

ИНТЕГРИРАН РИСК-БАЗИРАН МОДЕЛ ЗА УПРАВЛЕНИЕ НА ФИЗИЧЕСКАТА СИГУРНОСТ НА КЛАСИФИЦИРАНАТА ИНФОРМАЦИЯ

Георги Петровалиев

Докторант в задочна форма на обучение

Университет по библиотекознание и информационни технологии

Резюме: Докладът представя интегриран риск-базиран модел за управление на системата от мерки за физическа сигурност при защита на класифицираната информация. Моделът обвързва средата, риска, управленското решение, организационните, човешките и техническите компоненти, контрола и обратната връзка. Изведени са шест критериални области и механизъм за проследяване на коригиращите действия. Представени са резултатите от логическа верификация и експертна съдържателна валидация със седем експерти. Очертани са ограниченията на изследването и необходимостта от последващо независимо практическо пилотиране.

Ключови думи: класифицирана информация; физическа сигурност; управление на риска; интегриран модел; експертна валидация; управленска проследимост.

INTEGRATED RISK-BASED MODEL FOR MANAGING THE PHYSICAL SECURITY OF CLASSIFIED INFORMATION

Georgi Petrovaliev

Part-time PhD Student

University of Library Studies and Information Technologies

Abstract: This paper presents an integrated risk-based model for managing physical security measures protecting classified information. The model links context, risk assessment, managerial decisions, organizational, human and technical components, control, and feedback. Six assessment domains and a mechanism for tracing corrective actions are proposed. The study reports logical verification and expert content validation involving seven experts. The results support the conceptual coherence and methodological acceptability of the model, while operational effectiveness remains to be established through independent field testing and longitudinal evaluation.

Keywords: classified information; physical security; risk management; integrated model; expert validation; management traceability.

1. Въведение

Защитата на класифицираната информация от нерегламентиран достъп изисква съгласувано действие на нормативни, организационни, човешки и технически мерки. Физическата сигурност не може да бъде оценявана единствено чрез наличието на отделни защитни средства: решаващо значение има способността на управлението да идентифицира риска, да обосновава приоритетите, да разпределя отговорностите и да осигурява проверима обратна връзка. Националната правна рамка е установена в Закона за защита на класифицираната информация и правилника за неговото прилагане (Закон за защита на класифицираната информация; Правилник за прилагане на ЗЗКИ, 2002).

Изследователският проблем произтича от възможното разминаване между формално въведени мерки и тяхното интегрирано управление. Системният подход на Rasmussen (1997) и управлението чрез ранни индикатори при Leveson (2015) подкрепят разбирането, че рискът е динамичен и се влияе от взаимосвързани решения. Стандартът ISO 31000:2018 (ISO, 2018) предоставя методически ориентир за процеса на управление на риска, без да заменя задължителните национални изисквания.

Целта на доклада е да представи архитектурата на разработения в дисертационното изследване интегриран модел, неговата критериална система и основните резултати от експертната му проверка. Работната постановка е, че свързването на оценката на риска с решенията, изпълнението, контрола и корекциите създава проследима управленска рамка. Практическото повишаване на ефективността остава предмет на бъдеща емпирична проверка.

2. Методологическа основа

Използван е комбиниран изследователски подход, включващ теоретичен и нормативен анализ, емпирично проучване чрез седем анкетни карти и седем експертни интервюта, конструиране на модел, структурно-логическа верификация, експертна съдържателна валидация и сценарийна апробация. Експертната извадка е малка и целенасочена. Тя позволява качествено изследване на управленските зависимости, но не е основание за статистическо обобщение към всички организации.

При събирането и анализа на данните не са използвани сведения за идентифицируеми защитени обекти, оперативни конфигурации, конкретни пропускателни режими или "класифицирана информация, представляваща държавна или служебна тайна". Това ограничава възможността за непосредствено измерване на оперативни резултати, но позволява изследване на управленските функции на обобщено равнище.

В теоретичен план моделът се основава на системност, риск-базираност, интеграция, проследимост, измеримост, пропорционалност и адаптивност. Разграничават се три функции: описателна (компоненти и отношения), обяснителна (връзки между управленските действия) и предписваща (последователност за оценяване и корекция).

Изследователската логика следва разграничението между установяване на управленски проблем, конструиране на методически инструмент и оценяване на неговата съдържателна пригодност. В дисертационното изследване теоретичният и нормативният анализ очертават границите на допустимото управление, а емпиричният материал служи за извеждане на потребности, които не могат да бъдат обяснени само чрез формално наличие на правила. По този начин моделът не се извежда от един нормативен документ или от механично обединяване на контролни списъци, а от съпоставяне на различни източници на аргументация.

