктурата. Периодичната оценка позволява проследяване на тенденцията, докато оценката при промяна е приложима при внедряване на нова телемедицинска платформа, включване на медицински устройства, промяна на доставчик на облачна услуга или значително преструктуриране на мрежовата среда.

Методът може да бъде използван и като част от процеса по третиране на риска. След първоначално изчисление компонентите могат да бъдат подредени по P_i и R_i, да бъдат избрани мерки и след изпълнението им да се извърши повторна оценка. По този начин се формира цикъл:

оценка → приоритизация → мярка → повторна оценка

Това е съвместимо с общата логика на ISO/IEC 27005 и NIST CSF 2.0 за непрекъснато управление и подобряване на киберриска [10], [14].

3.4. Ограничения и бъдеща валидация

Основното ограничение на настоящото изследване е, че използваните сценарии са конструирани. Те проверяват поведението на формулите, но не доказват прогностична точност спрямо реални инциденти. Следващ етап е необходимо да включи данни от реални телемедицински инфраструктури и сравнение между изчисленото рисково ниво и наблюдавани инциденти, уязвимости или резултати от технически тестове.

Необходимо е също да бъде изследвана чувствителността спрямо λ и β в по-широк диапазон. Например могат да се сравнят стойности на λ от 0.10 до 0.50 и да се анализира при какви условия максималният компонент започва да доминира прекомерно. По аналогичен начин β трябва да бъде калибриран така, че критичността на услугата да влияе върху резултата, без да измества значението на техническото състояние.

Допълнителна посока е разработването на формализирана процедура за определяне на теглата. Възможно е да бъдат сравнени равномерни тегла, експертни оценки, AHP и статистически калибрирани тегла. Така ще може да се оцени устойчивостта на метода спрямо начина на параметризиране.

3.5. Съпоставка с използвани подходи в литературата

Съществуващите публикации в областта на telemedicine cybersecurity използват различни механизми за оценяване. Kim et al. [12] предлагат risk management-based security evaluation model, който структурира рисковете чрез набор от области и използва attack-tree анализ. Този подход е подходящ за подробно проследяване на заплахите, но изисква по-детайлно моделиране на атакуващите пътища. Настоящият метод избира по-компактна компонентна структура и се фокусира върху количествената интегрална оценка.

Nobili et al. [15] анализират telemedicine platform чрез многокритериален подход и AHP. AHP има предимство при определянето на относителната значимост на критериите, но резултатът зависи от експертните двойни сравнения. В настоящата разработка AHP може да бъде използван като допълнителен инструмент за определяне на w_i, без да бъде задължителна част от изчислителното ядро.

Систематичният обзор на Houser et al. [7] идентифицира разнообразни privacy and security risk factors, което показва необходимостта от широк обхват на оценяването. Настоящият метод не се стреми да включи всички възможни фактори като отделни променливи, а да ги групира в технически компоненти. Това намалява размерността и улеснява практическото приложение.

WHO/Europe [17], [18] предоставя maturity-oriented assessment на цифрови здравни информационни системи. Този тип оценка е подходящ за определяне на зрелостта на контролите и организационните практики. Предложеният тук подход има различна цел – да формира количествена стойност на техническия киберриск и да проследява нейното изменение. Двата подхода могат да бъдат допълващи се: maturity assessment може да идентифицира слабите контролни области, а количественият метод да оцени техния принос към общия риск.

Тази съпоставка показва, че предложението не дублира директно съществуващите методи. Неговият отличителен елемент е комбинацията от компонентен рисков вектор, претеглено агрегиране, максимална компонентна корекция и отделен контекстен параметър за критичност на услугата.

Заключение

В изследването е разработен метод за количествена оценка на киберриска в телемедицина, основан на седем технически рискови компонента: идентичност и достъп, крайни устройства, комуникационна среда, приложни компоненти, медицински данни, свързани медицински устройства и достъпност на услугата. Компонентното представяне позволява разпределената телемедицинска среда да бъде преобразувана в структуриран рисков вектор и да бъде оценявана чрез нормализирани показатели.

Основният математически механизъм съчетава претеглена компонентна оценка с корекция, отчитаща компонента с максимален риск. По този начин се намалява възможността локално критично състояние да бъде прикрито при усредняването. Допълнителният коефициент за критичност позволява техническата оценка да бъде свързана с предназначението на конкретната телемедицинска услуга, без да се допуска излизане на крайния резултат извън интервала ([0,1]).

Проведената проверка чрез три експериментални сценария потвърждава функционалната работоспособност и вътрешната математическа последователност на предложения метод. Получени са различими крайни стойности – 0.316, 0.694 и 0.872 – съответстващи на ниско, високо и много високо рисково състояние. Последователното им нарастване показва, че методът реагира адекватно при увеличаване на компонентния риск, като едновременно запазва влиянието на локално критичния компонент и отчита критичността на телемедицинската услуга. При намаляване на комуникационния риск във втория сценарий интегралната стойност се понижава от 0.694 до 0.609, което допълнително потвърждава чувствителността на метода към промяна на техническото състояние и възможността за количествено сравнение преди и след прилагане на защитна мярка.

