ВОЕННА АКАДЕМИЯ „ГЕОРГИ СТОЙКОВ РАКОВСКИ“

ФАКУЛТЕТ: НАЦИОНАЛНА СИГУРНОСТ И ОТБРАНА

КАТЕДРА: НАЦИОНАЛНА И МЕЖДУНАРОДНА СИГУРНОСТ

МИРОСЛАВА ОГНЯНОВА МЛАДЕНОВА

ИНТЕЛИГЕНТНИ РЕШЕНИЯ ЗА УПРАВЛЕНИЕ НА РИСКА В КОРПОРАТИВНАТА СИГУРНОСТ

АВТОРЕФЕРАТ

на дисертационен труд

за придобиване на образователна и научна степен „доктор“

област на висшето образование 9. „Сигурност и отбрана“

професионално направление 9.1. „Национална сигурност“

докторска програма „Военнополитически проблеми на сигурността“

Научен ръководител:

доц. д-р Илина Стефанова Козарова-Арменчева

София, 2024 г.

Дисертационният труд се състои от 228 стандартни страници, в т.ч.:

- Основен текст – 190 стр.;
- Научни приноси, научно-приложни приноси и публикации, свързани с дисертационния труд – 2 стр.;
- Бележки и библиография – 22 стр.;
- 3 приложения – 13 стр.;
- Основният текст съдържа 4 фигури и 1 таблица.
- Списъкът на цитираната и използвана литература включва 178 заглавия, от които 76 са на български език и 102 – на английски език.
- Изложеното е систематизирано в увод, три глави, общи изводи и препоръки, заключение.
- Заглавие: „Интелигентни решения за управление на риска в корпоративната сигурност".
- Автор: Мирослава Огнянова Младенова
- Тираж: 10 бр.
- Излиза от печат на __.__.2024 г.
- Военно издателство „Г. С. Раковски"

Докторантът е зачислен в докторантура чрез самостоятелна подготовка в катедра „Национална и международна сигурност" при факултет „Национална сигурност и отбрана" на Военна академия „Г. С. Раковски" и е отчислен с право на защита със заповед № СИ29-РД03-218/06.11.2023 г. на Началника на Военна академия „Г. С. Раковски", считано от 06.11.2023 г.

Дисертационният труд е обсъден и насочен за защита пред научно жури по докторска програма „Военнополитически проблеми на сигурността" на разширен катедрен съвет на катедра „Национална и международна сигурност"

при Факултет „Национална сигурност и отбрана“ на Военна академия „Г. С. Раковски“ на __.__.2024 г.

Докторантът работи в катедра „Национална и международна сигурност“ при Факултет „Национална сигурност и отбрана“ на Военна академия „Г. С. Раковски“, на длъжност „асистент“.

Материалите по защитата са на разположение на интересуващите се на сайта на Военна академия „Г. С. Раковски”.

Защитата на дисертацията ще се проведе на __.___.2024 г. от _____ ч. в зала ____ на Военна академия „Г. С. Раковски“, град София, на открито заседание на научно жури в състав:

1. доц. д-р Ирина Николаева Миндова-Дочева
2. доц. д-р Иван Петров Панчев
3. доц. д-р Пламен Николов Богданов
4. доц. д-р Константин Кирилов Казаков
5. проф. д-р Стефан Иванов Мичев

Резервни членове на научното жури:

1. проф. д-р Величка Иванова Милина
2. проф. д-р Евгени Петров Манев

СЪДЪРЖАНИЕ

I. ОБЩА ХАРАКТЕРИСТИКА НА ДИСЕРТАЦИОННИЯ ТРУД

1.1. Актуалност и значимост

В началото на XXI век, постигането на икономическото, информационно, технологично и политическо предимство е върховна цел. Правилата и международните норми се променят в ход, или се заобикалят от силните актьори. Частният интерес, в лицето на бизнеса, се превръща във фактор за влияние в международните процеси. Вложеният капитал от страна на корпорациите, на териториите на различни държави, ги поставя в двустранен модел на взаимодействие – те зависят от сигурността на държавите, в които извършват дейност и сигурността на тези държави се влияе от тях. В последните години, благодарение на ресурсите и информационното влияние, компаниите са важен фактор по множество социални и обществено значими проблеми. Наред с това, те спомагат за справяне с редица международни кризи, дефинирани като нетрадиционни[1].

Управлението на корпоративната сигурност е обект на научен интерес от академичната общност и от експерти от практиката. Същността на корпорациите, параметрите на тяхното функциониране и моделите на управление е изключително мултидисциплинарна тема, която се изследва от различни гледни точки. В българската литература тази сфера е застъпена от търговското право, като се отличават трудовете на О. Герджиков[2] и Т. Бузева[3]. От гледна точка на икономическите отношения, темата е разглеждана в трудовете на М. Стоименов[4], С. Савов[5], Т. Спасов и С. Статев[6], Н. Николова[7],

[1] Димов, Г., 2019. Кризисният мениджмънт между мира и войната. София: ВА „Г. С. Раковски“. ISBN 978-619-7478-40-2.
[2] Коментар на търговския закон. Книга Трета, 1998; Капиталови търговски дружества, 2011.
[3] Бузева, Т., 2006. Холдинг. София. Сиби. ISBN 9547303503.
[4] Стоименов, М., 1999. Финансиране на международната търговия. София. ISBN 9549050513.
[5] Савов, С., 1998. Икономикс. София. Тракия-М. ISBN 9549574202.
[6] Спасов, Т., Статев, С., 2008. Основи на икономическата теория. София. УНСС. ISBN 9789544949990.
[7] Николова, Н., 2016. Корпоративна икономика. Варна. ИК Стено. ISBN 978-954-449-860-3.

М. Нейчева[8], Н. Найденов[9]. Редица са и авторите, които изследват рамката на корпоративно управление с преобладаващ акцент върху конвенционалните рискове. Сред българските изследователи в областта на корпоративната сигурност и управлението на риска, се открояват имената и трудовете на Н. Слатински[10], Е. Василев[11], П. Иванов[12], Г. Сандев[13], Г. Торнев[14], Н. Крушков[15] и др. Изследванията в областта на процесите по управление на риска в компаниите са по-широко застъпени в чуждестранната литература и изследванията на М. Кабрич[16], М. Колиер[17], М. Марчети[18], Т. Мерна[19] и други. Сравнително по-малко се оказват теоретичните изследвания в областта на корпоративната сигурност, особено в частта, откроряваща значението на взаимодействието между националната и корпоративната сигурност. Определено липсват задълбочени изследвания в областта на т.нар. „нови рискове“ за корпоративната сигурност, които поради своя характер не биха могли да бъдат управлявани и предотвратявани с известните модели и инструменти.

[8]Нейчева, М., 2018. Икономика на многонационалната корпорация: предпоставки, практики, последици. Бургас. Флат. ISBN 978-619-7125-42-9.
[9]Найденов, Н., 2002. Корпоратизъм – нов тип социално-икономическа система: https://www.iki.bas.bg/Journals/EconomicThought/2002/2002-5/2.pdf. Посетен на: 20.11.2022.
[10] Слатински, Н., 2019. *Рискът – новото име на сигурността*. Изток-Запад. София. ISBN978-619-01-0526-8.
[11] Василев, Е., 2000. Фирмена сигурност: Нелоялна конкуренция и фирмен контрашпионаж. София. Труд. ISBN 954528188X.
[12] Иванов П. 2018. Усъвършенстване на корпоративната сигурност във финансова структура. Автореферат, УНСС. София.
[13] Сандев, Г., 2005. Стратегии за сигурност на фирмата. Шумен. УИ Епископ Константин Преславски. ISBN 954-577-310-3.
[14] Торнев, Г., 2020. Корпоративна сигурност. София. ВТУ Каблешков. ISBN 978-619-7472-12-7.
[15] Крушков, Н., 2020. Сигурност, креативност, лидерство. София. ИК-УНСС. ISBN - 978-619-232-303-5.
[16] Cabric, M., 2015. Corporate Security Management Challenges, Risks, and Strategies. Butterworth-Heinemann. ISBN 9780128029350.
[17] Collier, P., M., 2009. Fundamentals of Risk Management for Accountants and Managers: Tools & Techniques. Oxford Butterworth-Heinemann. 1st edition. ISBN–13: 978-0-7506-8650-1.
[18] Marchetti, A., M. 2011. Enterprise Risk Management Best Practices-From Assessment to Ongoing Compliance. Wiley Corporate F&A.
[19] Merna, T., Al-Thani, F., 2008. Corporate risk management. John Wiley & Sons Ltd - 2nd edition. ISBN 978-0-470-51833-5.

Средата, в която компаниите трябва да функционират днес е сложна, с нарастваща неопределеност, непредсказуемост на събитията и стратегически шокове от различен характер. Рискът, като основна характеристика на тази среда, е новата нормалност (Бек 2013). В подчинената на процесите на глобализацията действителност и промените на средата, понятието за сигурност се оказва в голяма степен обща, трайна и постоянно разширяваща се концепция (Димитров, А., Павлов, Г., Авторски колектив 2021, с. 25). Събитията, протичащи в рамките на националните държави днес, напускат техните граници и се ориентират към нова, наднационална представителност. Глобалните процеси формират нови среда за сигурност, фактори на влияние и инструменти за тяхното управление. В тази среда все по-актуален е въпросът за сигурността на компаниите и защитата на корпоративните активи. Изграждането на по-организирани и по-ефективни системи за управление на рисковете и противодействие на произлизащите от тях заплахи за сигурността на компаниите се превръща в основно предизвикателство. Това задава нов контекст и налага необходимостта от нова парадигма на корпоративната сигурност. Този нов контекст предполага актуализация на съществуващи стратегии, комбиниране и надграждане на инструментариума за управление на корпоративния риск, като се отчитат промените в националната и международната среда на сигурност.

Актуалността на темата произтича от осъзнатата необходимост от намирането и прилагането на по-ефективни решения при управление на рисковете за сигурността в организацията. Динамиката на средата в световен мащаб изисква по-задълбочен подход към заплахите на новото време и непредсказуемата среда, в която компаниите функционират. За да са в състояние компаниите да отговорят адекватно на заплахите се налага нуждата от имплементиране на иновативни, интелигентни решения за управление на риска в корпоративната сигурност, чиято цел е да бъде постигната устойчивост

чрез баланс на протичащите във вътрешната и външната среда процеси. Компаниите днес постоянно разширяват своя обхват и задълбочават влиянието си върху различни сфери на живота, като все по-нарастващо е значението им за състоянието на социално-икономическите, политическите, екологичните и други процеси в рамките на националните държави и на наднационално ниво. В този смисъл, тяхното влияние трябва да бъде отчитано от системите за международна и национална сигурност.

Значимостта на темата се обуславя от задълбочаващата се несигурност в глобален мащаб и крайната необходимост от навременна идентификация и управление на рисковете, произлизащи от динамиката на средата. Във време, в което състоянието на абсолютна „сигурност“ като цяло е недостижимо, корпорациите не могат да разчитат на традиционните средства за защита. Сега те се нуждаят от интелигентни решения, чрез които да управляват многообразието от рискове, при спазване на принципа за нормативно съответствие (compliance) и чрез прилагането на добри практики, имплементиране на автоматизирани решения в своите дейности и изпълнение на изискванията, дефинирани от национални и международни стандарти.

Изследването поставя акцент върху така наречените „интелигентни решения“ и тяхното приложение в процеса на управление на корпоративната сигурност. В последните години е широко наложена и затвърдена асоциацията на термина с развитието на технологиите и еволюцията на системите, базирани на изкуствен интелект. Заедно с това, следва да се отчете и фактът, че интелигентността е основна характеристика на човека, която бива дефинирана като биопсихологичен потенциал за обработване на информация (Авторски колектив 2021, с. 109, цит. по Гарднър) и нейното последващо използване в различни сфери на живота.

1.2. Обект, предмет и цел на изследването

Обект на изследването в дисертационния труд е корпоративната сигурност.

Предмет на изследването са възможните интелигентни решения за управление на рисковете за корпоративната сигурност, които да осигурят устойчива среда на функциониране чрез изграждане на способности за навременна адаптация към средата, имплементиране на съвременни управленски модели и прилагане на практики за корпоративна отговорност и ангажираност към заинтересованите страни на компанията.

Целта на дисертационния труд е да се формулира теоретичен модел на стратегия, който ще доведе до по-ефективно управление на рисковете за сигурността на корпорациите чрез проактивно изграждане на способности за навременна адаптация и функциониране в нарастващата неопределеност на средата.

1.3. Изследователски задачи

1. Да се изследва и анализира еволюцията на концепциите за корпорации, корпоративни структури и корпоративна сигурност, като се проследи развитието на моделите за управление в корпорациите и се идентифицират параметрите на корпоративната сигурност.

2. Да се идентифицират съвременните рискове за компаниите, като се изследва и анализира средата за сигурност и се дефинират нивата и възможните модели за управление на риска.

3. Да се изследват и анализират иновативни организационни подходи за управление на риска в компаниите и на базата на проведено проучване в различни по дейност корпоративни структури, да бъде формулиран теоретичен модел на стратегия за управление на риска в корпоративната сигурност.

1.4. Теза и работна хипотеза на дисертационния труд

Тезата на дисертационния труд е, че корпорациите, за да управляват ефективно рисковете за сигурността си и да постигат корпоративните си цели, трябва да прилагат нови, интелигентни решения за управление на рисковете, които отчитат интересите на всички заинтересовани страни и са в съответствие със законово установените правила и норми.

Работната хипотеза на дисертационния труд е, че ако компаниите прилагат нови, интелигентни решения за управление на рисковете чрез проактивно изграждане на способности за навременна адаптация, те могат да намалят своята уязвимост и да управляват по-ефективно рисковете за сигурността си.

1.5. Методология на изследването

Изследователските методи в работата са съобразени с формулираните задачи и спецификата на проблемите, които се изследват. В научното изследване са използвани следните традиционни методи за научно изследване:

- теоретичен анализ и синтез;
- системен анализ;
- метод на индукция и дедукция;
- събиране, обобщаване и анализиране на общодостъпна информация;
- проучване на информационни източници от хартиен носител и електронни;
- емпирично изследване и обработване на статистически данни.

1.6. Ограничения на изследването

1. Фокусът на изследване е поставен върху транснационалните корпорации (ТНК) и отъждествявани с тях икономически субекти.

2. Не са разглеждани банкови и финансови институции, поради спецификата на тяхната регламентация и дейност.

3. Терминът „корпоративна сигурност“ се отъждествява с понятието „организационна сигурност“, а понятията „организация“, „компания“ и „корпорация“ се използват като взаимнозаменяеми, за да бъдат избегнати тавтологии. Понятието „фирма“ е неприложимо съгласно разпоредбите на Търговския закон. Използвано е само, за да бъде проследена еволюцията на понятието „корпоративна сигурност“.