Емпиричната основа включва анкетни данни и експертни интервюта, анализирани на обобщено равнище. Тяхното предназначение е проучвателно: да открият възприемани дефицити в координацията, връзката между риск и решение, подготовката, контрола и обратната връзка. Ограниченият обем на извадката не позволява статистическо обобщаване за всички организации, които работят с класифицирана информация. Затова получените наблюдения се използват като основание за конструиране и експертно обсъждане на методическия модел, а не като измерване на разпространението на конкретни нарушения.

Методическата последователност е организирана в няколко етапа: извеждане на управленските функции; дефиниране на компонентите и техните отношения; преобразуване на установените потребности в критериални области; определяне на допустими показатели и доказателства; структурно-логическа проверка; съдържателна експертна оценка и сценарийно обсъждане. Всеки етап има различен доказателствен статут. Логическата непротиворечивост например е необходимо условие за приложение, но сама по себе си не доказва защитен резултат в реална среда.

3. Архитектура на интегрирания модел

Интегрираният модел се представя чрез формалната конструкция $M = \square E, R, D, O, H, T, C, F\square$, където E е средата и контекстът; R — оценката на риска; D — управленското решение; O — организационният компонент; H — човешкият компонент; T — техническият компонент; C — контролът; F — обратната връзка. Основното отношение на управленска проследимост е $P: R \rightarrow D \rightarrow \{O, H, T\} \rightarrow C \rightarrow F$.

Тази конструкция изисква за всяко съществено управленско решение да може да бъде възстановена връзката между установения риск, избраното действие, отговорните звена, доказателствата от контрола и последващата корекция. Следователно моделът не е статичен каталог на мерки, а затворен управленски цикъл. Той не създава нови правомощия, не отменя нормативни процедури и не допуска отклоняване от задължителни изисквания въз основа на субективна оценка на риска.

Практическата последователност включва идентифициране на контекста и риска, приоритизиране, разпределение на отговорности и ресурси, изпълнение, контрол, оценяване на остатъчния риск и актуализиране. Точките за управленско решение D1–D3 служат за преценка на необходимото действие, адекватността на изпълнението и приемливостта на остатъчния риск. При установено отклонение се изискват коригиращо действие и повторна проверка.

Освен осемте компонента, определяща характеристика на модела е отношението на управленска проследимост $P: R \rightarrow D \rightarrow \{O, H, T\} \rightarrow C \rightarrow F$. То означава, че всяка значима оценка на риска следва да може да се свърже с компетентно управленско решение, с конкретизирани отговорности и категории мерки, с проверка на изпълнението и с последваща реакция. Проследимостта не се свежда до съхраняване на документи, тя предполага доказуема причинно-управленска връзка между основанията за решение и неговото изпълнение.

Компонентът Е определя контекста, приложими изисквания, организационни функции, информационни активи и ограничения. Компонентът R идентифицира и оценява рисковете на подходящо ниво на обобщение, докато D обозначава компетентния избор на действие. Това разграничение е важно, защото аналитичната препоръка не е равнозначна на утвърдено решение. Организационният компонент О задава разпределението на роли и координацията, Н обхваща подготовката и човешкото изпълнение, а Т се отнася до управлението на техническите мерки през техния жизнен цикъл.

Контролът С установява съответствието между очакваното и фактическото състояние, а обратната връзка F насочва коригиращото действие и актуализирането на предходните оценки. При установено отклонение е възможно да се наложи промяна не само в техническа мярка, но и в организационните отговорности, обучението или първоначалната рискова оценка. Така обратната връзка затваря цикъла на управление и позволява системата да се адаптира към промяна на условията.

Моделът не представлява формула за изчисляване на вероятност от нерегламентиран достъп. Неговата формализация има структурно-аналитично предназначение, и то е да показва кои управленски отношения трябва да бъдат проверени. Това позволява да се избегне неправомерното представяне на един обобщен бал като пряко измерване на сигурността. По същата причина положителната оценка на един компонент не следва автоматично да компенсира критична слабост в друг.

4. Критериална система и оценяване

Въз основа на теоретичния анализ и емпирично установените потребности са формулирани шест взаимосвързани критериални области. Таблица 1 обобщава тяхното управленско предназначение, като представя съкратено критериалната структура на дисертационния модел.

