НОВ БЪЛГАРСКИ УНИВЕРСИТЕТ

ДЕПАРТАМЕНТ „НАЦИОНАЛНА И МЕЖДУНАРОДНА СИГУРНОСТ“

ДОКТОРСКА ПРОГРАМА „СТРАТЕГИИ И ПОЛИТИКИ НА СИГУРНОСТ“

ПОВИШАВАНЕ ЕФЕКТИВНОСТТА НА ПРОЦЕСА ЗА ИЗМЕРВАНЕ И ОЦЕНЯВАНЕ НА СПОСОБНОСТИТЕ ЗА КИБЕРСИГУРНОСТ НА ОРГАНИЗАЦИЯТА

АВТОРЕФЕРАТ

на дисертационен труд за придобиване на образователната и научна степен “доктор“ в област на висше образование: 9. Сигурност и отбрана, професионално направление: 9.1. Национална сигурност

Докторант: Димитър Красимиров Димитров

Научен ръководител: проф. д-р Венелин Георгиев

София, 2023г.

Дисертацията е обсъдена и допусната до защита на заседание на департамент „Национална и международна сигурност“, проведено на ……. 2024 г.

Дисертацията съдържа 146 страници, 15 фигури, 22 таблици, 2 приложения и библиография, включваща 63 заглавия.

Защитата на дисертацията ще се състои на ……. от …….. часа в зала …….. на корпус ……. на НБУ.

Материалите за защитата са на разположение на интересуващите се в офис 202 на втори корпус на НБУ, гр. София, ж.к. Овча купел, ул. Монтевидео № 21

Автор: Димитър Красимиров Димитров

Заглавие: Повишаване ефективността на процеса за измерване и оценяване на способностите за киберсигурност на организацията.

СЪДЪРЖАНИЕ

ОБЩА ХАРАКТЕРИСТИКА НА ДИСЕРТАЦИОННИЯ ТРУД....4

Актуалност, обект и предмет на изследването....4

Основни хипотези, цел и задачи....6

Методика и ограничения....7

Структура на дисертацията....8

СЪДЪРЖАНИЕ НА ДИСЕРТАЦИОННИЯ ТРУД....10

Първа глава. Теоретичен аспект на процеса за измерване и оценяване на способностите за киберсигурност на организацията....10

Втора глава. Сравнителен анализ на ефективността процеса за измерване и оценяване на киберсигурността на организацията....18

Трета глава. Моделиране на процеса за измерване и оценяване на способностите за киберсигурност на организациите с цел повишаване на неговата ефективност....23

ЗАКЛЮЧЕНИЕ И ОБЩИ ИЗВОДИ....28

ПРИНОСИ....31

СПИСЪК С ПУБЛИКАЦИИ ПО ТЕМАТА НА ДИСЕРТАЦИОННИЯ ТРУД ...32

ОБЩА ХАРАКТЕРИСТИКА НА ДИСЕРТАЦИОННИЯ ТРУД

Актуалност, обект и предмет на изследването

С навлизането на информационните технологии, мобилните устройства, компютърните мрежи и Интернет, както и постоянният приток на нови потребители на услугите и информацията в тях, киберпространството се превръща все повече в отражение на реалния свят. Никога преди човечеството не е било толкова обвързано помежду си, както през XXI век. Значителна част от хората са постоянно „онлайн“, а разнородни програми и приложения, уеб страници и социални мрежи предлагат на потребителите си виртуални изживявания, близки до тези от реалния свят - аналози на дейности, които ги свързват с близки и приятели, забавляват ги или ги подпомагат в работата.

Дигиталните продукти за повишаване на ефективността на работният процес отдавна са широко употребявани в бизнес средите. Продукти като Microsoft Word, Excel, PowerPoint, Visio, SPSS, AutoCAD и др. предоставят възможност за увеличаване на производителността, минимизиране на грешки, по-бързи изчисления, автоматична текстообработка и представяне на информацията в текстов, табличен и графичен вид.

С популяризирането на Интернет, електронните пощи, мигновените съобщения[1] и VoIP[2] разговорите изместват конвенционалните писма и телефония, като по-ефективен, по-удобен и по-нискобюджетен начин на комуникация. Заедно с това, бумът на социалните мрежи като Facebook, Twitter и Instagram, комуникацията с потребителите става още по-лична - бизнесът може да се представя и с човешко лице пред клиента.

[1] От Instant Messaging

[2] Voice over IP

Успоредно с това, не бива да се забравя, че киберпространството крие опасности. Бързата и безгранична връзка, носи със себе си рискове. Свързаността на отделните звена на киберпространството и достъпността до изграждащата го инфраструктура, носят заплахи както за конфиденциалността и целостта на информацията предавана по електронен път, така и за наличността на услугите, предлагани от бизнеса.

Милиардите долари загуби и постоянната промяна в подходите за атака на киберпрестъпниците правят проблемите, свързани с киберсигурността особено **актуални** за бизнеса. Бизнес организациите се принудени да подхождят проактивно в създаването на способности за защита, които да обхващат не само информационните и технологични звена на компаниите, но и на цялата си организационна структура.

За да се сдобият с **адекватни способности за киберсигурност**, организациите се нуждаят от **ефективен процес за тяхното избиране, изграждане и управление**. А, за да бъде този процес ефективен – от ефективен процес за измерване и оценяване на тези способности, който да предоставя възможност, както за избор на дейностите и практиките по осигуряване на сигурност, така и за измерване и оценяване на тяхното имплементиране в рамките на огранизацията. Настоящата дисертация разглежда тази взаимосвързана система.