4. Решения за управление на риска, базирани на изкуствен интелект, не са детайлно представени поради направеното по-горе уточнение, че – за целите на настоящия дисертационен труд, под „интелигентни решения“ ще се разбират онези решения, които са резултат от вродените и развити способности, присъщи за човешкия индивид, в комбинация с постиженията на научно-техническия прогрес.

1.7. Практико-приложна насоченост на научното изследване

Резултатите от дисертационния труд биха могли да бъдат в полза на експерти от публичните и частни среди, ангажирани в сферата на сигурността и управлението на риска. Основните тези от работата могат да намерят своето практическо приложение в дейността по управление на корпоративната среда за сигурност, като част от процеса за постигане на устойчивост и сигурност в национален, регионален и международен аспект. Не на последно място, разработката може да бъде в полза за студенти, изследователи в сферата на сигурността и отбраната, управлението на риска и на корпоративната сигурност.

Потребители на получените научни и приложни резултати

Потребители на получените научни и приложни резултати могат да бъдат студенти, специализанти и експерти от практиката, отговорни държавни структури, частни икономически субекти, желаещи да повишат квалификацията си в съответствие с изискванията на образователните стандарти в образователното направление 9.1. „Национална сигурност”.

1.8. Основни литературни и информационни източници

При разработване на настоящия дисертационен труд са обработени, проучени, анализирани и използвани: българска и чуждестранна специализирана литература, нормативни документи, доклади, неспециализирана литература, монографии и разнообразни онлайн ресурси.

Проучените за разработване на дисертационния труд източници са 178 източници, от които 76 са на български език и 102 – на английски език.

II. СТРУКТУРА И КРАТКО СЪДЪРЖАНИЕ НА ДИСЕРТАЦИОННИЯ ТРУД

2.1. Структура на дисертационния труд

Структурата на дисертационният труд включва увод, три глави, заключение, общи изводи и препоръки от направения анализ, библиография и приложения. Изложението включва три основни тематични части, всяка от които допринася в логическа последователно за изпълнение на задачите, постигане целта на дисертационния труд и смисловата завършеност на темата.

Изследването е с общ обем от 228 страници, от които 190 страници изложение на съдържанието; научни приноси, научно-приложни приноси и публикации, свързани с дисертационния труд 2 страници; 22 страници бележки и библиография; 13 страници приложения.

2.2. Съдържание и кратко изложение на дисертационния труд

Увод
Първа глава
Корпорации и корпоративна сигурност
1.1. Същност на корпорациите
1.1.1 Видове корпорации
1.1.2 Корпоративни структури и модели на корпоративно управление
1.2. Корпоративна сигурност в трансформиращия се свят
1.2.1 Корпоративна и национална сигурност – параметри на релацията
1.2.2 Управление на корпоративната сигурност
Изводи към първа глава

Втора глава
Новата парадигма на корпоративната сигурност
2.1. Рискът в контекста на корпоративната сигурност
2.1.1 Теория на риска и разбирането за риск в корпорациите
2.1.2 Анализ на съвременните корпоративни рискове
2.2. Процес по управление на риска в корпоративната сигурност
2.2.1 Структура и управление на риска в корпоративната сигурност
2.2.2 Нива на управление на риска в корпорацията
2.3. Възможни модели за управление на риска
2.3.1 Национални подходи за управление на риска
2.3.2. Добри практики и международни стандарти
Изводи към втора глава
Трета глава
Системен подход за интелигентно управление на риска в корпоративната сигурност
3.1. Организационни аспекти на управлението на риска в компаниите
3.1.1 Управление на промяната
3.1.2 Корпоративна култура
3.1.3Корпоративната социална отговорност и признаване на заинтересованите страни
3.1.4 Имплементиране на автоматизирани решения и такива, базирани на изкуствен интелект
3.2. Теоретичен модел на стратегия за интелигентно управление на риска в корпоративната сигурност
3.2.1 Анализ на резултати от проведено анкетно проучване
3.2.2 Теоретичен модел на стратегия за управление на риска в корпоративната сигурнос
Изводи към трета глава
Общи изводи и препоръки от дисертационния труд
Заключение
Научни и научно-приложни приноси
Научни приноси
Научни-приложни приноси
Научни публикации, свързани с дисертационния труд
Бележки
Библиография
Приложения
Приложение 1: Анкетна карта
Приложение 2: Резултати от анкетно проучване
Приложение 3: Списък на използвани съкращения

Кратко изложение на дисертационния труд

В **уводната част** на дисертационния труд са представени актуалността и значимостта на изследваната тема, като е обективизиран водещият в разработката проблем. За неговото последващо разрешаване са формулирани обекта, предмета и целта на дисертационния труд, като са формулирани основните за постигане на целта изследователски задачи и подзадачи. Прецизирани са ограниченията в процеса на разработване, дефинирани са основните подходи и методология на изследването.

Първа глава. Корпорации и корпоративна сигурност

Първа глава **„Корпорации и корпоративна сигурност“** е представена същността на корпорациите, като е направен съдържателен преглед от тяхното зараждане като социални и икономически субекти през развитието им в обособени исторически периоди. Представени са основните организационни структури и моделите на тяхното управление, подкрепени с обосновка за тяхната необходимост и излагане на техните отличителни характеристики. В разработката е направен плавен и логически последователен преход към обезпечаването на сигурността на тези, по настоящем глобални субекти. Изследвани са теоретичните постижения, които отразяват значението и все по-нарастващата роля на корпоративната сигурност. Анализирани са предпоставките за нейното възникване като процес, характеристиките и основните измерения на проявление и обхват. Идентифицирана е взаимовръзката между корпоративната и националната сигурност. Изведена е работна дефиниция за транснационална корпорация. Главата е съставена от два параграфа, с по две части, и в нея е изпълнена първата изследователска задача.

Първи параграф *„Същност на корпорациите“* се състои от две части.

В **първа част** са разгледани някои от утвърдените дефиниции за понятието „корпорация“. Представени са видовете корпорации и различни техни класификации, дефинирани въз основа на базовите им характеристики,

като: място и начин на функциониране; организационна структура и структура на управление; разпределение на собствеността. Освен това е представена еволюцията и характерните особености на корпоративните структури от периода на колониализма до съвременния облик на транснационалните компании.

Втора част изследва и представя многообразието на корпоративните структури и вариациите в моделите на управление. Изведени са базовите компоненти на транснационалните компании и основните характеристики на най-често приложимите корпоративни структури, с оглед на тяхната ефективност спрямо средата, която процесите на глобализацията формират.

Втори параграф *„Корпоративна сигурност в трансформиращия се свят“* е конструиран от две части.

Първа част представя релация на понятията национална – корпоративна сигурност. Като пресечна точка, в която се концентрират и обменят световните материални и нематериални ресурси днес, корпорациите и тяхната дейност оказват пряко влияние върху националната и международна сигурност, генерирайки трансформационни процеси в социалните, трудови, образователни, производствени и потребителски сфери. Това влияние на компаниите върху елементите на националната сигурност ги превръща в неин ключов компонент. Концентрацията на ресурси в тези частни икономически субекти, обуславя необходимостта от изграждане на структури за корпоративна сигурност, чиято основна цел е защита на всички корпоративни активи. Като продължение, в този параграф е разгледана същността на корпоративната сигурност и еволюция на понятието, като то е обвързано с наличните в различни теоретични източници концепции за фирмена и икономическа сигурност. Дефинирани са обектите на корпоративната сигурност и е отчетено влиянието на все по-засилващата се тенденция, в приоритет за корпоративната сигурност да се превръща защитата и

управлението на рисковете, които са насочени към нематериалните корпоративни активи.

Втора част поставя фокус върху процеса по управление на корпоративната сигурност и върху взаимодействието на корпоративните структури със заобикалящата ги среда, в качеството им на отворени системи. Изложено и защитено е твърдението, че в основата на системата за корпоративна сигурност и нейното управление стоят създаването и прилагането на вътрешни правила за контрол и регулация на процесите. Очертани са традиционните области на корпоративната сигурност, които с мащабното разгръщане на процесите на глобализацията се оказват недостатъчни и неефективни за справяне с рисковете, което от своя страна води до разширяване обхвата на дейността на корпоративната сигурност. В резултат от това, корпоративната сигурност в съвременните компании, е насочена към идентифициране и анализ на рисковете, тяхното количествено определяне, планиране и контрол на мерките, както и за измерването и оценяването на тяхната ефективност. Като ключово за корпоративната сигурност е изведено разбирането за стойност в корпоративен аспект и възприятието, че в бизнеса задължително условие за ефективността на един процес, е неговата рентабилност. В тази връзка, цената на сигурността на компанията се явява пряко обвързана със стойността на евентуалната загуба.

Изводи към първа глава

1. В корпорациите са концентрирани световните материални и нематериални ресурси, поради което те пряко оказват влияния върху националната и международната сигурност, чрез генериране на трансформационни процеси в социални, трудови, образователни, производствени и потребителски сфери.

2. Всеки от структурните периоди на глобализацията променя концепцията за корпорациите и моделите на обезпечаване на тяхната сигурност.

3. Сигурността на компаниите е в пряка зависимост от моделите на управление, които трябва да се адаптират към съвременните рискове и промените в средата.

4. Симбиозата и споделената отговорност между държавата и корпорациите е необходимо условие и фактор за постигане на национална и корпоративна сигурност.

Втора глава. Новата парадигма на корпоративната сигурност

Втората глава **„Новата парадигма на корпоративната сигурност“** поставя акцент върху анализ на конкретните за сигурността на компанията заплахи. Изследвани са понятието „риск“ и процесите за неговото управление, в контекста на частните икономически субекти. Дефинирана е основната теза, защитавана в изследването, че корпоративната сигурност се нуждае от интелигентни решения за управление на риска, като отговор на новите рискове и заплахи. Идентифицирани са съвременните рискове за сигурността на компанията, произлизащи от глобалните процеси и са представени различни възможности за тяхната класификация. Осъществяването на цялостния процес по управление на риска в компаниите е разгледано на три ключови организационни нива – на корпоративно, на стратегически бизнес единици и на проектно ниво. Идентифицирани са общите и специфични за всяко от нивата рискове, и е направена таксономия. Представени са възможни модели за управление на риска в корпоративната сигурност, чрез синтез и представяне на национални подходи в областта и дефинирани национални изисквания, подобряващи ефективността на процесите и взаимодействието между корпоративните и национални структури. Представени са и други добри

практики, международни стандарти, в управлението на риска. Главата е съставена от три параграфа, всеки от които е съставен от по две части. В тази глава е изпълнена втората изследователска задача.

Първи параграф, ***„Рискът в контекста на корпоративната сигурност“***, се състои от две части.

В **първа част** е разгледана теорията на риска, като е направен анализ и синтез на изследвания в областта на българската и чуждестранната научни общности, като сред тях се открояват две направления. Първото разглежда риска през призмата на математическите науки, а второто направление акцентира и разглежда риска като генериран от и управляван през призмата на социалните, културни и символни специфики на средата и обществото. Днес не може да се говори за сигурност, без да се отчита рискът в неговата многоаспектност. Сигурността и рискът в съвременната среда са неразривно свързани. В последните години се наблюдава промяна в позициите на основните понятия. Тенденциозно понятието „сигурност“ бива изместван от понятието „риск“ в стратегическите документи както на държавите, така и в тези на недържавните актьори.

Управлението на риска е този процес, който следва да създаде обща рамка, съотнесена към корпоративните активи за навременно противодействие на негативни последици и тяхното недопускане. От изключителна важност при възприемането на риска в корпорациите е оценката на ключовите за компанията активи, което налага задължителна ангажираност от страна на висшето ръководство. Единствено ръководството е в състояние да очертае границите на така наречения „апетит за риск“ на компанията, който е основополагащ за формиране на стратегия и последващи политики по управление на риска.

Направено е заключението, че корпоративните рискове са всички потенциални събития, които могат да окажат влияние върху крайния резултат, към който компанията се стреми.

Във **втора част** е извършен анализ и са идентифицирани съвременните рискове за сигурността на компанията, произлизащи от глобалните процеси. Изведени са възможности за класификация на идентифицираните рискове, като са представени различни социални, правни, икономически, екологични, политически и технологични аспекти, създаващи благоприятна среда за тяхното възникване. Като цяло, в резултат от извършения анализ се отчита фрагментация на генеричната среда, която е изпълнена с много нови и нетрадиционни рискове и предизвикателства, пред които са изправени както държавите, така и частните икономически субекти.

Втори параграф *„Процес по управление на риска в корпоративната сигурност“*, се състои от две части.

В **първа част** е отчетена организационната автономност, която компаниите имат в процеса по изграждане на своите звена за сигурност и тези, за управление на риска в частност. Представени са вариации спрямо позиционирането на звеното за управление на риска в общата организационна структура, като решението за това зависи както от вида на компанията и нейния мащаб, така и от културата на тази компания и отношението ѝ към риска. Рамката по управление на риска, за да е ефективна, трябва да включва ясно формулирани корпоративни процедури, които да дават яснота по отношение на четири ключови аспекта – процесите по управление на риска (УР) в цялостната корпоративна структура и организационна дейност; стратегия за УР, подкрепена с политики и базирани на риска решения, както и конкретно разпределение на отговорностите спрямо тях; прозрачност относно възвръщаемостта, която носи управлението на риска за компанията; изграждането и поддържането на риск култура в организацията.

Втора част акцентира върху обусловеното от нарастващата организационната сложност предизвикателство да бъдат дефинирани специфичните рискове, отнасящи се до различните йерархични нива на корпоративните органи. В дисертационния труд управлението на риска в компаниите е разделено на три ключови нива, които следва да обезпечат минимизирането на евентуални негативни последици и същевременно с това да предоставят възможности за управлението им. Това може да се постигне чрез управление на риска на корпоративно ниво, на стратегическо бизнес ниво (ниво бизнес единица) и на проектно ниво, изхождайки от практиката, в която всяка отделна дейност, в съвременните корпорациите, се изпълнява под формата на проект. Първото, корпоративно ниво, олицетворява компанията като цяло – политиките и жизненоважните решения в нея, свързани със сливания, придобивания, финанси. Второто ниво е нивото на отделните стратегически бизнес единици, които са отговорни за различните направления – производство, продажби, пласмент, филиални звена. Проектното ниво е най-ниското, трето ниво, в тази йерархична корпоративна структура. То подкрепя стратегическите бизнес единици (СБЕ), чрез осъществяване на нужните действия, за постигане на поставените им цели. В резултат от това условно разделение на нивата, на които следва да бъде управляван рискът в компаниите, са идентифицирани общите и специфични за всяко ниво рискове, и им е направена таксономия, която синтезирано е представена по-долу (таблица 1).

