IT4Sec Reports 145
http://dx.doi.org/10.11610/it4sec.0145

„Балансът“ като панацея за постигане на (кибер)сигурност

Венелин Георгиев

Институт по информационни и комуникационни технологии – БАН
секция “Информационни технологии в сигурността”
и секция „Оптимизация и моделиране“
www.IT4Sec.org

София, септември 2022

Венелин Георгиев, „Балансът“ като панацея за постигане на (кибер)сигурност**,** *IT4Sec Reports 145* (септември 2022), http://dx.doi.org/10.11610/it4sec.0145

IT4Sec Reports 145 „Балансът“ като панацея за постигане на (кибер)сигурност. Взимането на решения в сложна, комплексна, многослойна и мултифакторна среда, каквато е средата за сигурност, изисква постигане на баланс между факторите на заплахата и стратегиите за противодействие срещу тях. В този смисъл търсенето на единствено, опростено решение, разглеждано като панацея представлява нерационален управленски подход. В доклада се представят резултатите от изследване за разработване на модел за балансиране на решенията в сферата на киберсигурността.

Ключови думи: киберсигурност, контроли за сигурност, уязвимости, заплахи, рискове, способности, сценарии, баланс, панацея

IT4SecReports 145 "The "Balance" as a panacea for achieving (cyber) security" Decision-making in a complex, complex, multi-layered and multifactorial environment, such as the security environment, requires a balance between threat factors and strategies to counter them. In this sense, the search for a single, simple solution, seen as a panacea, is an irrational management approach. The report presents the results of a study to develop a model for balancing cybersecurity solutions.

Keywords: cybersecurity, security controls, vulnerabilities, threats, risks, capabilities, scenarios, balance, panacea

ISSN 1314-2119

ВЪВЕДЕНИЕ

Един от възможните и нерядко използвани подходи за търсене на решение по въпроси в сложен и комплексен контекст е свързан с модифициране на многофакторната среда и формулиране на опростено решение, което се възприема като панацея. Като пресен пример може да бъде посочен планът за противодействие срещу кризата, предизвикана от пандемията от COVID-19, който се базира на решения, до които се достига при отчитане на единствен фактор, който в случая е броят на заетите легла за интензивно лечение, с които разполагат болничните заведения.