Обект на изследването в дисертацията е **процесът за измерване и оценяване на способностите за киберсигурност** на организацията, а **предмет на изследването** е **ефективността на този процес**.

Основни хипотези, цел и задачи

Основната дисертационна теза е изградена от **две взаимносвързани хипотези:**

- посочените стратегически инструменти за измерване и оценяване на способностите за киберсигурност не изпълняват всички изисквания за осигуряване на ефективност на процеса и предпоставят възможност за пропуски при планирането и изграждането на киберсигурността в рамките на организацията;
- комбинирането им в нов модел би довело до повишаване на ефективността на процеса за измерване и оценка на способностите за киберсигурност в организацията, както и би подпомогнало процеса по планиране и изграждане на тези способности.

Целта на разработката е да се проведе изследване на ефективността на процеса за измерване и оценяване на способностите за киберсигурност на организацията и да се предложат възможности за нейното повишаване.

За постигането на целта в дисертацията последователно се решават следните **изследователски задачи**:

1. Изследване на теоретичния аспект на изграждането на способности за киберсигурност на организациите, като фокусът се поставя върху неговия процесен характер.
2. Създаване на концептуална основа за измерване на ефективността на процеса за оценяване и измерване на способностите за киберсигурност.
3. Извършване на сравнителен анализ на ефективността на процеса при управлението му чрез избраните стратегически инструменти за измерване и оценяване на способностите за киберсигурност на базата на определени критерии и очертаване на рамката на проблемен анализ за отстраняване на разкритите слаби страни.

4. Извършване на проблемен анализ за определяне на проблемните области за ефективността на процеса, управляван от избраните стратегически инструменти.
5. Създаване на концепция, изграждане и прилагане на модел за повишаване на ефективността на процеса измерване и оценяване на способностите за киберсигурност и на тази база формулиране на препоръки за усъвършенстване на процеса.

Методика и ограничения

За изпълнението на изследователската част се използват следните **изследователски подходи**: системен, процесен, исторически и моделен.

Чрез *системния подход* се анализират елементите и характеристиките на инструментите за измерване и оценка на киберсигурността в организациите в контекста на средата за тяхното прилагане.

Самият процес на измерване и оценяване на киберсигурността налага използването на *процесния подход* за неговото изследване.

Чрез *историческия подход* се проследява развитието, както на киберзаплахите в бизнеса, така и на развитието на инструментариума за планиране, изграждане и измерване на способностите за киберсигурност.

Чрез *моделния подход* се създават условия за изследване на процеса за измерване и оценяване на способностите за киберсигурност в условията на предварително определен сценарий.

Изследването на ефективността на инструментите за измерване и оценяване на киберсигурността се прави с помощта на следните **научно-изследователски методи**: теоретичен анализ, сравнителен анализ, синтез, научна абстракция, проблемен анализ, моделиране.

В рамките на настоящият дисертационен труд се поставят следните **ограничения и допускания**:

- Въпросите, свързани с киберсигурността в бизнес организациите са фирмена тайна.
- Целевият профил на киберсигурността на всяка бизнес организация е строго индивидуален.
- Фокусът на изследването е насочен към процеса за измерване и оценяване на способностите за киберсигурност в рамката на бизнес организациите, а не към конкретните мерки и способности за киберсигурност. Т.е., разглежда се процесът, така както е управляван от стратегическите инструменти за управление, които осигуряват възможност за оценка и контрол в рамките на цялата организационна структура и нейните звена. Изцяло технологичните инструменти, мерки и практики са извън фокусът на настоящото проучване.

Структура на дисертацията

В **съдържанието** на дисертацията са включени: въведение, три глави, общи изводи и препоръки, заключение, приложения, списък с таблици, списък с графики.

Въведението представя на читателя следните характеристики на изселдването: актуалност на темата, обект, предмет, цел и задачи на изследването, хипотези за изследване, методика, ограничения, приложимост на резултатите от разработката.

Първа глава поставя теоретичната постановка на проучването.

Изложена е кратка историческа справка за развитието на необходимостта за изграждане на киберсигурност в организациите и нейното изследване. Подробно е представен процеса за планиране и изграждане на способности за киберсигурност в рамките на организацията.

Предлага се дефиниция за *ефективен процес за измерване и оценяване на способностите за киберсигурност* и дефиницията се допълва от целева картина от фактори за ефективност на процеса. Определят се изискванията към инструментите за управление на процеса, за да могат да бъдат осигурена наличността на факторите за ефективност на процеса.

Главата разглежда същността на стратегическите инструменти за управление на процеса, в частност балансираната карта с показатели за измерване на киберсигурността и модела за измерване на равнището на способности за киберсигурност C2M2.

Във **втора глава** са преставени критериите и изискванията за извършване на сравнителните анализи на ефективността на процеса за измерване и оценяване на киберсигурността, управляван от избраните в Първа глава инструменти за измерване и оценка на киберсигурността. Описани са изследванията и анализите на избраните инструменти за управление на процеса за измерване и оценка на киберсигурнсотта чрез дефинираните критерии. Систематизирано са представени резултатите от тези изследвания.

Трета глава изследва възможността за повишаване на ефективността на процеса за измерване и оценяване на способностите за киберсигурността чрез предложение на комбиниран модел за планиране, измерване и изграждане на способности. Главата описва концептуалната основа, предпоставките за изграждане, както и самото изграждане на модела. Новопредложеният модел е подложен на аланогичен анализ, по пример на анализите, извършени във Втора глава.