Таблица 1. Общи и специфични рискове за сигурността на компанията.

Корпоративно ниво	**Ниво на СБЕ**	**Проектно ниво**
Поглъщания и финансови рискове	Липса на съответствие между отделните проекти	Иновационни
Монопол от страна на фирми, подкрепяни от държавата и различни форми на изнудване	Финансови рискове	Технологични
Модел на корпоративно управление и неефективна корпоративна култура	Закъснения при изпълнение – рискове, свързани със срокове и неспазване на времевата рамка	Ресурсни
Фалшифициране на продукти	Промени на външната и вътрешната среда	Културни (КК)
Тероризъм	Физически активи	Експлоатационни
Незачитане интересите на заинтересованите страни	Човешки ресурс	Породени от край на проекта или на конкретна дейност от него
Политически риск	Правна отговорност и по-конкретно – деликтно право (непозволено увреждане)	
Регулаторен и правен риск	Постигане и задържане на конкурентоспособно ниво в дейността, която е предмет на СБЕ	
Технологични рискове и кибератаки		
Здраве, безопасност и околна среда		
Репутационен риск		

Трети параграф е озаглавен ***„Възможни модели за управление на риска“*** и също се състои от две части.

В **първа част** са представени национални подходи за управление на риска. В този смисъл, като ключова в процесите по управление на риска в компаниите е изведена ангажираността на държавата при прилагането на изисквания към частните икономически субекти. Представени са възможни модели за управление на риска в корпоративната сигурност чрез синтез и представяне на национални подходи в областта и дефинирани национални изисквания/препоръки/закони, които подобряват ефективността на процесите

и взаимодействието между корпоративните и национални структури. Разгледани са практики на: Обединеното кралство, като е отчетено значението на докладите на Грийнбъри[20] от 1995 г.; на Хампел[21] от 1998 г.; на Алън Търнбул[22] от 1999 г.; докладите на Хигс[23] от 2003 г. и на Смит[24] от 2005, на Тайсън[25] от 2003; доклад на Kings College[26] от 2007 г.; на САЩ – Комисията на Организациите – Спонсори към Комисията Тредуей[27] (COSO) и законът Сарбейн Оксли[28] (Sarbanes Oxley Act); Каймановите острови – CIMA[29] и Закон за управление на компаниите[30]. Представени са четирите ключови елементи в представения през 2014 г., от ОИСР, модел за управление на риска и корпоративно управление, които са: Борд на директорите, комисии към Борда (по риска, одитни комисии) и главен служител по риска/риск мениджъра, заедно с техните основни правомощия, задължения и отговорности.

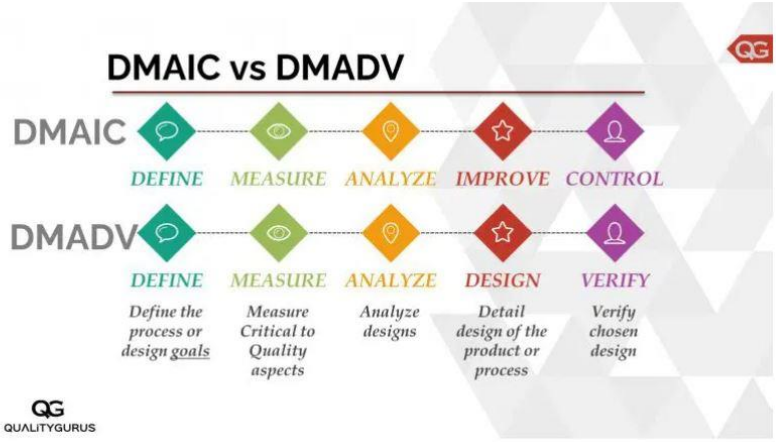
Във **втора част** са представени добри международни практики и стандарти при управлението за риска в корпоративната сигурност.

Представен е моделът Six Sigma, който е един от моделите за непрекъснато усъвършенстване като цикълът на Деминг, реализиран в четири стъпки, който стои в основата на редица международни стандарти, включително и тези, за управление на риска. Моделът е приложим за всяка организация, независимо от сферата на дейност, която иска навременно да идентифицира и отстранява грешките в своите дейности. Six Sigma се реализира в пет стъпки и може да бъде постигнат на шест нива. Това е статистически модел за вземане на управленски *решения въз основа на*

[20] The Greenbury report, 1995.
[21] The Hampel Report, 1998.
[22] The Turnbull Report, 1999.
[23] The Higgs Report, 2003.
[24] The Smith Report, 2005.
[25] The Tyson Report, 2003.
[26] King's College Report, 2007.
[27] Committee of Sponsoring Organizations of the Treadway Commission.
[28] The Sarbanes–Oxley Act, 2002.
[29] Cayman Islands Monetary Authority.
[30] Companies Management (Amendment) Act, 2023.

статистически анализ на количествени данни[31]. Методът предлага набор от инструменти, които компаниите могат да използват, за да намалят уязвимостите от извършваните дейности, да повишат качеството и печалбите си, а също и моралът на организационните членове.

Съществуват много дефиниции за метода, но концепцията най-общо се свежда до това, че Six Sigma е процесно ориентиран метод, с контрол на входа и на изхода. Six Sigma предлага два основни подхода/методологии – DMAIC и DMADV. Първият се прилага спрямо оптимизиране и подобряване на вече съществуващи бизнес процеси и проекти, и също така може да бъде използван за ефективно управление на промяната в организациите. Вторият подход – DMADV, е ориентиран към създаването на изцяло нови процеси в организацията, като би могъл да бъде от полза и когато се налага цялостна промяна на вече съществуващи такива, които са доказано неуспешни. Разликата между двата подхода се изразява в последните две фази и е показана на фиг. 1.



Фигура 1. Разлики и прилики между подходите DMAIC и DMADV[32]

[31] Cronemyr, P., 2007. Six Sigma Management: Action research with some contributions to theories and methods. Thesis for the degree of doctor of philosophy. Chalmers university of technology. Göteborg, Sweden.

[32] Източник: Difference and similarities between the Six Sigma DMAIC and DMADV methodologies: https://www.qualitygurus.com/difference-and-similarities-between-the-six-sigma-dmaic-and-dmadv-methodologies/. Last viewed: 12.09.2023.

Освен описания по-горе модел, тази част представя стандарти и различни колекции от стандарти на Международната стандартизационна организация (ISO).

Една от най-популярните и добри практики за управление на риска в корпорациите е стандартът ISO 31000:2018 Risk management – Guidelines, който е широко и общоприложим стандарт за организации с различна сфера на дейност и предназначение. Разработен през 2011 г., стандартът е актуализиран през 2018 г., като от 05.10.2023 г. има разрешение за продължаване на неговото действие. Актуализацията на стандарта от 2018 г. обръща особено внимание на разширения обхват на понятието и поставя фокус върху *включване на всички заинтересовани страни…и отчитане на човешките и културни фактори*. В началото на месец декември 2023 г. е направено предложение колекцията от стандарти ISO 31000 да бъде отново актуализирана. Промяната касае актуализация на ISO 31000:2018, която все още е на ниво „проект“ и СД Ръководство 73 на ISO:2011, което се отменя без да бъде заменяно с друг документ[33]. Стандартът не е сертификационен, а само дава насоки към организациите и няма задължителен характер за тяхното последващо прилагане. В дисертационния труд този стандарт не е обект на подробен анализ, тъй като е широко разпространен и добре познат, а настоящата разработка има за цел да изследва по-малко популярни за Република България модели за управление на риска.

Синтезирано е представен и стандартът ISO/IEC 21827:2008 Systems Security Engineering – Capability Maturity Model (SSE-CMM), който е първоначално разработен през 2002 г. и последващо актуализиран през 2008 г. Стандартът представлява модел за зрялост на инженеринга на сигурността на

[33] Български институт за стандартизация, Колекция ISO 31000 Управление на риска: https://bds-bg.org/bg/project/show/bds:proj:115039; Новият стандарт ISO 31000 опростява управлението на риска: https://bds-bg.org/bg/noviiat-standart-iso-31000-oprostiava-upravlenieto-na-riska_p3511.html. Посетени на 20.12.2023.

системите и дава описание за базови характеристики на процеса на инженеринг на сигурността на дадена организация[34]. Разработен е въз основа на Модела на зрялост на организациите (Capability Maturity Model), който е процесно-ориентиран.

Изводи към втора глава

1**.** Приоритетните рискове за корпоративната сигурност се генерират от ускорените темпове на дигитална трансформация, конкуренцията за таланти, киберсигурността и иновациите.

2. Формирането на способността на компаниите да управляват рисковете е от жизненоважно значение за постигане на общите корпоративни цели чрез управление на промените и навременна реакция.

3. Управлението на глобалните рискове, свързани със „здравето на планетата“, дигиталното неравенство, космическата надпревара, миграционните и бежанските кризи, става все по-значим фактор за сигурността на компаниите.

4. В Република България има необходимост от усъвършенстване на регулаторната рамка и механизмите в областта на управлението на корпоративния риск.

5. За да бъдат надеждни и ефективни процесите по управление на риска, те трябва постоянно да се обновяват и да са съобразени с променящата се среда за сигурност.

[34] ISO/IEC 21827:2008 Systems Security Engineering - Capability Maturity Model® (SSE-CMM®): https://www.iso.org/standard/44716.html. Last viewed: 21.08.2023.

Трета глава. Системен подход за интелигентно управление на риска в корпоративната сигурност

В трета глава – **„Системен подход за интелигентно управление на риска в корпоративната сигурност“,** са представени и анализирани организационните аспекти на компанията. Като ключови за нейното функциониране са изведени ефективността на процесите по управление на промяната, формирането и поддържането на корпоративна култура, признаване на заинтересованите страни на компанията и зачитането на техните интереси и корпоративната социална отговорност като управленски инструмент в процесите по управление на риска. Като друг организационен елемент са разгледани постиженията на научно-техническия прогрес. Синтезирани са и са представени основните характеристики на част от прилаганите от бизнеса автоматизирани решения и такива, базирани на изкуствен интелект, както и адаптирани към бизнес-процесите инструменти на военната тактика. Проведено е емпирично изследване под формата на анкетно проучване или т.нар. „структурирано интервю“, в резултат от което е предложен теоретичен модел на стратегия за управление на риска в корпоративната сигурност.

Първи параграф – *„Организационни аспекти на управлението на риска в компаниите“*, се състои от четири части.

Четирите части очертават рамките на холистичен подход, който компаниите трябва да прилагат при управлението на риска. Този подход е основан на четири ключови процеса в организацията:

- ефективно **управление на промяната** за постигане на корпоративна устойчивост;
- изграждане и поддържане на **корпоративна култура,** основана на ценности и норми, подпомагащи процесите по управление на риска;

- поемане на **корпоративна социална отговорност** и зачитане на интересите на **заинтересованите страни** на компанията чрез трансформация на бизнес-процесите и превръщане на компаниите в „корпоративни граждани“;
- имплементиране на **автоматизирани решения и такива, базирани на изкуствен интелект** в корпоративните дейности.

Изведени са ефективността на процесите по управление на промяната, както и формирането и поддържането на корпоративна култура, която подпомага обезпечаването на корпоративната сигурност и управлението на риска. Отчетена и обоснована е важността от признаване на заинтересованите страни на компанията и зачитането на техните интереси. Особено внимание е отделено на корпоративната социална отговорност като управленски инструмент в процесите по управление на риска. Като друг организационен аспект са разгледани постиженията на научно-техническия прогрес.

Синтезирани са и са представени основните характеристики на част от прилаганите от бизнеса автоматизирани решения и такива, базирани на изкуствен интелект, като са изведени предимствата за компаниите от тяхното имплементиране. Отчетено е приложението, което намират инструментите на военната тактика – CARVE(R) и FMEA, в съвременното управление на корпоративните рискове. И двата инструмента дават възможност за проактивен подход за управление на риска в компаниите. Представена е и системата за сигурност EDR (Endpoint Detection and Response), известна още като ETDR (Endpoint Threat Detection and Response), която най-общо има отношение към киберсигурността на компанията и представлява интегрирано решение за сигурност на крайните точки.

Втори параграф – „*Теоретичен модел на стратегия за интелигентно управление на риска в корпоративната сигурност*“, е съставен от две части.

В рамките на **първа част** е проведено емпирично изследване под формата на анкетно проучване, или т.нар. „структурирано интервю“. Като краен резултат, след анализ и оценка на приложимите корпоративни практики в процеса по управление на риска в компаниите и идентифицираните нагласи на служителите спрямо сигурността в организацията, са изведени пропуските, предизвикателствата и възникващите тенденции при управлението на корпоративните рискове.

Предоставената на респондентите анкета съдържа 24 въпроса с предварително зададени опции на отговори – структурирано интервю. Част от въпросите са и с възможност за предоставяне на допълнителна информация/опция да бъде даден различен от зададените шаблонни отговори. Целта е да бъде набавена и отчетена допълнителна информация, която може да послужи като допълнение към формулираната анкетна рамка и да е основа за *бъдещи изследвания и проследяване на тенденциите в областта*. Проучването е реализирано онлайн, чрез създадена анкетна карта в приложение Forms на платформа Microsoft Teams. Анкетата бе достъпна за респондентите в продължение на 14 дни, за периода от 03.10 до 17.10.2023 г., на линк: https://forms.office.com/e/B66wqPPzU6. Попълването на анкетната карта бе анонимно, а предоставената от респондентите информация се използва само в обобщен вид за целите на настоящия дисертационен труд.

В анкетното проучване участват 100 респонденти, професионално ангажирани в различни сфери на корпоративната дейност и заемащи различни позиции в йерархичните нива на организациите, в които работят.

В резултат от анализа на изследването следва да се установи наличието, или липсата на съответствие между представената теоретичната рамка и нейната приложимост от компаниите в практиката и процесите по управление на риска. При анализ на резултатите се отчита фактът, че част от респондентите не отговарят на някои от въпросите, което води до цифрово разминаване в броя

на дадените отговори и тяхното процентно съотношение. В тази връзка, процентното съотношение спрямо отговорите на всеки въпрос е на база брой дадени отговори на него.