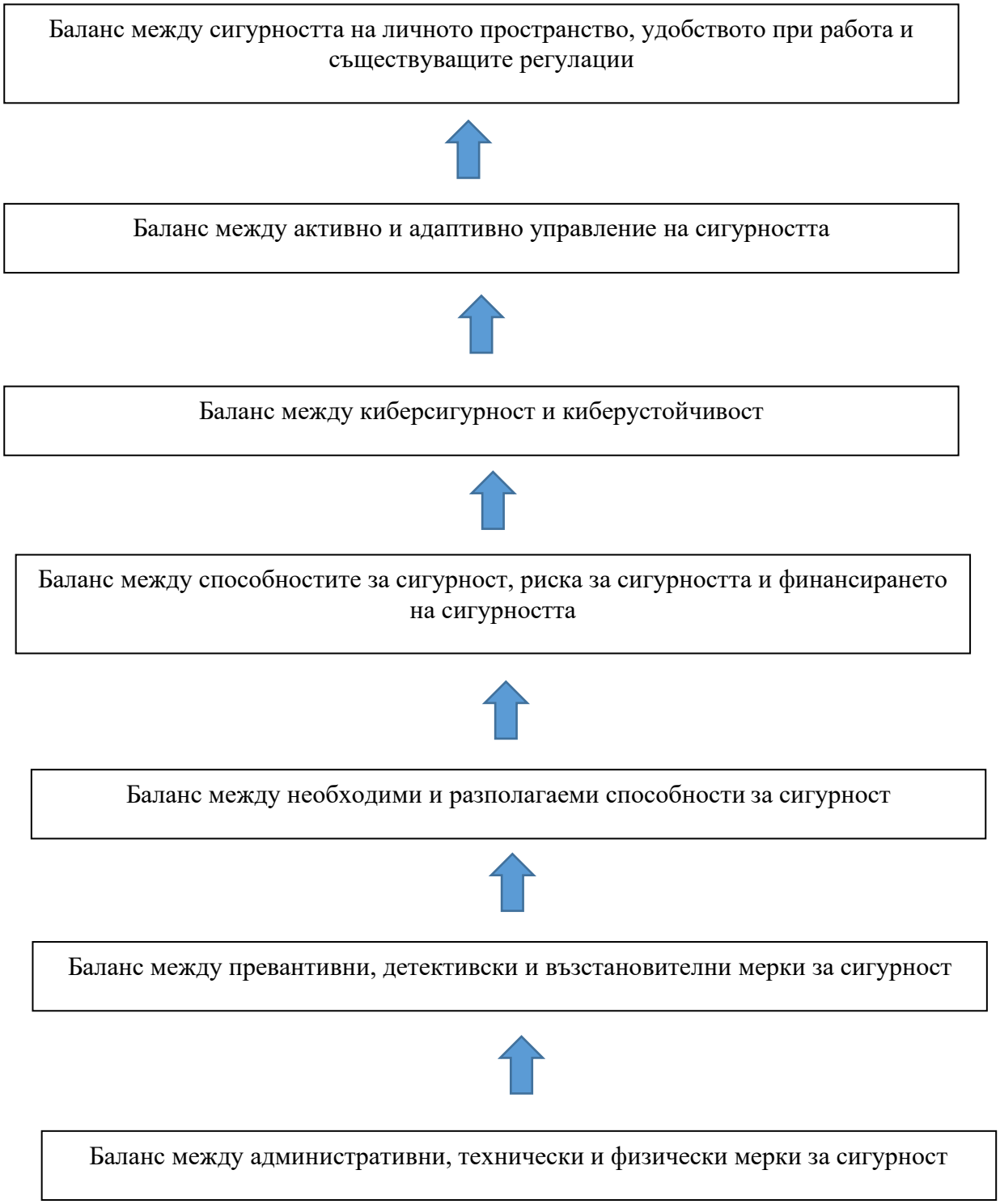
Подобен подход за опростяване видимо се прилага и при решаване на проблеми в сферата на сигурността и в частност в сферата на киберсигурността. Тук възниква въпросът доколко опростяването на средата повлиява върху ефективността на взиманите решения и доколко е възможно действително да се намери панацея (единствено правилно решение), която да реши всички проблеми в киберсигурността. От друга страна, в рационалния случай решаването на въпроси в многофакторна среда изисква търсене и постигане на баланс между влияещите фактори на заплахите и между стратегиите за противодействие срещу тях по начин, който да снижи заплахите, да компенсира уязвимостите и да сведе риска за сигурността до нивото на приемливия риск, т.е. до нивото на апетита към риска. На фона на направените по-горе коментари се поставя въпросът за това дали балансът може да играе ролята на панацея, когато се търси решение за проблемите в сигурността и в частност в киберсигурността. Защо именно балансът? Защото едно от клишетата, в което има голяма доза логика казва, че една среда или една система е толкова сигурна, колкото е сигурно нейното най-слабо звено.

Изследването, резултатите от което се представят в доклада е извършено с помощта на изследователски методи като анализ на документи, анализ, синтез и моделиране. Целта пред изследването е да бъде доказана верността на тезата за това, че в многофакторна среда търсенето на панацея чрез опростяване на решенията не води до постигане на резултати, отговарящи на потребностите от сигурност

МНОГОСЛОЕН, МУЛТИФАКТОРЕН МОДЕЛ ЗА БАЛАНСИРАНЕ НА РЕШЕНИЯТА ПО ПРОБЛЕМИТЕ НА КИБЕРСИГУРНОСТТА

Отсъствието на възможност за провеждане на изследване в реална среда налага необходимостта от използване на моделния подход, с помощта на който да се разработи адекватен на теоретичните концепции и добри практики модел за балансиране на решенията в сферата на киберсигурността на различни нива на конкретност. Моделният подход е целесъобразен предвид на факта, че той позволява създаване на модел с отчитане на различни фактори на заплахите и различни слоеве в сложната киберсреда. Ползата от модела се допълва и от възможностите за неговото използване за провеждане на изследвания в рамките на различни сценарии, т.е. в рамките на различни комбинации от влияещи фактори (сценарийни конфигурации).