Предложено е описание за имплементиране на предложения комбиниран модел в рамката с цел управление процеса за планиране и изграждане на способности за киберсигурност в организацията и повишаване на неговата ефективност.

СЪДЪРЖАНИЕ НА ДИСЕРТАЦИОННИЯ ТРУД

Първа глава. Теоретичен аспект на процеса за измерване и оценяване на способностите за киберсигурност на организацията

Първа глава е съставена от пет основни части и поставя теоретичната постановка на изследването.

Изложена е историческа справка за развитието на необходимостта за изграждане на киберсигурност в организациите и нейното изследване. Подробно е представен процеса за планиране и изграждане на способности за киберсигурност в рамките на организацията.

Предлага се дефиниция за *ефективен процес за измерване и оценяване на способностите за киберсигурност* и дефиницията се допълва от изисквания към инструментите за осигуряване ефективността на процеса.

Главата подробно разглежда същността на стратегическите инструменти за управление на процеса, в частност балансираната карта с показатели за измерване на киберсигурността и модела за измерване на равнището на способности за киберсигурност C2M2.

В първата част е представен историческият преглед на развитието на заплахите и изграждането на киберсигурността в организациите. Разгледани за данните и изводите от ежегодното проучване на Ponemon/Keeper [3, 4, 5, 6] за

[3] Keeper Security, Ponemon Institute (2017). The 2016 State of SMB Cybersecurity. Ponemon Institute SMB Cybersecurity Annual Report

4 Keeper Security, Ponemon Institute (2019). The 2018 State of SMB Cybersecurity. Ponemon Institute SMB Cybersecurity Annual Report.

5 Keeper Security, Ponemon Institute (2020). The 2019 SMB Cybersecurity Study. Ponemon Institute SMB Cybersecurity Annual Report.

6 Keeper Security, Ponemon Institute (2021). Cybersecurity in the Remote Work Era: A Global Risk Report. Ponemon Institute SMB Cybersecurity Annual Report.

периода 2016-2020 година с цел детайлен анализ на основните препятствия пред компаниите.

Въпросното проучване демострира следните тенденции:

- преобладаващата част от решенията за киберсигурността се взимат от висшето ръководство на организациите;
- при малка част от респондентите направленията на дейността на организацията определят приоритетите за киберсигурността;
- голям е процентът на отговорите „Нито една фукция не определя приоритетите за киберсигурността“.

Тези тенденции определят, че небрежността на служителите, липсата на ясни отговорни роли и приоритети за изграждането на киберсигурност, както и обвързаност на киберсигурността с основната дейност на организацията като *основните проблеми за ефективна отбрана срещу киберзаплахи за организациите*.

Във втората част на Първа глава е разгледано подробно изграждането на киберсигурността в организацията – компонентите на планирането и фазите на самия процес.

Основните компоненти на планирането са: процес, стратегия и инфраструктура[7]. Пълноценното оценяване на тези компоненти включва задълбочен анализ на стъпките на процеса за планиране на способностите за киберсигурност, които в обобщен вариант са следните:

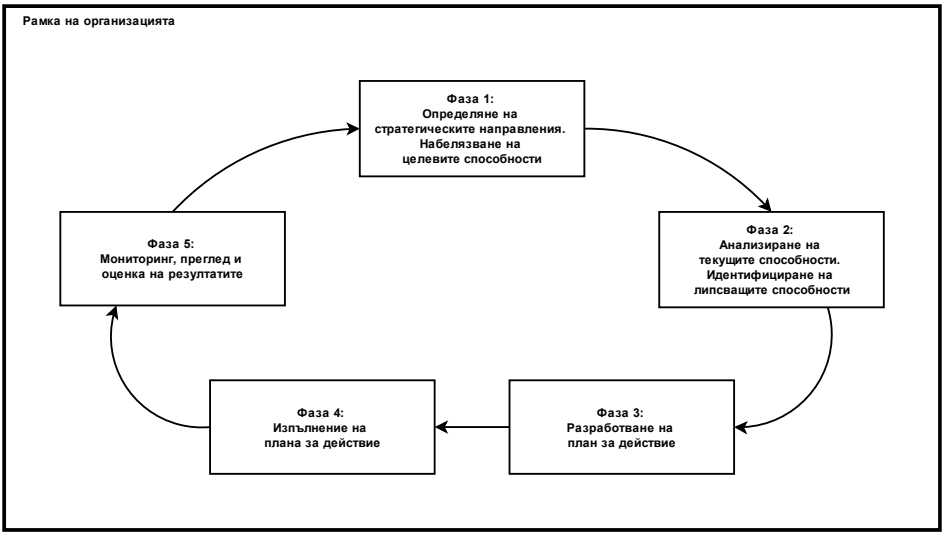
- Определяне на текущите способности за киберсигурност, описани с подходящи техни характеристики;

[7] Георгиев, В. (2015). „Планиране на способности за киберсигурност“. Сценарийно планиране на способности за киберсигурност. НБУ

- Анализ на целите и стратегията за развитие на организацията за определяне на изискванията за бъдещи способности за киберсигурност;
- Идентифициране на липсващите способности за киберсигурност и определяне на необходимите дейности за елиминиране на техните липси;
- Изготвяне на план за изграждане на дейностите в стъпки, изпълнението на които би довело до изграждането на необходимите способности за киберсигурност;

