ВОЕННА АКАДЕМИЯ „ГЕОРГИ СТОЙКОВ РАКОВСКИ”
1504, София, бул. „Евлоги и Христо Георгиеви” № 82,
тел. 02 92 26 501
e-mail: rnda@md.government.bg

ФАКУЛТЕТ „НАЦИОНАЛНА СИГУРНОСТ И ОТБРАНА”
КАТЕДРА „ПОЛИТИКИ, СТРАТЕГИИ И ОТБРАНИТЕЛНО ПЛАНИРАНЕ“

БОРЯНА КАЛЧЕВА ХИНОВА

ТЕМА:

СЪВРЕМЕННИ ИЗМЕРЕНИЯ НА СИГУРНОСТТА НА ИНФОРМАЦИЯТА В ДЪРЖАВНОТО УПРАВЛЕНИЕ

АВТОРЕФЕРАТ

На дисертационен труд за присъждане
на образователна и научна степен „доктор“
по научна специалност
„Организация и управление извън сферата на материалното производство
(Управление на сигурността и отбраната)“

Научен ръководител - Професор доктор Лидия Стоянова Велкова
Научен консултант - Полковник доцент доктор Георги Димитров Димов

Рецензенти:
1. …….
2. …….

СОФИЯ, 2020

Дисертационният труд е обсъден на катедрен съвет на катедра „Политики, стратегии и отбранително планиране“, факултет „Национална сигурност и отбрана“, Военна академия „Георги Стойков Раковски“, гр. София на 30.06.2020 г. и е предложен за защита пред научно жури.

Авторът е докторант в същата катедра. Изследванията и разработването на темата са извършени във Военна академия „Георги Стойков Раковски“ и в качеството на докторанта като сътрудник в Народното събрание на Република България.

Дисертационният труд е с обем 189 стандартни страници, в т. ч. 12 фигури и 2 таблици. Съдържа списък на използваните съкращения, увод, изложение в три части, заключение, използвана литература включваща 160 източника.

Брой на публикациите по дисертацията - 3.

Защитата на дисертационния труд ще се състои на …….. 2020 г. от _____ ч. в зала _____ на Военна академия „Г. С. Раковски“.

Материалите по защитата са на разположение на интересуващите се в стая № _____на Военна академия „Г. С. Раковски“ - София, тел. _____

Автор: Боряна Калчева ХИНОВА

Тема: „Съвременни измерения на сигурността на информацията в държавното управление“

Тираж: _____

Отпечатан на _____

I. ОБЩА ХАРАКТЕРИСТИКА НА ДИСЕРТАЦИОННИЯ ТРУД

В центъра на динамичните процеси от началото на XXI век се оказаха информационните технологии, които навлязоха във всички сфери на обществения живот на човечеството и предизвикаха глобална интеграция на информационното му пространство. Последните десетилетия от развитието и използването на информационните технологии в световен мащаб са белязани с настъпването на съществени промени в обществените отношения. От една страна, новите отношения носят на държавното управление съществени изгоди, но едновременно с това все повече насочват фокуса на ангажираните субекти към гарантиране сигурността на информацията от страна на правителството, бизнеса и различните организации и частни потребители, които разработват, владеят или обслужват съвременните информационни системи.

Методите за информационно осигуряване на системите за държавно управление датират още от времето, когато всяка управленска система е била затворена в рамките на професионалните си потребности. В днешния глобален свят, в който информацията е основен ресурс, а съвременните държави са изправени пред предизвикателствата да гарантират сигурността си като съществено условие за успешното си функциониране и запазване на националния си суверенитет, тези методи не могат да осигурят необходимото ефективно държавно управление. Съвременната информационно-комуникационна епоха поражда сложна взаимозависимост и обвързаност на всички жизненоважни за съществуването на обществото инфраструктури, което води до експоненциално нарастване на уязвимостите и рисковете за тяхното функциониране. Ето защо информационната сигурност се превръща в едно от най-важните предизвикателства на XXI-ви век и все повече се разглежда като съществен национален проблем, който засяга всички нива на обществото. В аспекта на възникналите пред държавното управление проблеми се поставя националната политика по информационна сигурност, която е призвана да даде отговор на новите предизвикателства и да гарантира сигурността в информационното общество.