Резултатите на настоящия етап представляват сценарийна проверка на поведението на метода. Следващо развитие следва да включи калибриране на тегловните коефициенти и параметрите (\lambda) и (\beta) върху реални данни, експертна оценка на критичността на услугите и емпирична валидация в реални телемедицински инфраструктури.

Литература

[1] **Chikwetu, L., Miao, Y., Woldetensae, M. K., Bell, D., Goldenholz, D. M., & Dunn, J.** (2023). Does deidentification of data from wearable devices give us a false sense of security? A systematic review. *The Lancet Digital Health, 5*(4), e239–e247. https://doi.org/10.1016/S2589-7500(22)00234-5.

[2] **ENISA.** (2023). *ENISA Threat Landscape: Health Sector*. European Union Agency for Cybersecurity.

[3] **European Parliament and Council of the European Union.** (2022). *Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union (NIS2 Directive). Official Journal of the European Union*.

[4] **European Parliament and Council of the European Union.** (2025). *Regulation (EU) 2025/327 of the European Parliament and of the Council of 11 February 2025 on the European Health Data Space and amending Directive 2011/24/EU and Regulation (EU) 2024/2847. Official Journal of the European Union*.

[5] **Freyer, O., Jahed, F., Ostermann, M., Rosenzweig, C., Werner, P., & Gilbert, S.** (2024). Consideration of cybersecurity risks in the benefit-risk analysis of medical devices: Scoping review. *Journal of Medical Internet Research, 26*, e65528. https://doi.org/10.2196/65528

[6] **Govindarajan, U. H., Singh, D. K., & Gohel, H. A.** (2023). Forecasting cyber security threats landscape and associated technical trends in telehealth using Bidirectional Encoder Representations from Transformers (BERT). *Computers & Security, 133*, 103404. https://doi.org/10.1016/j.cose.2023.103404

[7] **Houser, S. H., Flite, C. A., & Foster, S. L.** (2023). Privacy and security risk factors related to telehealth services: A systematic review. *Perspectives in Health Information Management, 20*(1), 1f.

[8] **International Organization for Standardization.** (2018). *ISO 31000:2018 Risk management — Guidelines*. ISO.

[9] **International Organization for Standardization & International Electrotechnical Commission.** (2022). *ISO/IEC 27001:2022 Information security, cybersecurity and privacy protection — Information security management systems — Requirements*. ISO.

[10] **International Organization for Standardization & International Electrotechnical Commission.** (2022). *ISO/IEC 27005:2022 Information security, cybersecurity and privacy protection — Guidance on managing information security risks*. ISO.

[11] **Javaid, M., Haleem, A., Singh, R. P., & Suman, R.** (2023). Towards insighting cybersecurity for healthcare domains: A comprehensive review of recent practices and trends. *Cyber Security and Applications, 1*, 100016. https://doi.org/10.1016/j.csa.2023.100016

[12] **Kim, D.-W., Choi, J.-Y., & Han, K.-H.** (2020). Risk management-based security evaluation model for telemedicine systems. *BMC Medical Informatics and Decision Making, 20*, 106. https://doi.org/10.1186/s12911-020-01145-7

[13] **Lieneck, C., McLauchlan, M., & Phillips, S.** (2023). Healthcare cybersecurity ethical concerns during the COVID-19 global pandemic: A rapid review. *Healthcare, 11*(22), 2983. https://doi.org/10.3390/healthcare11222983

[14] **National Institute of Standards and Technology.** (2024). *The NIST Cybersecurity Framework (CSF) 2.0*. NIST Cybersecurity White Paper 29. https://doi.org/10.6028/NIST.CSWP.29

[15] **Nobili, M., Raguseo, D., & Setola, R.** (2025). Cybersecurity analysis of a telemedicine platform. *Healthcare, 13*(2), 184. https://doi.org/10.3390/healthcare13020184

[16] **Pulivarti, R., Littlefield, K., Wang, S., Patrick, B., & Williams, R.** (2025). *Mitigating cybersecurity and privacy risks in telehealth smart home integration*. NIST Cybersecurity

White Paper 34. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.CSWP.34
[17] **World Health Organization, Regional Office for Europe.** (2025a). *Cybersecurity and privacy maturity assessment and strengthening for digital health information systems*. WHO Regional Office for Europe. WHO/EURO:2025-11827-51599-78854.
[18] **World Health Organization, Regional Office for Europe.** (2025b). *Cybersecurity and privacy maturity assessment and strengthening for digital health information systems: Web annex – Assessment instrument*. WHO Regional Office for Europe. WHO/EURO:2025-11827-51599-79106.