На базата на горепосочените стъпки се изработва методиката за планиране на способностите за киберсигурност на фирмата и се обобщава самия процес в следните фази:

- определяне на стратегичеките направления - извършва се анализ на стратегическия план на организацията и се идентифицират целите. Определят се целевите способности за киберсигурност;
- Анализ на текущите способности и идентифициране на липсващите способности за киберсигурност;
- Разработване на план за изграждането на липсващите способности. Избират се измерители за изпълнението на плана и постигане на целите на организацията;
- Изпълнение на плана за действие и оценяване на получените резултати с помощта на избраните измерители;
- Мониторинг, преглед и оценка на резултатите от изпълняването на плана;



Фигура 1. Фази на процеса за планиране и изграждане на способности за киберсигурност

Третата част на Първа глава дефинира условията за ефективност на процеса за измерване и оценяване на способностите за киберсигурност.

Аназилите и взимането на решения са основни фактори във всяка фаза на процеса. Отделните компоненти на планиране на процеса, както и техните елементи посочват киберсигурността като явление, обхващащо цялата организация. Паралелно с това, киберсигурността зависи и от външни фактори и от спецификата на самото киберпространство.

Ефективността на самият процес зависи от:

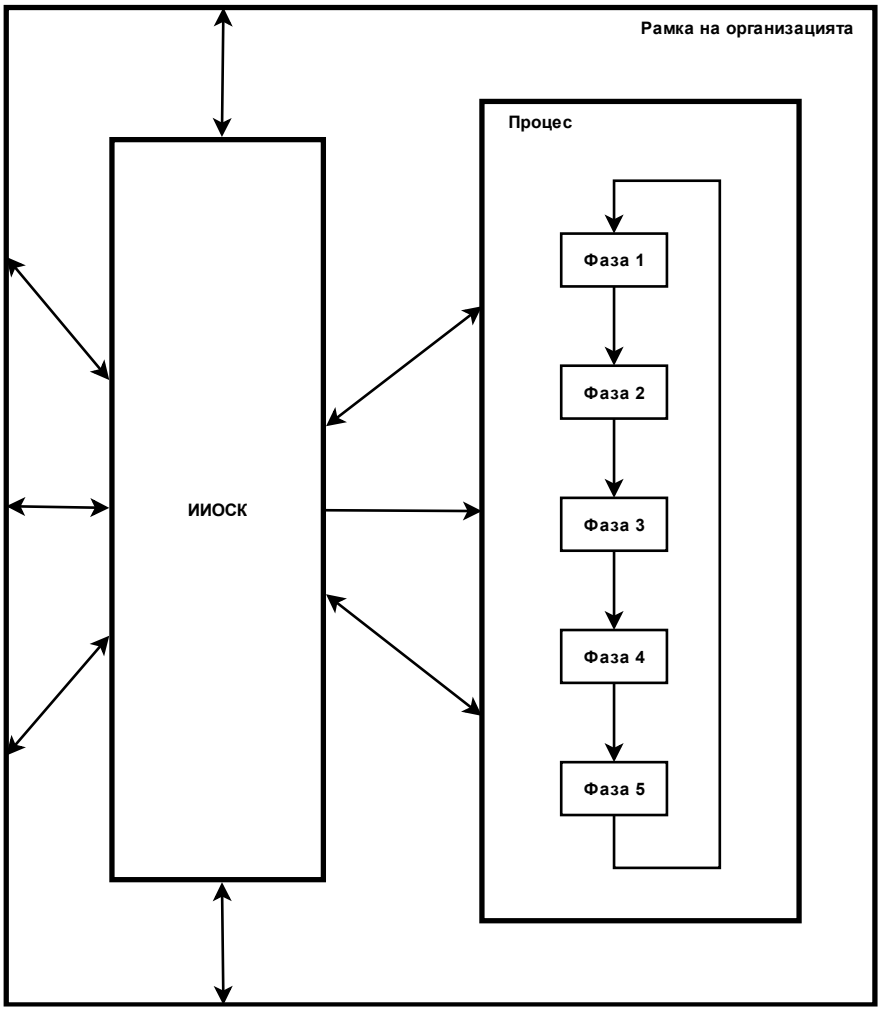
- възможността за правилно планиране на способностите, които ще се изграждат/надграждат;

- възможността за наблюдение на прогреса на процеса. Това изисква възможност за извличане на релевантни данни във всеки етап от процеса;
- възможност за представяне на извлечените данни и информация на релевантните групи, които трябва да анализират, оценят и вземат решение;

Следователно, тя е пряко зависима от инструментариума, който се използва за измерване и оценяване.

На базата на гореизложените условия се определят посоките, в които да се анализира даден инструмент, за да се определи ефективността, която осигурява за процеса в рамките на организацията:

- За да се осигури ефективен процес, инструментите трябва да обващат цялата организация – както вътрешната организация и функции, така и външните фактори, които определят контекста на нейната дейност. Това условие предопределя изборът на инструменти за управление на процеса с цел осигуряване на неговата ефективност.
- Необходимо е избраният инструмент да се изследва като междинна среда между субекта, който го използва за измерване (организацията и нейните заинтересовани нива) и обекта, който се измерва (процеса за планиране и изграждане на способности за киберсигурност). В този случай, за ефективния посредник (инструментът за оценка) трябва да има полезни двустранни взаимодействия и с двете системи, които свързва. По този начин могат да се изведат две основни гледни точки за ефективността на инструмента и да се направят изводи за всяка една от тях: *приспособимост към рамката* и *управление на процеса*.