Изследването показва че респондентите, които са отбелязали наличието на вътрешнокорпоративни стратегически документи и това, че са напълно запознати с тях, са част от компании, в които вече има имплементирани съвременни дигитални технологии и системи. Тези респонденти оценяват процесите по дигитализация като възможност за компаниите и смятат, че интелигентните технологии могат значително да подобрят процесите по управление на риска в организациите. Също така те участват, или са участвали веднъж годишно, или повече, в обучения по управление на риска. Това потвърждава тезата, че наличността на организационни правила и процедури и тяхното ефективно комуникиране чрез вътрешнокорпоративни мрежи/системи води до разбирането и прилагането им на практика, както и избягването на съпротива от страна на служителите. Нещо повече, в резултат от отговорите на респондентите, които споделят наличност на вътрешнокорпоративна документация, се забелязва висок процент на положителни отговори спрямо приложението и привеждането на компаниите в съответствие с международни/национални стандарти, които подпомагат управлението на риска. Наличието на формирана риск култура сред служителите в компанията в голям процент се отчита от тях като елемент, който оказва положително влияние върху процесите по управление на риска в компанията.

Като най-голяма слабост на съвременните компании, въз основа на резултатите от проведеното проучване, се откроява признаването на заинтересованите страни (извън клиентите) и зачитането на техните интереси. Други слабости, които могат да бъдат отчетени, са неефективна култура и обща ниска осведоменост на служителите за правила, процедури,

стандартизационна рамка относно процесите по управление на риска в компаниите.

Във **втора част** е предложен теоретичен модел на Стратегия за управление на риска в корпоративната сигурност, в обхвата на който попадат представените по-горе организационни аспекти, постиженията на научно-техническия прогрес и изкуствен интелект, без да се пренебрегват материалните и чисто финансовите измерения на процесите по управление на риска. Теоретичният модел предлага препоръчителна структура и съдържание на Стратегия за управление на риска в корпоративната сигурност в 9 основни пункта:

1. Въведение

Всяка стратегия трябва да започва с встъпителна част, която има за цел да даде яснота по въпросите, свързани с основополагащите за компанията концепции относно нейното съществуване. В този смисъл, въведението на стратегията за управление на риска трябва задължително да съдържа описание на следните компоненти:

- *Мисия*, изразяваща смисъла на съществуване.
- *Визия*, очертаваща желаното бъдеще състояние.
- Основните *принципи и ценности*, които са водещи за организацията и които са залегнали в основата на нейното функциониране под формата на писани и неписани правила, или т. нар. корпоративна култура.
- *Обхват* на стратегията, очертаваща рамката на действие на стратегията и всички обвързани в нейното изпълнение лица. Този обхват служи като база за разработване на последващи процедури и политики за взаимодействие с всички заинтересовани страни, които задължително трябва да бъдат отчетени в рамките на стратегията.
- *Водещото звено* в рамките на корпоративната структура, което е отговорно за изпълнението на стратегията и последващия контрол. Тук следва да се

посочат ангажираните с процеса лица, с техните роли, задължения, правомощия и отговорности.

- *Срок на действие на стратегията*. Всяка стратегия има срок на действие, като от гледна точка на времевата рамка, стратегиите могат да са краткосрочни – до 1 година; средносрочни – 3 –5 години и дългосрочни – 6 – 9 години. Посочените срокове са условни, тъй като теорията предлага различни времеви интервали за различните стратегии въз основа на времевия признак. С оглед на постоянно променящата се среда, настоящият модел предлага стратегията за управление на риска да е със срок на действие не повече от 5 години, като веднъж годишно се извършва преглед, а при нужда – актуализация. Стратегията може да бъде актуализирана и извън посочените срокове, с оглед динамичността на средата и установяването на обстоятелства, които налагат неизбежни нейни промени. За по-голяма гъвкавост, на организацията се препоръчва разработването на свързани със стратегията планове за изпълнение, в които са заложени ясни срокове за периода на стратегията. Към стратегията се разработват и други ръководни документи, наречени политики, в които се отразява визията на ръководството по определени процеси в организацията.

Мисията, визията, ценностите и принципите, посочени в стратегията за управление на риска, трябва задължително да са в съответствие и в хармония със заложените в общата корпоративна стратегия.

2. Дефиниране на основните понятия в документа

За да бъде разбрана от всички заинтересовани лица, в началото на стратегията е препоръчително да бъдат дадени основните използвани термини и техните дефиниции. Тази част може да бъде оформена и като отделен „речник на понятията“. Това е необходимо тъй като теоретичната рамка, дефинираща управлението на риска, е богата и липсата на такъв речник би могло да доведе до различни интерпретации.

- *Стратегия* – дефинициите на понятието „стратегия“ са многобройни и са съотносими към обекта, към който са насочени. Затова, в общата организационна стратегия и в произлизащите от нея стратегии по отделните организационни направления, трябва да бъде ясно дефинирано какво се разбира под това понятие в организацията, като бъде ясно очертана неговата рамка.
- *Политика* – определя начина на действие на организацията в различни направления от нейния жизнен цикъл, които да доведат за постигане на стратегическите цели на компанията.
- *Програма* – кратко описание на идеите, произлизащи от формираните политики и очертаване на необходимите дейности, които следва да бъдат реализирани.
- *План за изпълнение* (пътна карта) – ясно дефиниране на конкретни дейности и времето за тяхното изпълнение по начин, по който да бъдат подпомогнати общите стратегически цели. Както бе описано по-горе, те се разработват в по-кратки срокове (1 – 2 години), което позволява по-голяма гъвкавост на организация и по-лесна адаптация към промените. Плановете биват наричани още „пътни карти“, тоест документи, които описват стъпка по стъпка реализацията на заложената програма.
- *Риск* – за целите на стратегията организациите биха могли да използват дефиницията за „риск“, дадена в стандарта ISO 31000 „Управление на риска“, която гласи, че това е *влияние на неопределеността за постигане на целите*.
- *Апетит за риск* – апетитът за риск се изразява в размера и вида на риска, който организацията е готова да поеме, за да постигне своите дългосрочни стратегически цели.
- *Толерантност към риск* – очертава границите, които компанията не е готова да премине, за да постигне стратегическите си цели. Това може да

са активи, които организацията не е склонна да жертва и следователно трябва да намери друг, по-безопасен начин, за постигане на целите си.

- *Управление на риска* – примерна дефиниция, на която компаниите могат да се позоват в своите понятийни речници е тази, на наръчника на Съвета за корпоративно управление на САЩ, според която УР в компанията я подпомага, в условия на рискова среда, да е в състояние *да постигне своите бизнес цели; да формулира своето виждане за стойност; да оценява толерантността си към риска; и да проектира своите процеси, с оглед на разумните очаквания на заинтересованите страни*[35].
- *Заинтересовани страни* – това са всички, които могат да повлияят или да бъдат повлияни от дейността на компанията лица, групи, общности и др. Те могат да са както външни, така и вътрешни за организацията. От изключителна важност за управлението на рисковете се оказва признаването на тези страни от организациите. За съжаление, основна слабост на компаниите е именно процесът по идентифициране и отчитане на интересите на тези страни.
- *Ключови активи* – това са всички корпоративни активи – материални и нематериални, които са жизненоважни за компанията и без които тя не може да функционира и следователно, да постига целите си.
- *Съответствие* – привеждането в еднаквост с налични нормативни актове или изисквания в различни сфери на дейност от организационния живот; съотношение между изискуеми норми и тяхното изпълнение/прилагане в рамките на организацията.

3. Анализ на средата

Методологията за стратегическо планиране в Република България[36] дава един добър обхват и ясно описание на анализа на средата, като освен да отчита

[35] Risk Governance Guidance for Listed Boards, Corporate Governance Council, May 2012
[36] Методологията за стратегическо планиране в Република България, 2010 г.

основните компоненти на всяка система, този анализ трябва да предоставя обективна оценка на състоянието, в което се намира организацията. Целта на анализа е да се добие ясна представа къде се намира компанията към момента на неговото изготвяне, кои са основните характеристики на средата и кои са новите факти и обстоятелства, които организацията следва да вземе предвид. Анализът е изходната точка, която следва да бъде използвана за целеполагането в компанията и взимането на управленски решения в процеса на целепостигане. Резултатът от него е основа за разработване на програми, политики и планове по начин, по който те да са приложими и ефективни на фона на заобикалящата среда – вътрешна и външна за организацията. Препоръчително е такъв анализ да се извършва периодично (поне веднъж годишно) или при форсмажорни обстоятелства, които налагат промяна в стратегията или някой от нейните ключови компоненти.

Предлагат се редица аналитични методи и такива, за последваща оценка на средата, като GAP анализ, SWOT анализ, PESTE и други. Анализът на средата е средство за проследяване развитието на вече идентифицирани рискове и откриването на потенциални нови такива, които компанията следва да класифицира и да приоритизира въз основа на активите, към които са адресирани. Освен вече описаната информация, анализът може да бъде използван и за откриване на възможности, чрез идентифициране на характеристики на средата, които могат да повлияят благоприятно за постигане на корпоративните цели, ако бъдат навреме уловени.

4. Цели на стратегията

Цел на стратегията за управление на риска в корпоративната сигурност е да се гарантира защита на всички корпоративни активи, при пълно регулаторно съответствие на процесите в компанията, с поставяне на акцент/приоритет върху:

- *Околната среда* – чрез постигане на екологична ефективност и управление на екологичните рискове.
- *Информационните и интелектуални ресурси* – като основен обект на атаки.
- *Имплементирането на автоматизирани решения в корпоративните процеси по управление на риска* – като средство за генериране на бързи и ефективни решения, благодарение на безпрецедентните им възможности за обработка и анализ на огромни мащаби от данни.
- *Поемане на отговорност спрямо протичащите социални процеси и постигане на устойчивост* – прилагане на добри практики в областта на корпоративната социална отговорност и равни условия на труд.
- *Формиране и поддържане на култура за сигурност в компанията* - като инструмент на корпоративната сигурност и процесите по управление на риска, чрез привличане на човешкия фактор към постигане на общите организационни цели и изграждане на лоялност към компанията.

5. Етапи на изпълнение на стратегията

За ефективност на стратегията, настоящия теоретичен модел предлага следните базисни етапи за нейното изпълнение, изхождайки до известна степен, но не изцяло от известния Цикъл на Деминг. Концепцията се въвежда през 50-те години на XX век в Япония, а в съвремието е широко използвана за подобряване на процеси и управление на различни по характер промени в организациите. Цикълът Plan-Do-Check-Act (PDCA) е четиристепенен непрекъснат модел, чиито стъпки постоянно се повтарят и по този начин се осигурява проверка на ефективността на предвидените процеси. Цикълът на Деминг може да бъде срещнат и като Plan-Do-Study-Act (PDSA).

- *Разработване на политики*, процедури и правила за управление на риска в компанията, адресирани към ключовите активи.
- *Комуникиране* към вътрешните и външните заинтересовани страни чрез провеждане на информационни срещи и кампании.

- *Апробиране* на стратегията при нейното първоначално въвеждане и последващи актуализации.
- *Коригиращи действия* – въвеждане на механизми за мониторинг и отчетност на етапите на изпълнение, както и предприемане на коригиращи дейности при необходимост.

6. Мониторинг и контрол по цялостното изпълнение на стратегията.

В тази стъпка трябва да се формулират правила, чрез които да се проследява изпълнението на формулираната стратегия като цяло и ефективността на нейните планирани етапи. Отговорните за реализацията на тази стъпка от стратегията лица следва да създадат вътрешнокорпоративни механизми за извършване на проверки спрямо спазване на установените по управление на риска процедури и степента на тяхното възприятие от страна на организационните членове. В тази част стратегията може да предвижда различни по вид симулации, за да се проследи степента на усвояване и адекватно прилагане на разписаните процедури. Мониторингът също така има за цел да проследява прозрачното и ефективно използване на отпуснатите за изпълнение на дейностите по УР дейности финансови средства. Може да се дефинират и начини за отчетност, като например годишни доклади и други.

7. Финансово осигуряване на дейностите от стратегията за управление на риска

Финансовото осигуряване на дейностите може да бъде под формата на изготвена бюджетна рамка, която да е пряко обвързана с поставените стратегически цели и приоритетните области. Тя трябва да съдържа подробно описание на дейностите и стойността на тяхното финансово измерение, както и ангажираните с тяхното изпълнение звена/организационни структури. Изпълнението на дейностите по управление на риска е ресурсоемко, което изисква много добра обосновка на бюджета, за да бъде той одобрен още в процеса на подготовка на стратегията. В него трябва да бъдат включени всички

необходими ресурси, заедно с тяхното количествено и качествено остойностяване. Следва да се формират входни индикатори, въз основа на които да се измерят необходимите за изпълнението на дейностите ресурси и изходни индикатори, които да служат за оценка на изпълнението на бюджета.

8. Очаквани резултати от изпълнението на стратегията

Както всяка стратегия, така и тази за управление на риска в корпоративната сигурност трябва да очертава резултатите, които се предвижда да бъдат постигнати от нейното изпълнение. Именно тези резултати очертават разликата между анализа на средата, т.е. сегашното състояние на компанията и промяната, която следва да настъпи след прилагане на предвидените в стратегията дейности. Очакваните резултати трябва да отразяват промяна в състоянието на всички заинтересовани страни. Освен това трябва да бъдат документално представени чрез количествени, финансови и качествени данни като отчитат, с възможно най-голяма точност, степента на удовлетвореност на заинтересованите страни – вътрешни и външни.

9. Приложения

Теоретичният модел дава възможност към стратегията да бъдат създадени приложения, които да предоставят допълнителна информация по нейното изпълнение. В раздел „Приложения“ могат да бъдат разработени корпоративни шаблони за отчет и други дейности, които да унифицират вътрешнокорпоративната документация. Тук например, като приложение, може да бъде обособена стъпка 2 от настоящия теоретичен модел – „Речник на основните понятия“.

Като отворени системи и социални организации, компаниите разработват редица правила, които да служат като изходна точка при вземането на управленски решения. Постигането на общите организационни цели следва да се осъществява в рамките на предварително зададена рамка. В този смисъл, както дейността на компаниите като цяло, така и процесите по управление на

риска в тях имат нужда от общо и всеобхватно ръководство, което да очертава пътя към минимизиране на потенциалните негативни въздействия на средата. Днес невъзможно се оказва поддържането на жизнения цикъл на една организация, ако тя не разполага със стратегия за управление на риска.

Изводи към трета глава

1. Новата парадигма за корпоративна сигурност изисква отчитане на интересите на заинтересованите страни и новите характеристики на средата, които все повече имат социално, правно, технологично и екологично измерение.

2. Имплементирането на модели, основани на автоматизирани решения и изкуствен интелект, води до промяна в начините за взимане на решения, като провокира еволюция на установените практики за идентификация, анализ и оценка на рисковете.

3. Утвърдили се във военната област инструменти на военната тактика се адаптират към съвременни бизнес-процеси и намират своето приложение в управление на корпоративните рискове за удовлетворяване на потребността от сигурност на компаниите.