Създаването и използването на многослоен модел за балансиране на решенията в сферата на киберсигурността налага търсенето на баланс в различните слоеве и различните аспекти на киберпространството. Анализът на тези варианти за намиране на баланс се прави с помощта на подхода отдолу-нагоре, т.е. анализът започва със слоеве с по-високо ниво на конкретност и преминава към слоеве с по-общ характер, но намиращи се във връзка със слоевете от по-ниските нива (виж фиг. 1).

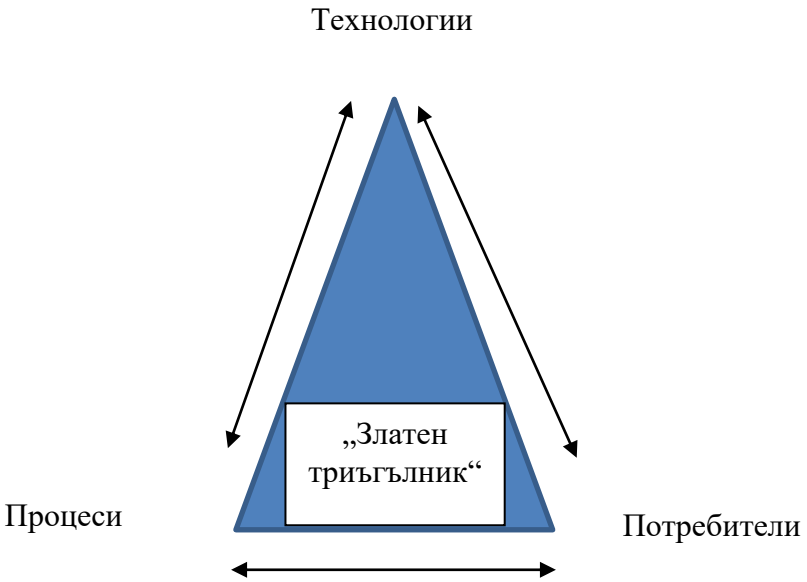


Фиг. 1. Многослоен, мултифакторен модел за балансиране на решенията по проблемите на киберсигурността

В общия случай, за постигането на киберсигурност са формулират, въвеждат и усъвършенстват съответни мерки (контроли). За да бъдат балансирани, тези мерки следва да покриват две направления:

- трите компонента (върха) в т.нар. „златен триъгълник “ на киберсигурността, които са технологии, процеси и потребители;[1]
- трите области от схемата на т.нар. „защита в дълбочина“, т.е. мерките следва да покриват административната, техническата и физическата област на киберсигурността;[2]

Едни от първите определения за киберпространството, включително по отношение на аспекта за сигурността на това пространство, включват в своето съдържание само свързани в мрежи технически (компютърни) системи. На по-късен етап към това разбиране за киберпространството се допълва разбирането за мястото и ролята на процесите, които протичат в неговите рамки, както за мястото и ролята на потребителите на услуги в киберпространството и на отношенията, в които тези потребители влизат в обхвата на киберпространството. Разширяването на обхвата на киберпространството и на аспектите за неговата сигурност въвеждат необходимостта от търсене на баланс между мерките за сигурност, отнасящи се до трите компонента на т.нар. „златен триъгълник“, разглеждани като източници на сигурност, респ. източници на несигурност (виж фиг. 2)..