Фигура 2. Инструмент за измерване и оценяване на способностите за киберсигурност (ИИОСК) като медиум между организационната рамка и процеса за планиране и изграждане на способности за киберсигурност на организацията

Четвъртата част на Първа глава представлява подробен преглед на структурата и приложението на балансираната карта с показатели за оценка на киберсигурността.

Целта на метриките, заложени в балансираната карта е да предоставят информация за аспектите на фирмената дейност, които са свързани с вътрешната организация, нивото на способности на персонала и отношенията с външни за компанията субекти.

За да се балансират показателите в картата, Каплан и Нортън[8,9] предлагат разпределение в четири групи, известни като гледни точки (перспективи или аспекти), като по този начин се създава достатъчно точна и пълна картина на дейностите в рамките на организацията. Въпросните четири аспекта са:

- *финансов* - в тази група влизат традиционните икономически показатели;
- *потребители* - тук попадат измерватели за ефективността при работа с клиенти;
- *вътрешни процеси* - групата съдържа метрики за ефективността на вътрешната организация;
- *обучение/развитие* - тук спадат мерките за степента на осигуряване на персонала със знания;

За пълнота, всеки от индикаторите в балансираната карта трябва да се опише със следните характеристики:

- цел - тясно свързана с рамката на организацията;
- показател, с който се измерва нивото на изпълнение на целта;
- целева стойност;
- измервана дейност;

[8] Kaplan, Robert S; Norton, D. P. (1996). "The Balanced Scorecard – Measures That Drive Performance". Harvard Business Review (January–February): 71–79.

[9] Kaplan, Robert S; Norton, D. P. (1996). The Balanced Scorecard: Translating Strategy into Action. Boston, MA.: Harvard Business School Press. ISBN 978-0-87584-651-4

По този начин се създава рамка, подпомагаща организациите в разпределянето по удобен и балансиран начин на показателите за измерване на ефективността на своята дейност. В тази рамка, те са свободни да избират конкретните метрики, които най-добре описват тяхната дейност. Също така, при необходимост, може да бъде добавен допълнителен аспект или да бъде пропуснат някой от предложените. Критична част от изборът на измерватели е метриките и гледните точки да бъдат в контекста на *фирмените визия, мисия, ценности и стратегия*.

В петата част на Първа глава са описани същността и приложението на модела C2M2.

Моделът е организиран в десет области (домейни). Те представляват логически свързани групи от практики за киберсигурност. От своя страна, практиките са групирани по цели, които компанията се опитва да достигне. В съдържанието на всяка област практиките са подредени по нива на зрялост [10].

За всяка от областите моделът дефинира четири нива на зрялост, които се прилагат независимо от останалите области. Нивата определят двойствена прогресия към зрелостта - прогресия на подхода и прогресия на институционализацията.

Прогресът на подхода се описва от целите и практиките за киберсигурност, описани в съответната област на модела.

Институционализацията описва до каква степен дадена практика, или дейност е ***интегрирана*** в организационните операции.

Възможността за измерване на промените между нивата позволява на организацията да използва скалата за да:

[10] U.S. Department of Energy и U.S. Departament of Homeland Security (2014). “Cybersecurity Capability Maturity Model Version 1.1”

- определи настоящото си ниво на зрялост;
- набележи бъдещо, по-високо ниво на зрялост;
- определи способностите, които трябва да придобие/развие (целеви и липсващи), за да достигне желаното ниво на зрялост.

C2M2 е разработен на базата на стандарти, рамки, програми и инициативи в областта на киберсигурността. Всяка област на модела съдържа структуриран инструментариум от практики, съдържащи дейностите, които организацията трябва да изпълни за да достигне следващото ниво за тази област.

Направеният исторически и документален разбор поставя теоретичната постановка за изследването и решава поставената във Въведението *първа изследователска задача*.

Втора глава. Сравнителен анализ на ефективността процеса за измерване и оценяване на киберсигурността на организацията

Втора глава е разделена на три основни части.

В нея са преставени критериите и изискванията за извършване на сравнителните анализи на ефективността на процеса за измерване и оценяване на киберсигурността, управляван от избраните в Първа глава инструменти за измерване и оценка на киберсигурността.

Описани са изследванията и анализите на избраните инструменти за управление на процеса за измерване и оценка на киберсигурнсотта чрез дефинираните критерии. Систематизирани и представени са и резултатите от тези изследвания.

В първата част на Втора глава за избрани критериите за последващите сравнителни анализи на базата на условията за ефективност, изведени в Първа

глава. Съставени са карти с критерии за оценяване на осигуряването на ефективност от страна на разглежданите инструменти за двете гледни точки.