4. Предизвикателство пред компаниите е мотивирането на служителите за проактивно поведение по отношение на новите рискове и заплахи.

5. Тенденцията за нарастване на атаките към нематериални корпоративни активи изисква ефективно управление на рисковете чрез нови модели, с акцент върху технологични и социални инструменти.

III. ОБЩИ ИЗВОДИ И ПРЕПОРЪКИ ОТ ДИСЕРТАЦИОННИЯ ТРУД

3.1. Общи изводи

1. Сигурността на компаниите е споделена отговорност между всички членове на организацията, а в основата на обезпечаването ѝ е заложен моделът на управление, чрез който се осъществява адаптация към промените и защита на всички корпоративни активи.

2. С оглед на съвременните рискове, подходите за тяхното ефективно управление, трябва да се основават на взаимодействието и взаимната ангажираност между структурите от системата за национална сигурност и звената за корпоративната сигурност в компаниите.

3. За ефективното управление на риска, основополагащо е наличието на вътрешнокорпоративна документация, която да дефинира процесите по управление на риска в компаниите и отговорностите на всички заинтересовани страни.

4. В управлението на риска намират успешно приложение адаптирани към бизнес-процеси инструменти на военната тактика, установени национални изисквания, различни национални/международни стандарти.

5. Нараства ролята на прогнозния анализ като ключова дейност при управлението на риска в корпорациите и заедно с базираните на изкуствен интелект системи повишава ефективността на управлението на риска и вземането на стратегически решения в компаниите.

6. Интелигентните решения за постигане на стратегическите цели на организацията трябва да са подчинени на колаборацията между интелигентността, резултат от научно-технологичния прогрес с интелигентността, присъща за човека.

7. Съвременните стратегии за управление на риска в корпоративната сигурност трябва да формират холистичен подход, в който водещи акценти да са: изграждане на способности за постигане на устойчивост чрез ефективни процеси по управление на промяната; прилагане на социално отговорни практики и признаване на всички заинтересовани страни; изграждане на ефективна корпоративна култура и имплементиране на автоматизирани решения в процесите по управление на риска.

3.2. Препоръки

В резултат от настоящото изследване могат да бъдат направени следните препоръки:

1. Да бъдат формулирани държавни препоръки за създаване на комисии по управление на риска, или друг вътрешнокорпоративен орган, като се предвидят и мерки по мотивация за тяхното прилагане от компаниите.

2. Да бъдат привлечени и представителни работодателски и съсловни организации като активни участници в процеса за разработване на единна държавна политика по управление на риска в корпорациите.

3. Да се популяризират държавните политики в сферата на корпоративната социална отговорност.

3.3. Заключение

Въздействието на корпоративния свят върху обществения, икономическия, политическия и социалния живот, а също и върху екологичните аспекти, поставя под въпрос съществуващите модели и практики за управление на риска. Това налага изграждане на нова парадигма, която в много по-широк аспект да отчита характеристиките на средата и нагласите на всички заинтересовани страни и да прилага нова, интелигентна рамка от механизми за управление на рисковете. Новите условия изискват не само защитен подход, но и по-голяма активност спрямо все по-непредсказуемите

атаки, които се реализират по все по-изкусни методи, благодарение на съвременните технологични средства.

Днес автоматизираните инструменти за управление на риска намират изключително широко приложение в различни области на корпоративния свят. Стремежът към оптимизиране на разходи и време, чрез заместване на човешкия фактор и прилагането на технологични решения за осъществяването на различни функции, постига своя успех спрямо процесите по управление на рисковете, но в същото време именно този технологичен напредък повишава и уязвимостта на компаниите. Рисковете за сигурността на корпоративните активи и щетите, които могат да бъдат нанесени от употребата на изкуствен интелект, са поле на настоящи изследвания, които ще добиват все по-голяма актуалност със задълбочаващите се процеси по имплементиране на тези решения в различни сфери на дейност.

В общата рамка на организацията, управление на риска има както оперативно, така и стратегическо значение. За да бъдат постигнати висшите цели на компанията, стратегията за сигурност и тази за управлението на риска трябва да са синхронизирани с общата организационна стратегия. Обратното би довело до непродуктивност и невъзможност за ефективна и ефикасна защита на корпоративните ресурси. Процесът по синхронизация в организацията отразява метода на координиране между нейните съставни елементи по начин, по който всеки от тях да бъде интегриран в постигането на корпоративните цели и разпределението на ресурси, да е обхванат от корпоративната култура, да участва ефективно в организационните дейности. За да бъде успешна дейността на корпоративната сигурност, на ниво висше ръководство следва да бъдат предприети стъпки по стратегически анализ, разработване и последващо внедряване на стратегията за управление на риска.

Отделно от постиженията на научно-техническия прогрес, управлението на риска днес не може да не отчита нематериалните активи на компанията,

които трябва да са акцент в разработването на стратегии за управление на риска. Формирани като основен обект на атаки, отчитането на тези активи е задължително, за да може по-детайлно и в по-голяма дълбочина да бъдат идентифицирани и последващо управлявани съвременните корпоративни рискове.

3.4. Научни и научно-приложни приноси

Научни приноси

1. Дефинирана е нова парадигма на корпоративната сигурност. Обоснована е тезата за необходимост от симбиоза между национална и корпоративна сигурност, и споделена отговорност за тяхното постигане.
2. Управлението на риска е концептуализирано като проблем на сигурността на компаниите в съвременната среда на тяхното функциониране. Дефинирани са ново съдържание и измерения на ефективно управление на съвременните корпоративни рискове.

Научно-приложни приноси

1. Идентифицирани са актуалните рискове за сигурността на компанията, като те са анализирани и класифицирани на ниво корпорация, стратегически бизнес единици и на проектно ниво.
2. Направен е сравнителен анализ на международни „добри практики“ на управление на риска за сигурността на корпорацията и е оценена тяхната приложимост.
3. Разработен е теоретичен модел на Стратегия за управление на риска за корпоративната сигурност на база проведено емпирично изследване, което дефинира новите фактори за ефективно управление на сигурността в компаниите.
4. Формулирани са препоръки за усъвършенстване и повишаване на ефективността на процесите по управление на риска в компаниите.

3.5. Научни публикации, свързани с дисертационния труд

1. МЛАДЕНОВА, М., 2019. Корпоративна култура: Невидимото конкурентно предимство. *Военен журнал*, том 126, бр. 3, с. 108 – 113. София: Военна академия „Георги Стойков Раковски“. ISSN 0861-7392.

2. МЛАДЕНОВА, М., 2020. Употребата на персонални устройства в организацията и рисковете за сигурността. В: С*борник доклади от Международна научна конференция „Сигурност – образование, наука, индустрия“, Първа част,* с. 191 – 194. София: Военна академия „Георги Стойков Раковски“. ISBN 978-619-7478-57-0.

3. МЛАДЕНОВА, М., 2022. Корпоративна социална отговорност като инструмент на корпоративната сигурност. В: *Сборник доклади от Годишна научна конференция на ВА – „110 години традиция, качество, престиж“, Първа част*, с. 163 – 167. София: Военна академия „Георги Стойков Раковски“. ISBN (online): 978-619-7478-93-8.

ВОЕННА АКАДЕМИЯ „ГЕОРГИ СТОЙКОВ РАКОВСКИ“

FACULTY: NATIONAL SECURITY AND DEFENSE

DEPARTMENT: NATIONAL AND INTERNATIONAL SECURITY

MIROSLAVA OGNYANOVA MLADENOVA

INTELLIGENT SOLUTIONS FOR RISK MANAGEMENT IN CORPORATE SECURITY

ABSTRACT

of a Dissertation Thesis

for the acquisition of the educational and scientific degree "Doctor"

in the field of higher education: 9. "Security and Defense"

professional direction 9.1. "National Security"

Doctoral program "Military-Political Issues of Security"

Scientific supervisor:

Associate Professor Dr. Ilina Stefanova Kozarova-Armencheva

Sofia, 2024

The thesis consists of 228 standard pages, including:

• Main text - 190 pages;

• Scientific contributions, scientific-applied contributions and publications related to the dissertation - 2 pages;

• Notes and bibliography - 22 pages;

• 3 appendices - 13 pages;

• The main text contains 4 figures and 1 table.

• The list of cited and used literature includes 178 titles, of which 76 are in Bulgarian and 102 in English.

• What has been presented is systematized in an introduction, three chapters, a conclusion, general conclusions and recommendations.

• Title: "Intelligent Solutions for Risk Management in Corporate Security".

• Author: Miroslava Ognyanova Mladenova

• Circulation: 10 pcs.

• Goes out of print on __.__.2024.

• "G. S. Rakovski" Military Publishing House

The PhD student was enrolled in doctoral studies through independent training in the "National and International Security" Department at the "National Security and Defence" Faculty of "G. S. Rakovski" National Defense College and granted the right of defence by order No. SI29-RD03-218/06.11.2023 of the Commandant of "G. S. Rakovski" National Defence College, effective from 06.11.2023.

The PhD thesis was discussed before a scientific jury under the "Military-Political Problems of Security" doctoral program at the extended faculty council of

"National and International Security" Department of "National Security and Defense" Faculty of "G. S. Rakovski" National Defence College, on __.__.2024.

The PhD student works in the "National and International Security" Department at the "National Security and Defense" Faculty of "G. S. Rakovski" National Defence College, in the position of "Assistant".

Materials are available to all interested on the website of the "G. S. Rakovski" National Defence College.

The defence of the dissertation thesis will be held on ___.___.2024 at _____ in hall ____ of "G. S. Rakovski" National Defence College, Sofia at an open session of a scientific jury composed of:

1. Associate Professor Dr. Irina Nikolaeva Mindova-Docheva

2. Associate Professor Dr. Ivan Petrov Panchev

3. Associate Professor Dr. Plamen Nikolov Bogdanov

4. Associate Professor Dr. Konstantin Kirilov Kazakov

5. Professor Dr. Stefan Ivanov Michev

Reserve members of the scientific jury:

1. Professor Dr. Velichka Ivanova Milina

2. Professor Dr. Evgeni Petrov Manev

CONTENT OF THE ABSTRACT

I. COMMON CHARACTERISTICS OF THE PHD THESIS

1.1. Relevance and significance

In the beginning of XIX century, achieving economic, informational, technological and political superiority becomes an ultimate goal. International rules and norms are dynamically changing and are sometimes circumvented by the powerful companies and "players" of the day. Private interest, specifically in the business area, turns into an influential factor affecting significant international processes and events. Capital invested on behalf of different corporations located in different countries puts them into two-way interactive process; on one hand, they are dependent on the security of the countries they operate in, but on the other the same countries' security is highly dependent on them. In the last few years, thanks to the resources and the impact of information, companies start exerting big influence on different socially significant issues. Along with that, they help manage a lot of international crises, defined as non-traditional[1].

Corporate security management has become an object of scientific interest on the part of the academic community and expert-practitioners. The nature of corporations, the parameters of their functioning and management models is a truly multidisciplinary topic, which has been viewed from various perspectives. In Bulgarian scientific literature, this area has been explored from the perspective of commercial law, where we can distinguish the work of O. Gerdgikov[2] and T. Buzeva[3]. From the point of view of economic relations, this topic has been examined in the work of M. Stoimenov[4], S.Savov[5], T. Spasow[6], and S.Statev, N. Nikolova[7],

[1] Dimov, G., 2019. Krizisniyat menidzhmant mezhdu mira i voynata. Sofia: VA „G.S. Rakovski". ISBN 978-619-7478-40-2.
[2] Komentar na targovskia zakon. Glava Treta, 1998; Kapitalovi targovski druzhestva, 2011.
[3] Buzeva, T., 2006. Holding. Sofia. ISBN 9547303503.
[4] Stoimenov, M., 1999. Finansirane na mezhdunarodnata targovia. Sofia. ISBN 9549050513.
[5] Savov, S., 1998. Ikonomiks. Sofia. Trakia-M. ISBN 9549574202.
[6] Spasov, T., Statev, S., 2008. Osnovi na ikonomicheskata teoria. Sofia. UNSS. ISBN 9789544949990.
[7] Nikolova, N., 2016. Korporativna ikonomika. Varna. IK Steno. ISBN 978-954-449-860-3.

M.Neicheva[8], N. Naidenov[9]. A number of authors devote a special attention to the frame of corporate management with a focus on conventional risks. Among the active researchers in the field of corporate security and risk management we can point out the name and work of N. Slatinski,[10] E. Vasilev[11], P. Ivanov[12], G. Sandev[13], G. Tornev[14], N. Krushkov[15], etc. More research in the area of management of risk processes concerning corporate companies is largely conducted in foreign scientific work, in particular M. Kabrich[16], M.Colier[17], M. Marchetti[18], T. Merna[19] etc. Scientific research dealing with the interaction between national and corporate security and its significance is much harder to find. It should be mentioned that thorough research is mostly lacking in the area of so-called "new risks" for corporate security, which because of their nature cannot be managed and prevented with the familiar models and instruments.

The environment in which companies have to operate nowadays is complex, with increasing ambiguity and unpredictability of events; it is also subject to various strategic shocks of. Risk, being defined as the basic characteristic of this environment is the new normality (Bek 2013). In this new reality, subjected to the globalization processes and changes in the environment, the notion of security turns out to be, to a large extent, a sustained/stable and constantly growing concept (Dimitrov, A.,

[8] Neycheva, M. , 2018. Ikonomika na mnogonatsionalnata korporatsia: predpostavki, praktiki, posleditsi. Burgas. Flat. ISBN 978-619-7125-42-9.
[9]Naydenov, N., 2002. Korporatizam – nov tip sotsialno-ikonomicheska sistema: http://www.iki.bas.bg/Journals/EconomicThought/2002/2002-5/2.pdf. Poseten na: 20.11.2022.
[10] Slatinski, N., 2019. Riskat – novoto ime na sigurnostta. Iztok-Zapad. Sofia. ISBN 978-619-01-0526-8.
[11] Vasilev, E., 2000. Firmena sigurnost. Neloyalna konkurentsia i firmen shpionazh. Sofia. Trud. ISBN – 954528188X.
[12] Ivanov P. 2018. Usavarshenstvane na korporativnata sigurnost vav finansova struktura. Avtoreferat, UNSS. Sofia.
[13] Sandev, G., 2005. Strategii za sigurnost na firmata. Shumen. UI Episkop Konstantin Preslavski. ISBN 954-577-310-3.
[14] Tornev, G., 2020. Korporativna sigurnost. VTU Kableshkov. ISBN 978-6197472-12-7.
[15] Krushkov, N., 2020. Sigurnost, kreativnost, liderstvo. Sofia. IK-UNSS. ISBN -978-619-232-303-5.
[16] Cabrich, M., 2015. Corporate Security Management Challenges, Risks and Strategies. Butterworth-Heinemann. ISBN – 9780128029350.
[17] Colier, P., M., 2009. Fundamentals of Risk Management for Accountants and Managers. Tools and Techniques. Oxford Butterworth-Heinemann. 1st edition. ISBN 13: 978-0-7506-8650-1.
[18] Marchetti, A., M. 2011. Enterprise Risk Management Best Practices. From Assessment to Ongoing Compliance. Wiley Corporate F&A.
[19] Merna, T., Al-Thani, F., 2008. Corporate Risk Management. John Wiley & Sons Ltd – 2d edition. ISBN 978-0-470-5 978-0-470-51833-5.