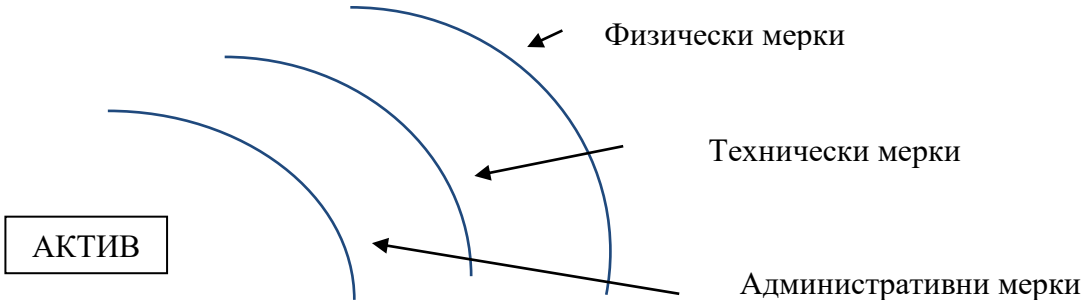


Фиг. 2. Графичен модел на т.нар. „златен триъгълник “ на киберсигурността

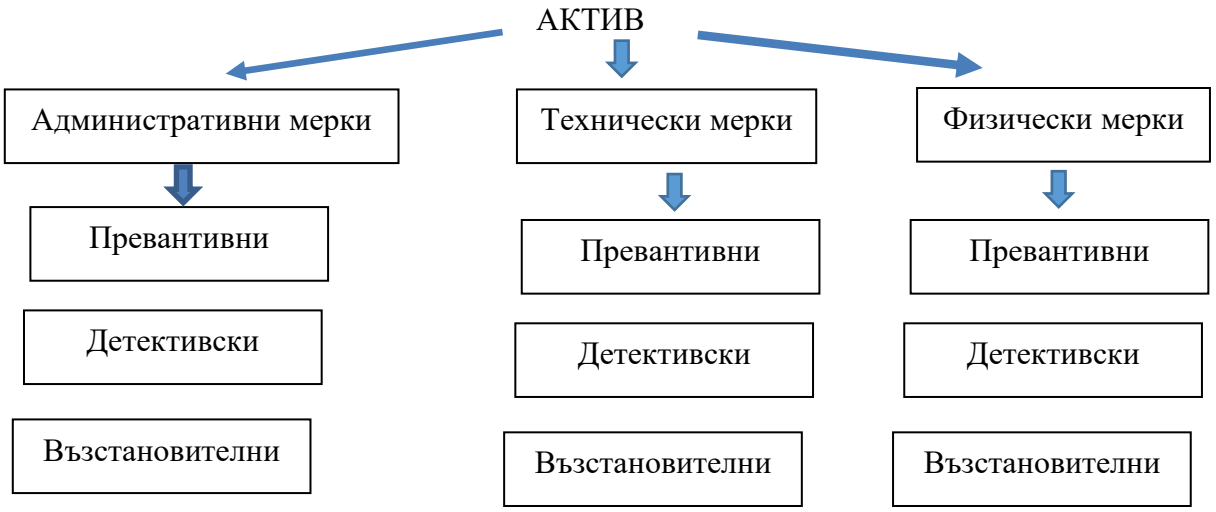
Защитата в дълбочина е друга теоретична концепция от този първи слой на многофакторния модел, която изправя предизвикателства при намирането на баланс между административните, техническите и физическите контроли за киберсигурност (виж фиг. 3). Административните мерки за защита на сигурността на информационните активи имат за цел да поставят основите за изграждане и поддържане на сигурно киберпространство. Те включват, но не се изчерпват с принципи, политики, стандарти, указания, регулации, оперативни процедури. Липсата на административни мерки за киберсигурност може да се представи като започване на стоежа на една сграда от първия етаж, без да бъдат изградени основите на тази сграда. Специфичният характер на заплахите, уязвимости, активите и атаките срещу киберсигурността без съмнение правят необходимо създаването и

[1] Mike Chapple, *Certified Information Systems Security Professional* (ISC, 2018).
[2] Пак там

прилагането на технически мерки за сигурност (наричани от някои автори логически мерки за сигурност).



Фиг. 3. Графичен модел на т.нар. схема „защита в дълбочина“



Фиг. 4. Място и роля на превантивните, детективските и възстановителните мерки за киберсигурност

В същото време, без съмнение е тезата, че без достатъчно сигурна физическа среда всички административни и технически мерки могат да загубят своята ефективност. Този факт аргументира мястото и ролята на физическите мерки за сигурност в киберпространството. Погледнато от гледната точка на правения анализ може да се каже, че нито административните, нито техническите, нито физическите мерки сами по себе си могат да постигнат желано ниво на сигурност. Търсената ефективност на решенията за киберсигурност е пряко свързана с постигането на баланс между трите типа мерки за сигурност.