Категория	Приспособимост към:
Бизнес рамка	визия
	мисия
	ценности
	стратегия
Вътрешна рамка	цели
	организационна структура
	вътрешни политики
Холистичен модел	вътрешни процеси
	персонал
	технологии
Външна рамка	външните политики
	външните процеси
	въздействието на външната среда

Таблица 1. Карта с критерии за приспособимост към рамката

Фази на процеса	Подпомага / Предопределя
Фаза 1	създаването на целево ниво на киберсигурност
Фаза 2	измерването на текущото ниво на киберсигурност
	определянето на липсващите способности за киберсигурност
Фаза 3	избора на стандарти, процедури и практики за изграждане на киберсигурност
Фаза 4	ефективното наблюдение над изпълнението на плана
	интегрирането на избраните стандарти, практики и процедури в общата организационна структура и дейност
Фаза 5	оценяването на резултатите от изпълнението на плана
	визуализацията и анализа на данните
	взимането на информирани решения
	итерацията на процеса

Таблица 2. Карта с критерии за управление на процеса за планиране и изграждане на способностите за киберсигурност

С цел по-лесното представяне на резултатите от изследването е предложен „коефициент за осигуряване на ефективност на процеса“, който се изчислява по следната формула:

$$E = \frac{\sum_{i=1}^{n} pr_i}{\sum_{i=1}^{n} pt_i} \quad (1)$$

където:

- **E** е коефициент на осигуряване на ефективност
- **n** е броят на критериите
- **pr** е реален точков резултат за покритие на критерия
- **pt** е целеви точков резултат за покритие на критерия

За целта се използва 5-степенна скала за покритието на всеки от критериите в картите.

Концептуализирането на измерването на ефективността на процеса, представено в тази част разрешава *втората изследователска задача*.

Във втората част на Втора глава са представени резултатите от сравнителните анализи между целевите карти (тези с максимален резултат за всички критерии) и покритието на избраните критерии от страна на двата инструмента.

Категория	Приспособимост към:	Целеви резултат	Резултат БК	Резултат C2M2
Бизнес рамка	визия	++	++	-
	мисия	++	++	-
	ценности	++	++	-
	стратегия	++	++	-
Вътрешна рамка	цели	++	++	-
	организационна структура	++	+	+
	вътрешни политики	++	+	-
Холистичен модел	вътрешни процеси	++	+	-
	персонал	++	+	-
	технологии	++	+	+
Външна рамка	външните политики	++	+	-
	външните процеси	++	+	-
	въздействието на външната среда	++	+	-

Таблица 3. Обобщен сравнителен анализ на покритието на критериите за приспособимост към рамката на БК и C2M2

Фази на процеса	Подпомага / Предопределя	Целеви резултат	Резултат БК	Резултат C2M2
Фаза 1	създаването на целево ниво на киберсигурност	++	-	+
Фаза 2	измерването на текущото ниво на киберсигурност	++	-	+
	определянето на липсващите способности за киберсигурност	++	-	+
Фаза 3	избора на стандарти, процедури и практики за изграждане на киберсигурност	++	-	+
Фаза 4	наблюдение над изпълнението на плана	++	?	++
	интегрирането на избраните стандарти, практики и процедури в общата организационна структура и дейност	++	-	++
Фаза 5	оценяването на резултатите от изпълнението на плана	++	?	++
	визуализацията и анализа на данните	++	+	++
	взимането на информирани решения	++	+	++
	итерацията на процеса	++	+	++

Таблица 4. Обобщен сравнителен анализ на покритието на критериите за управление на процеса за БК и C2M2

Изчислени са коефициентите за осигуряване на ефективност:

- $E(ПР^{11})_{БК} \approx 0.88$ и $E(УП^{12})_{БК} = 0.56$
- $E(ПР)_{C2M2} \approx 0.46$ и $E(УП)_{C2M2} = 0.92$

Резултатите от тези анализи и голямата разлика между изчислелите коефициенти и целевия коефициент ($E_Ц = 1$) демонстрират слабости в инструментите и възможност за въвеждане на слабости и неефективност на процеса. Тези слабости могат да се изследват допълнително чрез проблемен анализ.

Направените сравнителни анализи разрешават *третата изследователска задача*.

Третата част на Втора глава представя резултатите от гореспоменатия проблемен анализ. Чрез него се дефинират проблемните области на инструментите:

- за БК - формулирането, планирането и подпомагането на процеса;
- за модела C2M2 - приспособяването на инструмента към рамката на организацията.

Провеждането на проблемният анализ решава *четвъртата изследователска задача* и потвърждава *първата хипотеза на дисертацията*.

[11] ПР = Приспособимост към рамката
[12] УП = Управление на процеса

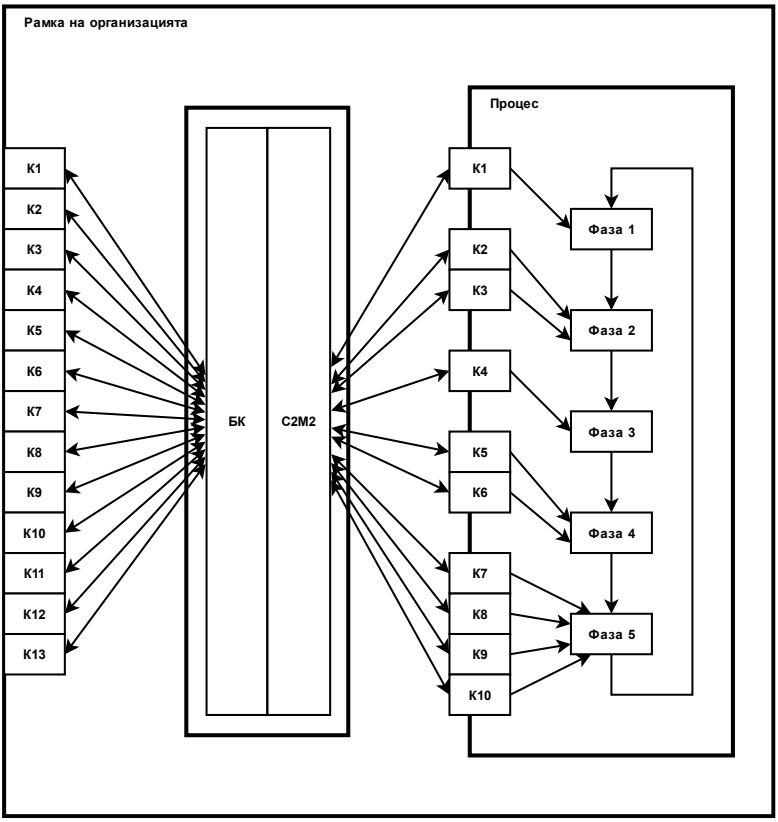
Трета глава. Моделиране на процеса за измерване и оценяване на способностите за киберсигурност на организациите с цел повишаване на неговата ефективност