Таблица 1

Критериални области на интегрирания модел

Критериална област	Предмет на оценяване
K1. Риск-базирано планиране	Връзка между оценката на риска, приоритетите и ресурсните решения.
K2. Координация и отговорности	Яснота на ролите, взаимодействието и изпълнението на решенията.
K3. Човешки фактор и подготовка	Съответствие на подготовката с функциите и актуализиране при промяна.
K4. Контрол и коригиращи действия	Проследяване на отклоненията, корекциите и повторните проверки.
K5. Технически мерки	Поддръжка, работоспособност и актуализация през жизнения цикъл.
K6. Интегрирано управление	Съгласуваност между риск, организационни, човешки и технически мерки.

Шестте области имат едновременно диагностична и конструктивна функция, при която те показват къде възниква управленски дефицит и към кой компонент следва да се насочи коригиращото действие. При оценяването се разграничават входни, процесни, резултатни показатели и показатели за обратна връзка. В съответствие с ограниченията на малката експертна извадка не се въвеждат универсални числови прагове или тежести.

Предложеният управленски инструментариум включва матрица за проследимост и управленско табло, в които се свързват показателят, източникът на доказателство, констатираното отклонение, отговорното лице или звено, коригиращото действие, срокът и повторната проверка. Подходът е съпоставим на методическо равнище с разграничението между мерки за контрол и оценяване на тяхното изпълнение в NIST SP 800-53 и SP 800-53A (NIST, 2020; NIST, 2022), без тези документи да се третира като пряко приложими национални правни норми.

Критериалните области образуват функционална последователност. К1 проверява дали оценката на риска действително влияе върху приоритетите и ресурсите. К2 разглежда разпределението на отговорностите и координацията, включително при конкуриращи се задачи. К3 поставя акцент върху съответствието между подготовката на персонала и възложените функции, а не само върху броя проведени обучения. К4 проследява цикъла „контрол – коригиращо действие – повторна проверка“. К5 оценява процесите по поддръжка и обновяване на техническите мерки, без да разкрива конкретни конфигурации. К6 обединява информацията от останалите области и проверява дали тя води до управленско адаптиране.

Предложеното оценяване използва петстепенна порядкова скала, като липсата на приложимост се отбелязва отделно с „НП“. Скалата подпомага съпоставимото описание на степента на прилагане и проследимост на дадена функция, но не измерва пряко вероятността за инцидент. При липса на надеждни доказателства не бива да се присъжда привидно точна оценка. Непълнотата на информацията се отчита като самостоятелно ограничение, което може да наложи допълнителна проверка.

Практическото използване на критериалната матрица изисква разграничаване между наличие на правило, доказателство за изпълнение и резултат от проверка. Например съществуването на утвърден ред не доказва, че координацията функционира при промяна на условията. Аналогично наличието на отчет за обучение не удостоверява автоматично готовността за изпълнение на конкретна задача. Това разграничение създава възможност оценката да посочва не само слабост, но и необходимата управленска реакция.

5. Верификация и експертна валидация

Структурно-логическата верификация обхваща пълнотата на осемте компонента, последователността на управленската проследимост, функционалната свързаност на критериите К1–К6 и затворения цикъл на коригиращите действия. Проверява се дали всяка функция има теоретично или нормативно основание, емпирична опора, определено място в модела, наблюдаем резултат и връзка с обратната връзка.

Експертната съдържателна валидация е проведена със седем експерти, обозначени с кодове V01–V07. Според окончателната матрица на дисертационното изследване са получени 105 от 105 максимални оценки по част А и 35 от 35 максимални оценки по част С. При сценарийната проверка са отчетени 84 от 84 положителни оценки. Използвани са четири обобщени сценария, които не съдържат данни за реални защитени обекти.

Единодушната експертна подкрепа обосновава съдържателната приемливост и логическата съгласуваност на предложената рамка в рамките на конкретния панел. Липсата на вариация в оценките обаче ограничава възможността за анализ на различия между експертите. Резултатите не представляват доказателство за измерено намаляване на нерегламентирания достъп, за подобрена оперативна резултатност или за ефект след реално внедряване.

Съдържателната валидация и сценарийната апробация отговарят на различни въпроси. Първата изследва дали предложените компоненти, критерии и връзки са разбираеми, релевантни и логически съгласувани според участващите експерти. Втората проверява дали последователността на управленските действия може да бъде приложена логически към типови ситуации. В дисертационното изследване са използвани четири обобщени сценария: промяна в рисковата среда, установено отклонение при контрол, организационна или кадрова промяна и изменение в техническия компонент.