Следващият слой на модела, показан на фиг. 1, е продължение на концепцията за балансиране на мерките за киберсигурност, но погледната от друг ъгъл. Този слой включва превантивни, детективски и възстановителни мерки за киберсигурност[3], които се явяват

[3] Венелин Георгиев, *Основи на киберсигурността* (София: Авангард, 2019).

компоненти на разгледаните по-горе административни, технически и физически мерки за киберсигурност (виж фиг. 4).

Различията между тези три вида мерки за сигурност са разбираеми на базата на техните наименования: превантивните мерки за киберсигурност имат за цел да предотвратят възникването на киберинцидент, детективските мерки за киберсигурност целят разкриване възникването на подобен инцидент, възстановителните мерки за киберсигурност имат за цел да подпомогнат преодоляването на последствията от киберинцидента и възстановяване на нормалната работа на системите и мрежите. Независимо от различията в същността и предназначението на тези три групи мерки, желаното ниво на киберсигурност се постигна за сметка на тяхното балансиране.

Третият слой на модела, показан на фиг. 1, включва необходимото за прилагане в практиката на посочените в предходните два слоя мерки за киберсигурност. Става въпрос за способностите за киберсигурност, разбирани като съвкупност от ресурси, които позволяват изпълнението на определени задачи, в определена среда, по пределен начин, в отговор на заплахите за киберсигурността. Концепцията за сценарийно планиране за способности за киберсигурност включва създаването и използването на контекстни и ситуационни пакети от сценарии, които освен че трябва да бъдат правдоподобни, следва да бъдат и балансирани[4]. Очевидна в случая е необходимостта от балансираност в две плоскости: първо, балансиране на различните видове необходими ресурси (човешки, материални, информационни, финансови и т.н.) и второ балансиране на тези ресурси със сценариите за тяхното използване. Нивото и зрелостта на способностите за изпълнение на мерките за киберсигурност следва да бъдат измервани и оценявани. За целта се изисква разработване и прилагане на система от метрики за киберсигурност и модел за оценяване на зрелостта на способностите за киберсигурност[5]. Взети поотделно и системата от метрики, и модела за оценяване на зрелостта на способности изискват наличие на вътрешно балансиране.

В следващият, четвъртия слой на анализирания модел, показан на фиг. 1, споменатите по-горе способности за киберсигурност следва да бъдат балансирани с риска, оставащ след прилагане на мерките за сигурност и с финансовата осигуреност за изграждане, поддържане и развитие на способностите за киберсигурност. За да бъде анализиран и постиган този баланс е необходимо:

- да бъде зададен апетита към риска за киберсигурността, определящ се с вида и количеството риск за сигурността на системите и мрежите, който може да бъде поет, без това да застраши постигане на целите на организацията;
- да бъдат разработени бюджетни сценарии, които в общия случай са три: песимистичен, оптимистичен и най-вероятен.

Отново се явява необходимост от вътрешно балансиране както на апетита към риска от влияещите фактори, така и на бюджетните сценарии.

Петият слой на модела за балансиране на решенията в областта на киберсигурността, показан на фиг. 1, трябва да разпредели способностите в две области, а именно киберсигурност и киберустойчивост[6]. Разделителната линия между тези две области може да бъде очертана когато се проследява жизнения цикъл на един инцидент с киберсигурността. Киберсигурността фокусира своето внимание върху превенцията, докато киберустойчивостта

---

[4] Д. Димитров, *Приложение на сценарийното планиране в бизнес, отбраната и сигурността* (София: Издателство на УНСС, 2012).

[5] Венелин Георгиев и Веселин Монев, *Метрики за киберсигурност* (София: Авангард, 2016.

[6] Венелин Георгиев, *Киберустойчивост* (София: Авангард, 2021).

поставя във фокуса способността на организацията да запазва работоспособно състояние в смутена среда, т.е. при възникване на инцидент със сигурността на системите и мрежите (виж фиг. 5). Казано по друг начин, разликата между киберсигурността и киберустойчивостта става видима в отношението „не ако, а когато“, касаещо възникването на киберинцидент. Независимо от видимите различия между зоните на интерес пред киберсигурността и киберустойчивостта, двата компонента взети заедно изграждат сигурното киберпространство, поради което следва да бъдат балансирани.