Pavlov, G. 2021, p. 25). Events, which used to take place within the borders of countries, nowadays “spill beyond borders” and achieve a new supranational representativeness. Global processes form a new security environment, new impact factors, as well as new tools for their management. In this new reality, the question about the companies’ security and the security of the corporate assets becomes more and more current. Establishment of more organized and efficient risk management systems, as well as counteracting the threats arising from them, turns into a major challenge. This fact creates a new context and necessitates a new paradigm of corporate security. Moreover, this new context requires an update of existing strategies, as well as combining and sophistication of the set of instruments used for corporate risk management. All this should be done while taking into account the changes in the national and international security environment.

The relevance of the subject comes from the urgent necessity of finding and applying more effective decisions for risk management for the sake of corporate security. The environment dynamics on a global scale requires a more thorough approach to the threats of the new reality and the unpredictable environment in which the companies exist. In order to meet adequately the posed threats, the companies need to implement innovative intelligent decisions for risk management in corporate security, whose ultimate aim is, through balance, to achieve sustainability of the processes taking place in the companies and between them. Companies nowadays constantly expand their reach and deepen their influence over different areas in our life, as their importance for the socio-economic, political, and environmental processes increase. This holds true both at national and supranational level. In this respect, their impact should be taken into account from the systems of international and national security.

The significance of the subject comes from the increasing insecurity on a global scale and the utmost necessity of timely risk identification and management, all this caused by the dynamic environment. At a time when a state of absolute

"security" is almost impossible to achieve, corporations cannot rely on the traditional means of defense only. Now they need intelligent decisions, through which to manage the multitude of risks through good practices and automatic decision implementation in their actions when norm compliance is met. Along with that, the requirements defined by the national and international standards should be met.

The research of the thesis puts a focus on the so called "intelligent decisions" and their application in the process of corporate security management. In the last years, the association of the term with the technological advance and evolution of systems, based on artificial intelligence, has been widely accepted. Along with this, one should take into account the fact that intelligence is a basic characteristic of a person, which is defined as a biopsychological potential for processing information (Gardner et al. 2021, p. 109) and its subsequent use in various areas of life.

1.2. Object, subject and purpose of the study

The object of research in the thesis is corporate security.

The subject of the study is the possible intelligent solutions for the management of corporate security risks, which would ensure a sustainable operating environment by building capabilities for timely adaptation to the environment, implementing modern management models and applying corporate responsibility practices and commitment to the stakeholders of the company.

The aim of the thesis is to formulate a theoretical strategy model that will lead to more effective corporate security risk management by proactively building capabilities for timely adaptation and functioning in an increasingly uncertain environment.

1.3. Research tasks

1. To explore and analyse the evolution of the concepts of corporations, corporate structures and corporate security, tracing the development of governance models in corporations and identifying the parameters of corporate security.

2. To identify the current risks for companies by examining and analysing the security environment and defining the levels and possible risk management models.

3. To research and analyse innovative organizational approaches to risk management in companies and, on the basis of research carried out in various corporate structures, to formulate a theoretical model of a risk management strategy in corporate security.

1.4. Thesis and working hypothesis of the dissertation

The thesis of the dissertation is that corporations, in order to effectively manage their security risks and achieve their corporate goals, must implement new, intelligent risk management solutions that take into account the interests of all stakeholders and are in line with legally established rules and norms.

The working hypothesis of the thesis is that if companies implement new, intelligent risk management solutions, by proactively building capabilities for timely adaptation, they can reduce their vulnerability and manage their security risks more effectively.

1.5. Research methodology

The research methods in the thesis are tailored to the formulated tasks and the specifics of the problems being investigated. The following traditional methods of scientific research were used in the scientific research:

- theoretical analysis and synthesis;
- system analysis;
- Induction and deduction;
- collecting, summarizing and analysing publicly available information;
- research of paper and electronic information sources;
- empirical research and processing of statistical data.

1.6. Limitations of the study

1. Research focus is placed on transnational corporations (TNCs) and the economic subjects identified with them.

2. Banking and financial institutions were not considered, due to the specifics of their regulation and activity.

3. The term "corporate security" is equated with the concept of "organizational security" and the terms "organization", "company" and "corporation" are used interchangeably to avoid tautologies. The concept of "firm" is inapplicable, according to the provisions of the Commerce Act. It is used only to trace the evolution of the concept of "corporate security".

4. Risk management solutions based on artificial intelligence are not presented in detail, due to the clarification made above that for the purposes of this thesis, "intelligent solutions" will be understood as those solutions that are the result of innate and developed abilities inherent in the human individual, in combination with the achievements of scientific and technical progress.

1.7. Practical-applied focus of scientific research

The results of the thesis could be of benefit to experts from the public and private entities involved in the field of security and risk management. The main theses of the work can find their practical application in the activity of managing corporate security environment, as part of the process of achieving sustainability and security, from a national, regional and international perspectives. Last but not least, the development can benefit students, researchers in the field of security and defense, risk management and corporate security.

Users of the obtained scientific and applied results

Users of the obtained scientific and applied results can be students, experts and practitioners, specific government agencies, private economic entities wishing to improve their qualifications, in accordance with the requirements of the educational standards in Educational Field 9.1. "National Security".

1.8. Main literary and informational sources

In the development of this thesis, the following were processed, studied, analysed and used: Bulgarian and foreign specialized literature; legislative and

regulatory documents, reports, non-specialized literature, monographs and various online resources.

The sources studied for the development of the thesis consist 164 sources, of which 64 are in Bulgarian and 100 in English.

II. STRUCTURE AND BRIEF CONTENTS OF THE THESIS

2.1. Structure of the thesis

The structure of the thesis includes an introduction, three chapters, a conclusion, general conclusions and recommendations from the analysis, bibliography and appendices. The exposition includes three main thematic parts, each of which contributes in a logical sequence to the fulfilment of the tasks, the achievement of the goal of the thesis and the meaningful completion of the topic.

The study has a total volume of 228 pages, of which 190 pages are an exposition of the content; scientific contributions, scientific-applied contributions and publications related to the thesis, 2 pages; 22 pages of notes and bibliography; 13 pages of appendices.

2.2. Contents and summary of the thesis

Introduction

Chapter One

Corporations and Corporate Security

1.1. Nature of Corporations

1.1.1 Types of Corporations

1.1.2 Corporate Structures and Models of Corporate Governance

1.2. Corporate Security in a Changing World

1.2.1 Corporate and national security – relationship parameters

1.2.2 Corporate Security Management

Conclusions to the first chapter

Chapter Two

The New Paradigm of Corporate Security

2.1. Risk in the Context of Corporate Security

2.1.1 Risk Theory and the Understanding of Corporate Risk

2.1.2 Analysis of Modern Corporate Risks

2.2. Corporate Security Risk Management Process

2.2.1 Structure and Corporate Security Risk Management

2.2.2 Levels of Risk Management in a Corporation

2.3. Possible Risk Management Models

2.3.1 National Approaches to Risk Management

2.3.2. Good Practices and International Standards

Conclusions to Chapter Two

Chapter Three

A Systems Approach to Intelligent Risk Management in Corporate Security

3.1. Organizational Aspects of Corporate Risk Management

3.1.1 Change Management

3.1.2 Corporate Culture

3.1.3 Corporate Social Responsibility and Recognition of Stakeholders

3.1.4 Implementation of Automated Solutions and Ones Based on Artificial Intelligence

3.2. A Theoretical Model of an Intelligent Risk Management Strategy in Corporate Security

3.2.1 Analysis of survey results

3.2.2 Theoretical model of risk management strategy in corporate security

Conclusions to Chapter Three

General conclusions and recommendations from the dissertation work

Conclusion

Scientific and scientific-applied contributions

Scientific contributions

Scientific and applied contributions

Scientific publications related to the dissertation work

Notes

Bibliography

Appendices

Appendix 1: Questionnaire

Appendix 2: Survey results

Appendix 3: List of abbreviations

Brief presentation of the thesis

In the **introductory part** of the thesis, the currency and significance of the researched topic are presented, objectifying the leading problem in the development. For its subsequent resolution, the object, the subject and the purpose of the thesis are formulated, and the main research tasks and sub-tasks for achieving the goal are formulated. The limitations in the development process are specified, the main approaches and research methodology are defined.

Chapter One. Corporations and Corporate Security

The first chapter **"Corporations and Corporate Security"** presents the essence of corporations, with a comprehensive overview of their origin as social and economic entities through their development in specific historical periods. The main organizational structures and their management models are presented, supported by a rationale for their necessity and an exposition of their distinguishing characteristics. The development makes a smooth and logically consistent transition to the issue of ensuring the security of these, currently global entities. Theoretical advances that reflect the importance and ever-increasing role of corporate security are explored. The prerequisites for its emergence as a process, the characteristics and the main dimensions of manifestation and scope are analysed. The interrelationship between

corporate and national security is identified. A working definition of a transnational corporation is derived. The chapter is composed of two paragraphs, with two parts each, and it fulfils the first research task.

The first paragraph, *"The Nature of Corporations"*, consists of two parts.

The first part examines some of the established definitions of the concept of "corporation". The types of corporations and their various classifications are presented, defined on the basis of their basic characteristics, such as: location and mode of functioning; organizational structure and management structure; distribution of property. In addition, it presents the evolution and characteristic features of corporate structures from the period of colonialism, until the appearance of modern transnational companies.

The second part explores and presents the diversity of corporate structures and variations in governance models. The basic components of transnational companies and the main characteristics of the most frequently applicable corporate structures are derived, with a view to their effectiveness in relation to the environment that globalization processes form.

The second paragraph, *"Corporate Security in a Changing World"*, is constructed in two parts.

The first part presents a relationship between the concepts of national and corporate security. As the intersection where the world's material and immaterial resources are concentrated and exchanged today, corporations and their activities have a direct impact on national and international security, generating transformational processes in the social, labour, educational, production and consumer areas. This influence of companies on elements of national security makes them a key component. The concentration of resources in these private economic entities determines the need to build corporate security structures, the main purpose of which is the protection of all corporate assets. As a continuation, this paragraph examines the essence of corporate security and the evolution of the concept, as it is

linked to the concepts of company and economic security available in various theoretical sources. The objects of corporate security are defined and the influence of the ever-increasing tendency to make risk protection and management, aimed at intangible corporate assets, a priority for corporate security.

The second part focuses on the corporate security management process and the interaction of corporate structures with their environment, as open systems. It presents and defends the claim that the basis of the corporate security system and its management is the creation and application of internal rules for control and regulation of processes. The traditional areas of corporate security are outlined, which, with the large-scale development of globalization processes, prove to be insufficient and ineffective for dealing with risks, which in turn leads to the expansion of the scope of corporate security activities. As a result, corporate security in modern companies is aimed at identifying and analysing risks, quantifying them, planning and controlling measures, as well as measuring and evaluating their effectiveness. The key to corporate security is the understanding of value in a corporate aspect and the perception that in business, a mandatory condition for the efficiency of a process is its profitability. In this regard, the cost of the company's security is directly related to the size of the possible loss.

Conclusions to the first chapter

1. The world's material and immaterial resources are concentrated in corporations, which is why they directly influence national and international security by generating transformational processes in social, labour, educational, production and consumer areas.

2. Each of the structural periods of globalization changes the concept of corporations and the models of ensuring their security.

3. The security of companies is directly dependent on management models, which must adapt to modern risks and changes in the environment.

4. The symbiosis and shared responsibility between the state and corporations is a necessary condition and factor for achieving national and corporate security.

Chapter Two. The new paradigm of corporate security

Chapter Two, "The New Corporate Security Paradigm" focuses on an analysis of the company's specific security threats. The concept of "risk" and the processes for its management, in the context of private economic entities, are explored. The main thesis defended in the research is defined that corporate security needs intelligent risk management solutions as a response to new risks and threats. Modern company security risks arising from global processes are identified and various possibilities for their classification are presented. The implementation of the overall process of risk management in companies is examined at three key organizational levels - at the corporate level, at the strategic business unit's level, and at the project level. Common and specific risks for each of the levels are identified and a taxonomy is established. Possible corporate security risk management models are presented, through synthesis and presentation of national approaches in the field and defined national requirements, improving the efficiency of processes and the interaction between corporate and national structures. Other good practices, international standards, with regards to risk management are also presented. The chapter is made up of three paragraphs, each of which is made up of two parts. This chapter fulfils the second research task.

The first paragraph, ***"Risk in the Context of Corporate Security"*** consists of two parts.

In the first part, the theory of risk is examined, with an analysis and synthesis of research in the field of the Bulgarian and foreign scientific communities, among which two directions stand out. The first considers risk through the lens of mathematical sciences, and the second direction emphasizes and considers risk as generated by and managed through the lens of social, cultural and symbolic specifics

of the environment and society. Today, one cannot talk about security without taking into account risk in its multifaceted nature. Security and risk in today's environment are inextricably linked. In recent years, a change in the positions of the main concepts has been observed. The concept of "security" tends to be replaced by the concept of "risk" in the strategic documents of both states and non-state actors.

Risk management is the process that should create a general framework related to corporate assets for timely countermeasures against negative consequences and their prevention. Of extreme importance, in the perception of risk in corporations, is the assessment of the company's key assets, which requires a mandatory commitment on the part of senior management. Only management is able to define the limits of the so-called "risk appetite" of the company, which is fundamental for the establishment of strategy and subsequent risk management policies.

It is concluded that corporate risks are all potential events that can have an impact on the final result to which the company strives.

In the second part, an analysis is carried out and contemporary risks to the company's security arising from global processes is identified. Options for the classification of the identified risks are outlined, presenting various social, legal, economic, environmental, political and technological aspects, creating a favourable environment for their occurrence. In general, as a result of the analysis, a fragmentation of the generic environment is reported, which is filled with many new and unconventional risks and challenges that both states and private economic entities face.

The second paragraph, *"Risk Management Process in Corporate Security"*, consists of two parts.