Сценарийната проверка се провежда на абстрактно ниво, без разкриване на реални защитени обекти, конкретни режимни зони или технически конфигурации. Това е съществено условие за публичното научно представяне на темата. Същевременно положителните сценарийни отговори не могат да бъдат приравнени на наблюдение на реална реакция на персонала или на измерено намаляване на остатъчния риск. За подобна оценка е необходим отделен етап на внедряване и проследяване.

6. Научно-приложни резултати и ограничения

Основният научен резултат е систематизирането на физическата сигурност като динамична управленска система, в която оценката на риска има значение само ако води до проследими решения, изпълнение, контрол и адаптация. Формалната архитектура М и отношението Р предоставят общ език за описание на зависимостите между управленските функции. Шестте критериални области създават основа за проверяемо оценяване, което не се свежда до преброяване на налични мерки.

Научно-приложната стойност е свързана с възможността за използване на алгоритмичната последователност, критериалната матрица и управленското табло като помощни инструменти при вътрешна оценка и планиране на коригиращи действия. Прилагането им следва да се съобразява с конкретния правен режим, компетентностите и ограниченията за достъп до информация.

Ограниченията включват целенасочения малък експертен панел, липсата на вариация в окончателните оценки, използването на обобщени сценарии и отсъствието на сравнителни наблюдения при реално внедряване. Поради това бъдещата работа трябва

да включва независимо пилотно прилагане, калибриране на показатели, изходно и последващо измерване и проверка на устойчивостта на резултатите в различни организационни условия.

Практическото прилагане на модела може да се разгърне в три управленски ситуации: първоначално структуриране на оценката, периодичен преглед на вече действащи мерки и извънредно преразглеждане при съществена промяна на средата. Във всеки случай е необходимо предварително да се определят обхватът, отговорните лица, допустимите информационни източници, редът за утвърждаване на решения и механизмът за последващ контрол. Без тези предпоставки инструментът рискува да остане формален отчет.

Важен принцип е нормативната подчиненост на модела. Той не въвежда нов правен режим, не изменя компетентностите на органите и не може да оправдае неизпълнение на задължителна мярка въз основа на благоприятна оценка по друг критерий. Неговата функция е да подпомага обосноваването и проследяването на решения в рамките на приложимата уредба. При практическо използване оценяването трябва да бъде пропорционално на организационния капацитет и да не създава ненужна административна тежест.

За последваща емпирична проверка могат да се проследяват предварително определени, допустими за обобщаване индикатори: своевременност на коригиращите действия, пълнота на доказателствата, честота на преразглеждане на рисковите основания и изпълнение на планираните проверки. Подобно наблюдение би позволило да се изследва дали използването на модела действително подобрява управленската проследимост. Едва след това могат да се обсъждат по-силни твърдения за ефективност, и то при ясно определени показатели и сравнителна основа.

7. Заключение

Представеният интегриран модел обвързва нормативно съобразеното управление на физическата сигурност с оценката на риска, управленското решение, координираното изпълнение и проверимата обратна връзка. Разработената критериална система и инструментите за проследимост подпомагат аргументирането на управленските действия и създават предпоставки за последващо емпирично измерване. Логическата верификация и експертната валидация подкрепят методическата съгласуваност на модела, но не заменят проверката на неговата ефективност в реална среда.

Използвана литература

Закон за защита на класифицираната информация. Официален текст: ДКСИ.

<https://www.dksi.bg/нормативна-уредба/закон/>.

Правилник за прилагане на Закона за защита на класифицираната информация. ПМС № 276 от 02.12.2002 г.

ISO. ISO 31000:2018. Risk management — Guidelines. Geneva: International Organization for Standardization, 2018.

Leveson, N. G. A systems approach to risk management through leading safety indicators. – B: Reliability Engineering & System Safety. 2015, Vol. 136, p. 17 – 34.

NIST. Assessing Security and Privacy Controls in Information Systems and Organizations. NIST SP 800-53A, Rev. 5. 2022.

NIST. Security and Privacy Controls for Information Systems and Organizations. NIST SP 800-53, Rev. 5. 2020.

Rasmussen, J. Risk management in a dynamic society: A modelling problem. – B: Safety Science. 1997, Vol. 27, № 2–3, p. 183 – 213.