Трета глава е съставена от три основни части.

Главата описва концептуалната основа, предпоставките за изграждане, както и самото изграждане на комбиниран модел за планиране, измерване и оценяване на способностите за киберсигурност. Описана е имплементацията на модела и е изследвано осигуряването на ефективност за процеса.

В първата част на Трета глава е поставена концептуалната основа на комбинирания модел.

На базата на проблемния анализ, проведен във Втора глава, може да се заключи, че балансираната карта и моделът C2M2 предполагат възможност за пропуски в правилното управление и оценяване на киберсигурността. При анализиране на резултатите се наблюдава възможност за припокриване на областите на единия инструмент с тези на другия с цел минимизиране на слабостите им и повишаване на ефективността на процеса. Желаният резултат е представен на фиг. 3.



Фигура 3. Схематично представяне на концептуалната основа на Комбинирания модел за измерване и оценка на способностите за киберсигурност

В основата на концептуалния модел е да се запазят силните страни на двата инструмента и да се минимизират слабостите им, като:

- елементите, заети от балансираната карта трябва да осигурят добра приспособимост към рамката и балансирано разпределение на планираните дейности

- елементите, заети от модела C2M2 трябва да осигурят инструментариума за планирането, изграждането, оценяването и институционализирането им.

Втората част на Трета глава описва декомпозицията на двата инструмента на съставните им елементи и синтезът на комбинираният модел.

Аспектите „Вътрешни процеси“ и „Потребители“ (от БК) изграждат оперативната област на комбинирания модел. Тя е насочена към измерване и оценяване на способностите за киберсигурност, свързани с основната дейност и функции на организацията.

Област „Тактически управление“ съдържа способности, които обслужват тактическото управление на киберсигурността. Тези способности са насочени към специалистите по киберсигурност.

Представените метрики в областта „Стратегически управление“ са насочени за стратегическо управление на организацията. Изгражда се от аспекти “Финансова гледна точка” и “Развитие/обучение” и в него не присъстват конкретни способности, а се описва цялостното развитие на програмата за изграждане на киберсигурност на организацията и нейното бюджетиране.

Представената концепция разрешава *петата изследователска задача*.

В третата част на Трета глава са изложени резултатите от сравнителните анализи и изчисленията на коефициентите за осигуряване на ефективност на инструмента.

Категория	Приспособимост към:	Целеви резултат	Резултат КМ
Бизнес рамка	визия	++	++
	мисия	++	++
	ценности	++	++
	стратегия	++	++
Вътрешна рамка	цели	++	++
	организационна структура	++	+
	вътрешни политики	++	+
Холистичен модел	вътрешни процеси	++	+
	персонал	++	+
	технологии	++	+
Външна рамка	външните политики	++	+
	външните процеси	++	+
	въздействието на външната среда	++	+

Таблица 5. Сравнителен анализ между целевите стойности на критериите за приспособимост и резултатите на комбинирания модел (КМ)

Фази на процеса	Подпомага / Предопределя	Целеви резултат	Резултат КМ
Фаза 1	създаването на целево ниво на киберсигурност	++	+
Фаза 2	измерването на текущото ниво на киберсигурност	++	+
	определянето на липсващите способности за киберсигурност	++	+
Фаза 3	избора на стандарти, процедури и практики за изграждане на киберсигурност	++	+
Фаза 4	наблюдение над изпълнението на плана	++	++
	интегрирането на избраните стандарти, практики и процедури в общата организационна структура и дейност	++	++
Фаза 5	оценяването на резултатите от изпълнението на плана	++	++
	визуализацията и анализа на данните	++	++
	взимането на информирани решения	++	++
	итерацията на процеса	++	++

Таблица 6. Сравнителен анализ между целевите стойности на критериите за управление на процеса и резултатите на комбинирания модел (КМ)

	Целево ниво	БК	C2M2	КМ
Е(ПР)	1	0.88	0.46	0.88
Е(УП)	1	0.56	0.92	0.92
Е	1	0.74	0.66	0.9

Таблица 7. Коефициенти на осигуряване на ефективност на процеса на БК, C2M2 и КМ

Обобщено, разултатите демонстрират повишена обща ефективност на процеса за измерване и оценяване на способностите за киберсигурност при използването на комбинираният модел за неговото управление, както за приспособяване към рамката на организацията, така и при управлението на процеса за планиране и изграждане на киберсигурността и потвърждават хипотеза 2.