In the first part, the organizational autonomy that companies have in the process of building their security units and those for risk management in particular is reported. Variations are presented on the positioning of the risk management unit within the overall organizational structure, the decision to do so depending on both

the type of company and its size, as well as the culture of that company and its attitude to risk. For a risk management framework, to be effective, must include clearly articulated corporate procedures that provide clarity in relation to four key aspects – the risk management processes in the overall corporate structure and organizational activity; an risk management strategy supported by policies and risk-based solutions, as well as a specific allocation of responsibilities for them; transparency about the returns that risk management brings to the company; building and maintaining a risk culture in the organization.

The second part focuses on the challenge of defining the specific risks related to the different hierarchical levels of the corporate bodies, caused by the growing organizational complexity. In the dissertation, risk management in companies is divided into three key levels, which should ensure the minimization of possible negative consequences and, at the same time, provide opportunities for their management. This can be achieved by risk management at the corporate level, at the strategic business level (business unit level) and at the project level, starting from the practice in which each individual activity, in modern corporations, is carried out in the form of a project. The first, corporate level, embodies the company as a whole - its policies and vital decisions related to mergers, acquisitions, finances, etc. The second level is the level of individual strategic business units, which are responsible for the various directions – production, sales, placement, and affiliate units. The project level is the lowest, third level, in this hierarchical corporate structure. It supports strategic business units by implementing the necessary actions to achieve their goals. As a result of this conditional division of the levels at which risk should be managed in companies, the general and specific risks for each level were identified and a taxonomy was made, which is summarized below (table 1).

Table 1. General and specific risks for the security of the company.

Corporate level	**Strategic Business Unit level**	**Project level**
Aqcuisitions and financial risks	Lack of compliance between individual projects	Innovative
Monopoly by state-backed firms and various forms of extortion	Financial Risks	Technological
A model of corporate governance and ineffective corporate culture	Implementation delays - risks related to deadlines and not meeting the time frame	Resources
Counterfeiting of products	Changes in the external and internal environment	Cultural
Terrorism	Physical assets	Operational
Disregard of the interests of stakeholders	Human resources	Resulting from the end of the project or a specific related activity
Political risk	Legal responsibility and more specifically - tort law	
Regulatory and legal risk	Achieving and maintaining a competitive level in the the subject activity	
Technological risks and cyber attacks		
Health, Safety and Environment		
Reputational risk		

The third paragraph is entitled *"Possible models for risk management"* and also consists of two parts.

The first part presents national approaches to risk management. In this sense, the involvement of the state in the application of regulations to private economic entities has been identified as key in the processes of risk management in companies. Possible models for risk management in corporate security are presented, through the synthesis and presentation of national approaches in the field, and defined national requirements/recommendations/laws that improve the efficiency of processes and interaction between corporate and national structures. Examined practices include:

the United Kingdom, taking into account the importance of the Greenbury[20] reports of 1995; Hampel[21] from 1998; Alan Turnbull's[22] Report from 1999; the Higgs[23] from 2003, Smith[24] from 2005, and Tyson[25] from 2003 reports; the Kings College[26] from 2007; of the USA - Commission on Organizations - Sponsors of the Treadway Commission[27] (COSO) and the Sarbanes Oxley Act[28]; Cayman Islands - CIMA[29] and the Companies Management Act[30]. The four key elements in the 2014 OECD risk management and corporate governance model are presented, which are: Board of Directors, Board Committees (Risk, Audit Committees) and Chief Risk Officer/Risk Manager, together with their essential powers, duties and responsibilities.

The second part presents good international practices and standards in risk management in the area of corporate security.

The Six Sigma model is presented, which is one of the models for continuous improvement such as the Deming cycle, implemented in four steps, which represents the basis of a number of international standards, including those in the area of risk management. The model is applicable to any organization, regardless of the field of activity that wants to timely identify and eliminate errors in its activities. Six Sigma is implemented in five steps and can be achieved at six levels. It is a statistical model for making management decisions based on statistical analysis of quantitative data[31]. The method offers a set of tools that companies can use to reduce operational

[20] The Greenbury report, 1995.
[21] The Hampel Report, 1998.
[22] The Turnbull Report, 1999.
[23] The Higgs Report, 2003.
[24] The Smith Report, 2005.
[25] The Tyson Report, 2003.
[26] King's College Report, 2007.
[27] Committee of Sponsoring Organizations of the Treadway Commission.
[28] The Sarbanes–Oxley Act, 2002.
[29] Cayman Islands Monetary Authority.
[30] Companies Management (Amendment) Act, 2023.
[31] Cronemyr, P., 2007. Six Sigma Management: Action research with some contributions to theories and methods. Thesis for the degree of doctor of philosophy. Chalmers university of technology. Göteborg, Sweden

vulnerabilities, improve quality and profits, and improve the morale of organizational members.

There are many definitions of the method, but the concept generally boils down to Six Sigma being a process-oriented method, with input and output control. Six Sigma offers two main approaches/methodologies – DMAIC and DMADV. The first applies to the optimization and improvement of already existing business processes and projects, and can also be used to effectively manage change in organizations. The second approach - DMADV - is oriented towards the creation of completely new processes in the organization, and it could also be useful when there is a need to completely change existing ones that have been proven unsuccessful. The difference between the two approaches is expressed in the last two phases and is shown in Fig. 1.

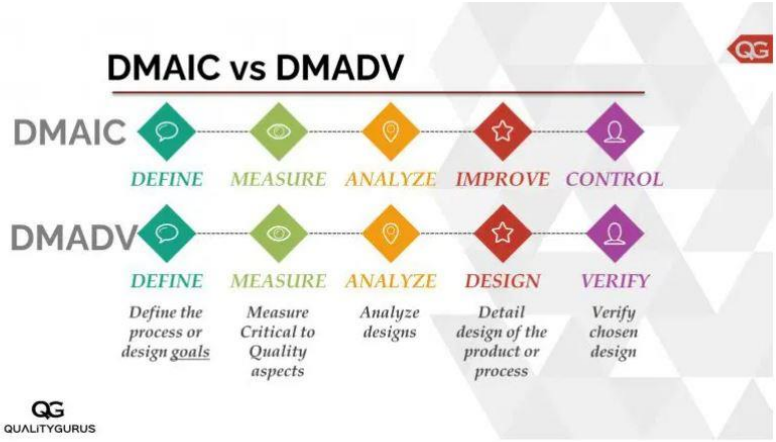


Figure 1. Differences and similarities between the DMAIC and DMADV approaches [32]

In addition to the model described above, this part presents standards and various collections of standards of the International Standardization Organization (ISO).

[32]Iztochnik: Difference and similarities between the Six Sigma DMAIC and DMADV methodologies: https://www.qualitygurus.com/difference-and-similarities-between-the-six-sigma-dmaic-and-dmadv-methodologies/. Poseten na: 12.09.2023.

One of the most popular and good practices for risk management in corporations is the ISO 31000:2018 Risk management - Guidelines standard, which is a widely and generally applicable standard for organizations with different areas of activity and purpose. Developed in 2011, the standard was updated in 2018, and ever since 05.10.2023 it continues to be operational. The 2018 update of the standard pays particular attention to the expanded scope of the concept and places a focus on the inclusion of all stakeholders and consideration of human and cultural factors. At the beginning of December 2023, a proposal was made to update the ISO 31000 collection of standards again. The change concerns an update of ISO 31000:2018, which remains at "draft" level, and Guide 73 of ISO: 2011, which is being withdrawn without being replaced by another document.[33] The standard is not a certification, but only gives guidelines to organizations and is does not make their subsequent implementation mandatory. In the current thesis this standard is not the subject of a detailed analysis, as it is widespread and well-known, and the current research aims to investigate risk management models that are less popular for the Republic of Bulgaria.

The ISO/IEC 21827:2008 standard specifies the Systems Security Engineering – Capability Maturity Model (SSE-CMM), which was initially developed in 2002 and subsequently updated in 2008, is also presented in a synthesis. The standard is a Security Engineering Maturity Model of the systems and provides a description of the basic characteristics of the security engineering process of a given organization.[34] It was developed based on the Capability Maturity Model, which is process-oriented.

[33]Balgarski institut za standartizatsia, Kolektsia ISO 31000 Upravlenie na riska: https://bds-bg.org/bg/project/show/bds:proj:115039; Noviyat standart ISO 31000 oprostyava upravlenieto na riska: https://bds-bg.org/bg/noviiat-standart-iso-31000-oprostiava-upravlenieto-na-riska_p3511.html. Poseteni na: 20.12.2023.

[34] ISO/IEC 21827:2008 Systems Security Engineering - Capability Maturity Model® (SSE-CMM®): https://www.iso.org/standard/44716.html. Last viewed: 21.08.2023.

Conclusions to Chapter Two

1. The priority risks for corporate security are generated by the accelerated pace of digital transformation, competition for talent, cybersecurity and innovation.

2. Building companies' ability to manage risks is vital to achieving overall corporate goals through change management and timely response.

3. Managing global risks related to the "health of the planet", the digital divide, the space race, the migration and refugee crises, is becoming an increasingly important factor with regards to the security of companies.

4. In the Republic of Bulgaria, there is a need to improve the regulatory framework and mechanisms in the field of corporate risk management.

5. To be reliable and effective, risk management processes must be constantly updated and adapted to the changing security environment.

Chapter Three. A systems approach to intelligent risk management in corporate security

Chapter Three - **"System Approach to Intelligent Risk Management in Corporate Security"** presents and analyses the organizational aspects of the company. The effectiveness of change management processes, the formation and maintenance of corporate culture, recognition of the company's stakeholders and respect for their interests, and corporate social responsibility as a management tool in risk management processes are identified as key to its functioning. The achievements of scientific and technical progress are considered as another organizational element. The main characteristics of some of the business-implemented automated solutions and those based on artificial intelligence, as well as military tactics tools adapted to business processes are synthesized and presented. Empirical research is conducted in the form of a survey, or the so-called "structured interview", as a result of which a theoretical model of risk management strategy in corporate security is proposed.

The first paragraph, ***"Organizational Aspects of Risk Management in Companies"*** consists of four parts.

The four parts outline the framework for a holistic approach that companies should apply to risk management. This approach is based on 4 (four) key processes in the organization:

- effective **change management** to achieve corporate sustainability;

- building and maintaining a **corporate culture** based on values and norms supporting risk management processes;

- assuming **corporate social responsibility** and respecting the **interests of the company's stakeholders** through transformation of business processes and turning companies into "corporate citizens";

- implementation of **automated solutions and those based on artificial intelligence** in corporate activities.

The effectiveness of change management processes, as well as the formation and maintenance of a corporate culture, which supports the provision of corporate security and risk management, are derived. The importance of recognizing the company's stakeholders and respecting their interests is reported and justified. Particular attention is paid to corporate social responsibility as a management tool in risk management processes. The achievements of scientific and technical progress are considered, as another organizational aspect.

The main characteristics of some of the automated solutions applied by the businesses and those based on artificial intelligence are synthesized and presented, and the advantages for companies of their implementation are deduced. The application of military tactics tools - CARVE(R) and FMEA - in modern corporate risk management is reported. Both tools enable a proactive approach to risk management in companies. Also introduced is the EDR (Endpoint Detection and Response) security system, also known as ETDR (Endpoint Threat Detection and

Response), which generally relates to the company's cyber security and is an integrated endpoint security solution.

The second paragraph, ***"Theoretical Model of an Intelligent Risk Management Strategy in Corporate Security"*** consists of two parts.

Within the framework of the **first part**, an empirical study is carried out in the form of a survey, or the so-called "structured interview". As a final result, after analysis and evaluation of the applicable corporate practices in the process of risk management in companies and the identified attitudes of employees towards security in the organization, gaps, challenges and emerging trends in the management of corporate risks are identified.

The survey provided to the respondents contains 24 (twenty-four) questions, with predetermined answer options - a structured interview. Some of the questions are also have the option of providing additional information/option to give answers, different from the set template. The goal is to obtain and report additional information that can serve as a supplement to the formulated survey framework and be the basis for future research and tracking of trends in the field. The survey was implemented online, through a questionnaire created using the Forms application on the Microsoft Teams platform. The survey was available to respondents for 14 (fourteen) days, for the period from 03.10 to 17.10.2023, at the link: https://forms.office.com/e/B66wqPPzU6. The questionnaire was filled out anonymously, and the information provided by the respondents is used only in a summarized form for the purposes of this dissertation.

In the survey participated 100 (one hundred) respondents, professionally engaged in various areas of corporate activity and occupying various positions in the hierarchical levels of the organizations in which they work.

As a result of the research analysis, the presence or absence of correspondence between the presented theoretical framework and its applicability by companies in practice and risk management processes had to be established. When analysing the

results, the fact that some of the respondents do not answer some of the questions is taken into account, which leads to a numerical discrepancy in the number of answers given and their percentage ratio. In this regard, the percentage ratio to the answers to each question is based on the number of answers given to it.

The research shows that the respondents who noted the presence of internal corporate strategic documents and report the fact that they are fully familiar with them are part of companies in which modern digital technologies and systems have already been implemented. These respondents assess digitization processes as an opportunity for companies and believe that smart technologies can significantly improve risk management processes in organizations. They also participate, or have participated once a year or more, in risk management training. This confirms the thesis that the availability of organizational rules and procedures, and their effective communication through intra-corporate networks/systems, leads to their understanding and implementation in practice, as well as to avoiding resistance from employees. Moreover, judging by the feedback from the respondents who shared the availability of internal corporate documentation, a high percentage of positive responses was observed towards the application by and alignment of companies with international/national standards that support risk management. The existence of an established risk culture among the company's employees is reported by a large percentage of the latter as an element that has a positive impact on the company's risk management processes.

The biggest weakness of modern companies, based on the results of the conducted research, is the recognition of interested parties (beside customers) and the need for respect for their interests. Other weaknesses that can be reported are ineffective corporate culture and general low awareness of employees about rules, procedures, and standardization framework regarding risk management processes in companies.

In the **second part**, a theoretical model of Risk Management Strategy for corporate security is proposed, within the scope of which fall the organizational aspects presented above, the achievements of scientific and technical progress and artificial intelligence, without neglecting the material and purely financial dimensions of the processes in risk management. The theoretical model offers a recommended structure and content of a Risk Management Strategy for corporate security in 9 (nine) main points:

1. Introduction

Every strategy should start with an introductory part that aims to clarify the issues related to the company's fundamental concepts regarding its existence. In this sense, the introduction of the risk management strategy must necessarily contain a description of the following components:

- A *mission* expressing the importance of its existence.

- A *vision* outlining the desired future state.

- The main *principles and values* that guide the organization and that are the basis of its functioning in the form of written and unwritten rules or the so-called corporate culture.

- *Scope* of the strategy, outlining the framework of implementation of the strategy and all persons bound in its implementation. This scope serves as a basis for developing subsequent procedures and policies for interaction with all stakeholders, which must necessarily be taken into account within the strategy.