Изкачвайки се нагоре по слоевете на модела, показан на фиг. 1, се достига до необходимостта от балансиране на активното и адаптивното управление на киберсигурността[7]. Разликата между двата модела за управление идва от разликата в теоретичните концепции, които ги обслужват. При активното управление такава концепция е управлението на риска, докато при адаптивното управление обслужващата теоретична концепция е управлението при кризи. В чисто теоретичен план между посочените две концепции съществуват както сходства, така и различия, но в конкретния случай по-важна е необходимостта от балансиране на възможностите на организацията изпреварващо да се противопоставя на заплахите, т.е. да прилага активна управление, а също така да реагира по подходящ начин на възможни кибератаки, т.е. да прилага адаптивно управление.

Фиг. 5. Зависимост между киберсигурността и киберустойчивостта

Последният слой на модела, показан на фиг. 1, излиза извън рамката на киберсигурността, но показва връзката между този специфичен вид сигурност и общото предназначение на организацията[8]. Дейността на всяка организация е насочена към постигане на поставени цели по пътя на реализиране на съответните бизнес процеси, голяма част от които са компютъризирани и в основата на които стои персонала, за който трябва да бъде създадена удобна работна среда. От друга страна дейността на организацията се повлиява и трябва да бъде съобразена с редица регулации на международно, национално, отраслово и местно ниво. Едно от изискванията, поставяни в тези регулации касае мерките за запазване на личното пространство на потребителите и гарантиране на неговата сигурност. В крайна сметка, постигането на целите на организацията, което на практика определя крайното състояние на всички предходни усилия, изисква балансиране на сигурността на личното пространство, удобството при работа и действащите регулации.

Направеният по-горе анализ на модела, показан на фиг. 1, доказва тезата, че постигането на сигурност и в частност на киберсигурност изисква намирането на баланс в една сложна, комплексна, многослойна и многофакторна среда. На пръв поглед доказването

---

[7] Joseph Hallett, “The Cybersecurity Body of Knowledge,” The National Cyber Security Centre, 2019.

[8] Chris Moschovitis, *Cybersecurity Program Development for Business: The Essential Planning Guide* (Willey, 2018).

на тезата дава основание да се направи извода, че балансът може да бъде разглеждан като панацея за постигане на сигурност.

Направеният извод повдига нов въпрос: защо е толкова трудно да се създава сигурност след като се приема, че балансът е търсената панацея. Възможни са редица отговори, които покриват областите на недостатъчен аналитичен потенциал за решаване на оптимизационни задачи, недостатъчно ефективна информационно-аналитична дейност, липса на взаимодействие между всички заинтересовани групи лица, недостатъчен размер на разполагаемите ресурси и т.н.

ЗАКЛЮЧЕНИЕ

Направените по-горе разсъждения разкриват несъстоятелността на тезата, че е възможно намиране на единствено решение на въпроси в сложна, комплексна и многофакторна среда. Опростяването на областта на сигурността и свеждането на решаването на свързаните проблеми до търсене на панацея е не само грешен подход, но само по себе си създава рискове за сигурността. Картината става още по-сложна когато се търсят отговори на зададените въпроси на всяко от петте равнища са сигурност, отношението към които само по себе си се нуждае от баланс

ИЗПОЛЗВАНА ЛИТЕРАТУРА

[1] Mike Chapple, Certified Information Systems Security Professional (ISC, 2018).

[2] Венелин Георгиев, Основи на киберсигурността (София: Авангард, 2019), ISBN 978-619-239-212-3.

[3] Д. Димитров, Приложение на сценарийното планиране в бизнес, отбраната и сигурността (София: Издателство на УНСС, 2012).

[4] Венелин Георгиев, Киберустойчивост (София: Авангард, 2021).

[5] Венелин Георгиев и Веселин Монев, Метрики за киберсигурност (София: Авангард, 2016), ISBN 978-619-160-683-2.

[6] Joseph Hallett, “The Cybersecurity Body of Knowledge,” The National Cyber Security Centre, 2019.

[7] Chris Moschovitis, Cybersecurity Program Development for Business: The Essential Planning Guide (Willey, 2018).