ЗАКЛЮЧЕНИЕ И ОБЩИ ИЗВОДИ

Обектът на изследването в настоящата дисертация **е процесът за измерване и оценяване на способностите за киберсигурност в организацията**, като трудът се фокусира върху неговата **ефективност**. В течението на прегледа на документите и резултатите от вече проведените проучвания се установяват наличието на слабости в осигуряването на адекватна киберсигурност в организациите и значимостта на човешкият фактор за това. Тези изводи, заедно с новостта на тази специфична сфера на сигурността доказват **актуалността на темата на дисертацията**.

Резултатите от направения исторически преглед на развитието на киберсигурността в организациите доказва необходимостта от **ефективен процес за планирането и изграждането ѝ** и нуждата от подпомагащ **ефективен процес за нейното измерване и оценяване.** Този процес се управлява от т.н. инструменти за измерване и оценка, като последвалото изследване на данните от проучванията и документите сочат, че тези инструменти трябва да са стратегически по мащаб, т.е. да включват в управлението на процеса цялата структура на организацията.

Разглеждането на теоретичният аспект и разглеждането на процесният характер на изграждането на киберсигурността в рамките на организацията осигурява необходимата теоретична постановка на изследването и разрешава първата изследователска задача, поставена във Въведението.

На базата на тази теоретична постановка се дефинират условията „ефективен процес за измерване и оценяване на способностите за киберсигурност в организацията“ и се концептуализира основата за нейното измерване. Изграждат се целеви карти с критериим които трябва да се покрият за осигуряване на ефективност. Дефинира се и коефициент за осигуряване на ефективност. По този начин се разрешава втората изследователска задача. Също така,

теоретичната постановка обосновава избора на инструментите за изследване – балансираната карта с показатели за измерване на киберсигурността и модела C2M2.

По методът на сравнителния анализ са изведени възможни слабости на инструментите, които могат да са предпоставка за ниска ефективност на процеса. Това се демострира и посредством изчислението на коефициента на осигуряване на ефективност за всеки инструмент. Тази стъпка решава третата изследователска задача и се потвърждава първата хипотеза.

Изведените предпоставки за ниска ефективност са допълнително разгледани чрез проблемен анализ и са дефинирани конкретните проблемни области за инструментите. Чрез това е разрешена и четвъртата изследователска задача.

Чрез изпълнението на тези задачи се постига първата част от целта на дисертацията - изследването на ефективността на процеса за измерване и оценяване на способностите за киберсигурност на организацията.

Петата изследователска задача се разрешава като се предлага предложение за повишаване на ефективността на процеса за измерване и оценяване на способностите за киберсигурност в организацията под формата на концепция за комбиниран модел за планиране, измерване и оценяване на киберсигурността. Посредством анализ и последващ синтез на елементите на балансираната карта и модела C2M2 е предложен начин за минимизиране на техните слабости. Разгледано е имплементирането на новия модел за управление на всяка от фазите на процеса за планиране и изграждане на киберсигурността. Последващият сравнителен анализ и изчислението на коефициента за осигуряване на ефективност демострират повишена ефективност на процеса, управляван чрез новия модел.

С разрешаването на петата изследователска задача се потвърждава втората хипотеза и се постига окончателно целта на изследването.

Чрез предложения комбиниран модел се предоставя възможност на организациите от всеки мащаб, най-вече на тези от малкия и среден бизнес да изградят ефективна и адекватна киберзащита, базирана на добри практики и процедури и съобразена с тяхната рамка и дейност.

ПРИНОСИ

Научно-приложните приноси допринасят за развитие на знанията в областта на тематиката на дисертацията и се формулират по следния начин:

- дефиниране на необходимите условия за „ефективен процес за измерване и оценка на киберсигурността в организацията“;
- създаване на концептуална основа за измерване на ефективността на процеса за оценяване и измерване на способностите за киберсигурност;
- моделиране на комбиниран инструмент за планиране, измерване и оценяване на способностите за киберсигурност в организацията.

Приложните приноси имат пряко отношение към внедряване на разработения модел в практиката и се формулират по следния начин:

- разработване на система от критерии за осигуряване на ефективност на процеса за измерване и оценяване на киберсигурността, насочена към инструментите за управление на този процес;
- синтезиране на комбинирания модел за планиране, измерване и оценяване на способностите за киберсигурност в организацията;
- описание на имплементацията на комбинирания модел за управление на процеса на измерване и оценяване на киберсигуността в организацията.

СПИСЪК С ПУБЛИКАЦИИ ПО ТЕМАТА НА ДИСЕРТАЦИОННИЯ ТРУД

1. Димитров, Д. (2020). Дистопия в утопията. Киберзаплахите за "умния град", Националната сигурност и Европейският съюз: младежки дискусионен форум по сигурност „Актуални проблеми на градската сигурност в държавите-членки на ЕС“, 29 ноември 2019 г., Студентски уебинар по сигурност „Национална сигурност и Европейският съюз“, 12 юни 2020 г.: сборник доклади, Авангард Прима, София, стр. 7-12, ISBN 978-619-239-520-9

2. Димитров, Д. (2020). Социалното инженерство - основна заплаха за бизнеса. Препоръчани мерки за защита, Сборник научни трудове международна научна конференция „Широката сигурност”, том 2, Департамент „Национална и международна сигурност“, НБУ, София, 2020, стр. 570-572, ISBN 978-619-7383-19-5

3. Димитров, Д. (2020). Киберсигурност в бизнеса: човешкият фактор, Сборник научни трудове международна научна конференция „Широката сигурност”, том 2, Департамент „Национална и международна сигурност“, НБУ, София, 2020, стр. 392-398, ISBN 978-619-7383-19-5