- The *leading unit*, within the corporate structure, which is responsible for the implementation of the strategy and subsequent control. The persons involved in the process should be indicated here, with their roles, duties, powers and responsibilities.

- *Duration of the strategy*. Each strategy has a period of validity, and from the point of view of the time frame, the strategies can be short-term - up to 1 year; medium-term - 3-5 years and long-term - 6-9 years. The given time frames are conditional, as the theory suggests different time intervals for different strategies,

based on the time frame. In view of the constantly changing environment, the current model proposes that the risk management strategy should be valid for no more than 5 years, with an annual review and, if necessary, an update. The strategy can be updated beyond the stated timeframe, in view of the dynamism of the environment and the establishment of circumstances that necessitate its inevitable changes. For greater flexibility, the organization is recommended to develop strategy-related implementation plans that set clear deadlines for the strategy period. Along with the strategy, other guiding documents called policies are developed, which reflect the management's vision for certain processes in the organization.

The mission, vision, values and principles stated in the risk management strategy must necessarily be in line and in harmony with those laid down in the general corporate strategy.

2. Defining the main concepts in the document

In order for it to be understood by all interested parties, it is advisable to provide the main terms used, as well as their definitions at the establishment of the strategy. This part can also be designed as a separate "glossary of concepts". This is necessary because the theoretical framework defining risk management is rich and the lack of such a glossary could lead to different interpretations.

- *Strategy* - the definitions of the term "strategy" are numerous and related to the object to which they are directed. Therefore, in the general organizational strategy and in the strategies derived from it in the individual organizational areas, it must be clearly defined what is meant by this concept in the organization, by clearly delineating its framework.

- *Policy* – determines the way the organization operates in different areas of its life cycle, which lead to the achievement of the company's strategic goals.

- *Program* – a brief description of the ideas arising from the established policies and an outline of the necessary activities that should be implemented.

- *Implementation plan (roadmap)* – clearly defining specific activities and the time for their implementation in a way that will support the overall strategic goals. As described above, they are developed for shorter time frames (1-2 years), which allows greater organizational flexibility and easier adaptation to changes. Plans are also called "road maps", that is, documents that describe the step-by-step implementation of the set program.

- *Risk* – for strategy purposes, organizations could use the definition of "risk" given in the ISO 31000 "Risk Management" standard, which states that it is the impact of uncertainty on the achievement of objectives.

- *Risk appetite* – risk appetite is expressed in the amount and type of risk that the organization is willing to take in order to achieve its long-term strategic goals.

- *Risk tolerance* - outlines the boundaries that the company is not ready to cross in order to achieve its strategic goals. These may be assets that the organization is unwilling to sacrifice and therefore must find another, safer way to achieve its goals.

- *Risk management* - an example definition that companies can refer to in their glossaries is that of the US Corporate Governance Council handbook, according to which Risk Management in a company helps it, in a risky environment, to be able to achieve its business objectives; to articulate its view of value; assess its risk tolerance; and to design its processes, taking into account the reasonable expectations of stakeholders.[35]

- *Stakeholders* – these are all individuals, groups, communities, etc. who can influence or be influenced by the company's activities. They can be both external and internal to the organization. Organizational recognition of these parties is of utmost importance for risk management. Unfortunately, the main weakness of the

[35] Risk Governance Guidance for Listed Boards, Corporate Governance Council, May 2012

companies is precisely the process of identifying and considering the interests of these parties.

- *Key assets* - these are all corporate assets - tangible and intangible, which are vital for the company and without which it cannot function and, therefore, achieve its goals.

- *Compliance* - bringing it into line with existing legislation or requirements in various areas of activity of the organization's life; relationship between required norms and their implementation/application within the organization.

3. Analysis of the environment

The methodology for strategic planning in the Republic of Bulgaria[36] gives a good scope and a clear description of the analysis of the environment, and in addition to taking into account the main components of each system, this analysis should provide an objective assessment of the state in which the organization is at a given point. The purpose of the analysis is to get a clear idea of where the company is at the time of its preparation, what are the main characteristics of the environment and what are the new facts and circumstances that the organization should take into account. The analysis is the starting point that should be used for setting goals by the company and making management decisions in the process of goal achievement. Its result is a basis for developing programs, policies and plans in such a way that they are applicable and effective against the background of the surrounding environment - internal and external to the organization. It is recommended that such an analysis be performed periodically (at least once a year), or in case of force majeure circumstances that require a change in the strategy or one of its key components.

A number of analytical methods and those for subsequent assessment of the environment are available, such as GAP analysis, SWOT analysis, PESTE and others. Environmental analysis is a means of tracking the development of already

[36] Metodologiya za strategichesko planirane v Republika Bulgaria, 2010.

identified risks and the discovery of potential new ones, which the company should classify and prioritize based on the assets to which they are addressed. In addition to the information already described, analysis can also be used to detect opportunities by identifying characteristics of the environment that can favourably influence the achievement of corporate goals if detected in time.

4. Objectives of the strategy

The aim of the corporate security risk management strategy is to ensure the protection of all corporate assets, with full regulatory compliance of the company's processes, with an emphasis/priority on:

- *The environment* – by achieving environmental efficiency and managing environmental risks.

- *Information and intellectual resources* - as the main object of attacks.

- *The implementation of automated solutions in the corporate processes of risk management* - as a means of generating fast and effective solutions, thanks to their unprecedented capabilities for processing and analysing huge amounts of data.

- *Taking responsibility for ongoing social processes and achieving sustainability* – application of good practices in the field of corporate social responsibility and equal working conditions.

- *Formation and maintenance of a security culture in the company* – as a tool of corporate security and risk management processes, by attracting the human factor to achieve common organizational goals and building loyalty to the company.

5. Stages of strategy implementation

With regards to the effectiveness of the strategy, the present theoretical model proposes the following basic stages for its implementation, based to some extent, but not entirely, on the famous Deming Cycle. The concept was introduced in the 1950s in Japan, and nowadays it is widely used to improve processes and manage various changes in organizations. The Plan-Do-Check-Act (PDCA) cycle is a four-step continuous model, the steps of which are constantly repeated, thus ensuring the

effectiveness of the intended processes. The Deming cycle can also be referred to as Plan-Do-Study-Act (PDSA).

- *Development of policies*, procedures and rules for risk management in the company, addressed to the key assets.

- *Communicating* with internal and external stakeholders by conducting informational meetings and campaigns.

- *Approving* the strategy during its initial introduction and subsequent updates.

- *Corrective actions* – introduction of mechanisms for monitoring and accountability at the stages of implementation, as well as taking corrective actions if necessary.

6. Monitoring and control of the overall implementation of the strategy.

In this step, rules should be formulated to track the implementation of the formulated strategy as a whole and the effectiveness of its planned stages. The persons responsible for the implementation of this step of the strategy should create internal corporate mechanisms to carry out checks for compliance with the established risk management procedures and the degree of their adoption by the organizational members. This part of the strategy can envisage different types of simulations in order to track the degree of adoption and adequate application of the scheduled procedures. The monitoring also aims to track the transparent and effective use of the financial resources allocated for the implementation of the activities under RM activities. Accountability methods can also be defined, such as annual reports and others.

7. Financial provision of the activities of the risk management strategy

The financial provision of the activities can be in the form of a prepared budget framework, which is directly linked to the set strategic goals and priority areas. It must contain a detailed description of the activities and the value of their financial dimensions, as well as the units/organizational structures involved in their implementation. The implementation of risk management activities is resource-

intensive, which requires a very good justification of the budget to be approved already in the strategy preparation process. It should include all necessary resources, along with their quantitative and qualitative valuation. Input indicators should be established, on the basis of which to measure the resources necessary for the implementation of the activities, as well as output indicators, which will serve to evaluate the implementation of the budget.

8. Expected results of the implementation of the strategy

Any corporate security risk management strategy should outline the results that are expected to be achieved from its implementation. It is these results that outline the difference between the analysis of the environment, i.e. the current state of the company and the change that should occur after implementing the activities foreseen in the strategy. Expected results should reflect a change in the status of all stakeholders. In addition, they must be documented through quantitative, financial and qualitative data, taking into account, with the greatest possible accuracy, the degree of satisfaction of the interested parties - internal and external.

9. Applications

The theoretical model allows to create appendices of the strategy that provide additional information on its implementation. In the "Appendices" section, corporate templates for reporting and other activities can be developed to unify internal corporate documentation. Here, for example, as an appendix, step 2 of the current theoretical model - "Glossary of Basic Concepts" can be singled out.

As open systems and social organizations, companies develop a set of rules to serve as a starting point for management decisions. The achievement of general organizational goals should be achieved within a predetermined framework. In this sense, both the activity of the companies as a whole and the risk management processes in them need a general and comprehensive guide that outlines the way to minimize the potential negative impacts of the environment. Today, it is impossible

to maintain the life cycle of an organization if it does not have a risk management strategy.

Conclusions to Chapter Three

1. The new paradigm for corporate security requires taking into account the interests of stakeholders and the new characteristics of the environment, which increasingly have social, legal, technological and environmental dimensions.

2. The implementation of models based on automated decisions and artificial intelligence leads to a change in decision making, provoking an evolution of established practices for identification, analysis and assessment of risks.

3. Military tactics tools from the military field are adapted to modern business processes and find their application in corporate risk management to satisfy the security needs of companies.

4. A challenge for companies is to motivate employees for proactive behaviour regarding new risks and threats.

5. The trend of increasing attacks on intangible corporate assets requires effective risk management through new models, with an emphasis on technological and social tools.

III. GENERAL CONCLUSIONS AND RECOMMENDATIONS FROM THE THESIS

3.1. General conclusions

1. The security of companies is a shared responsibility among all members of the organization, and the basis of its provision is the management model, through which adaptation to changes and protection of all corporate assets is carried out.

2. In view of modern risks, the approaches to their effective management should be based on the interaction and mutual engagement between the structures of the national security system and the corporate security units in the companies.

3. For effective risk management, it is fundamental to have internal corporate documentation that defines company risk management processes and the responsibilities of all interested parties.

4. Military tactics tools adapted to business processes, established national requirements, various national/international standards are successfully applied in risk management.

5. The role of predictive analytics is growing as a key activity in corporate risk management and, together with artificial intelligence-based systems, it increases the effectiveness of risk management and strategic decision-making in companies.

6. Intelligent decisions to achieve the organization's strategic goals must be subordinated to the collaboration between the intelligence resulting from scientific and technological progress and the intelligence inherent to man.

7. Modern risk management strategies in corporate security must form a holistic approach, in which the main emphasis should be on building capabilities to achieve sustainability through effective change management processes; the implementation of socially responsible practices and recognition of all stakeholders; building an effective corporate culture and implementing automated solutions in risk management processes.

3.2. Recommendations

As a result of the present study, the following recommendations can be made:

1. To establish government recommendations for the creation of risk management committees or other internal corporate bodies, providing for motivational measures for their implementation by companies.

2. To enlist corporations and representative employer and class organizations as active participants in the process of developing a unified government policy on risk management.

3. To popularize government policies in the field of corporate social responsibility.

3.3. Conclusion

The impact of the corporate world on public, economic, political and social life, as well as on environmental aspects, calls into question the existing risk management models and practices. This necessitates the construction of a new paradigm, which in a much broader aspect takes into account the characteristics of the environment and the attitudes of all interested parties and applies a new, intelligent framework of risk management mechanisms. The new conditions require not only a protective approach, but also greater activity against the increasingly unpredictable attacks, which are implemented using increasingly sophisticated methods, thanks to modern technologies.

Today, automated risk management tools are extremely widely used in various areas of the corporate world. The drive to optimize costs and time, by replacing the human factor and applying technological solutions for the implementation of various functions, achieves its success in terms of risk management processes, but at the same time, precisely this technological progress increases the vulnerability of companies. The risks to the security of corporate assets and the damage that can be caused by the use of artificial intelligence are a field of current research that will gain more and more relevance with the deepening processes of implementing these solutions in various areas of activity.

In the overall framework of the organization, risk management has both operational and strategic importance. In order to achieve the higher goals of the company, the security and risk management strategy must be synchronized with the overall organizational strategy. The opposite would lead to non-productivity and the impossibility of effective and efficient protection of corporate assets. The process of synchronization in the organization reflects the method of coordination between its constituent elements in such a way that each of them is integrated in the achievement of corporate goals, the distribution of resources. It should be reflected by the corporate culture, and should participate effectively in organizational activities. For

the corporate security activity to be successful, at the senior management level, steps should be taken on strategic analysis, development and subsequent implementation of the risk management strategy.

Apart from the achievements of scientific and technical progress, today's risk management cannot fail to take into account the company's intangible assets, which must be emphasized in the development of risk management strategies. Formed as the main target of attacks, the reporting of these assets is mandatory in order to identify and subsequently manage today's corporate risks in greater detail and depth.

3.4. Scientific and scientific-applied contributions

Scientific contributions

1. A new paradigm of corporate security is defined. The thesis of the need for symbiosis between national and corporate security and shared responsibility for their achievement is substantiated.
2. Risk management is conceptualized as a problem of companies' security in the modern operational environment. New content and dimensions of effective management of modern corporate risks are defined.

Scientific-applied contributions

1. The current security risks of the company are identified, and they are analysed and classified at the level of the corporation, strategic business units and at the project level.
2. A comparative analysis of international "good practices" of corporate security risk management is made and their applicability assessed.
3. A theoretical model of Risk Management Strategy for corporate security is developed, based on empirical research, which defines the new factors for effective security management in companies.
4. Recommendations are formulated for improving and increasing the effectiveness of risk management processes in companies.

3.5. Scientific publications relevant to the thesis

1. Mladenova, M., 2019. Article: Corporate Culture: The Invisible Competitive Advantage. Military Journal, № 3/2019, pp. 108 – 113. Sofia: “Georgi Stoykov Rakovski” National Defense College. ISSN 0861-7392.

2. Mladenova., M., 2020. Scientific report: The Use of Personal Devices in the Organization and Security Risks. In: Proceedings of the "Security - Education, Science, Industry" International Scientific Conference, Part One, pp. 191 - 194. Sofia: "Georgi Stoykov Rakovski" National Defense College. ISBN 978-619-7478-57-0.

3. Mladenova., M., 2022. Scientific report: Corporate Social Responsibility as a Tool of Corporate Security. In: collection of reports from the Annual Scientific Conference of “G.S.Rakovski” National Defence College - "110 years of Tradition, Quality, and Prestige", April 12 - 13, 2022, Part One, pp. 163 - 167. Sofia: "Georgi Stoykov Rakovski" National Defense College. ISBN (online): 978-619-7478-93-8.