Всяка държава осъществява функционирането и управлението си чрез система от дейности и посредством балансирано взаимодействие между държавните институции. В рамките на този механизъм протичат вътрешните процеси, свързани с гражданите и обществените отношения, и се формират външните процеси, свързани с международната политика и междудържавни отношения. Държавните органи се намират в определени връзки и отношения, като формите на държавното управление показват степента на тяхното

структуриране и интегриране в управлението на държавата. От своя страна, формите на държавно управление показват начините за организиране на висшите органи на властта в държавата и тяхната структура, принципите, които са залегнали в основата на взаимодействието между държавните органи и механизмите за осъществяване на комуникацията между върховната власт и гражданите. Съществено място при функционирането на органите на държавното управление има гарантирането и зачитането на основните права и свободи на гражданите.

Така поставен въпросът за управлението на държавата[1] има като основна мисия гарантирането на демократичните й устои и на държавността. Това не би могло да се осъществи, ако не бъдат гарантирани и защитени териториалната цялост, суверенитет и конституционен ред, демократичното функциониране на институциите и основните права и свободи на гражданите, за да може нацията да се развива и увеличава своето благосъстояние, а страната успешно да защитава националните си интереси и да реализира националните си приоритети. В обобщение това означава да бъде гарантирана и защитена националната сигурност на държавата.[2]

Днес е постулат, че държавата има жизненоважна роля за осигуряване и защита на националната си сигурност. Тя е главен фактор и носи отговорност, както за сигурността на отделния човек, така и на обществото като цяло. Националната сигурност стои в основата на изграждането на държавните политики и концепции за развитие на страните. В съвременния глобализиран свят защитата на сигурността на обществото и гражданите, опазването на териториалната цялост и отстояване на националните интереси, са сред главните приоритети на всяка една държава. Новите тенденции и процеси в средата за сигурност предполагат необходимостта от добро взаимодействие между ангажираните държавни институции и обществото за постигане и поддържане на стабилност в системите за национална сигурност, като чрез тези връзки ще се способства за изграждането и реализирането на добри политики за сигурност на национално и международно равнище. В толкова сложна

---

[1] „Строеж на държавата днес означава създаване на нови институции за управление и укрепване на вече съществуващите.” Фукуямя, Ф. Строежът на държавата, С., „Обсидиан”, 2004, с. 9.

[2]Закон за управление и функциониране на системата за защита на националната сигурност (УФСЗНС), в сила 01.11.2015 г., обн. ДВ, бр.61 от 11 август 2015 г.

социална система, каквато е системата за защита на националната сигурност, именно държавата е главният фактор.[3]

В тази връзка информационната сигурност в информационната епоха се явява един от най-важните компоненти на националната сигурност на държавата, защото информационното пространство е мястото, където се осъществяват основните социални дейности в съвременното общество. Свободният и безопасен достъп до информационното пространство, сигурността и защитеността на циркулиращите в обществото и отделните организации информационни потоци са от жизнено значение за осигуряване на възможностите за развитие и просперитет на отделната личност, обществото и държавата като цяло. От своя страна, тези сложни обществени процеси изискват формиране на нова регулационна рамка за гарантиране на информационната сигурност в управленски, организационен и програмно-технически аспект. Те изведоха на дневен ред въпроса за разработка на ефективни политики, правила и процедури за информационна сигурност и защита на класифицираната информация в органите на държавното управление. Това постави нови предизвикателства пред политиката за сигурност, която обхваща не само общите насоки и приоритетите на държавното управление, но и отделните секторни политики и съставящите ги компоненти.

Днес повече от всякога е необходимо изграждането и поддържането на съвременни информационни системи, чрез които субектите, участващи в процесите на управление на държавата, да могат да получават необходимия информационен ресурс за вземане на ефективни управленски решения. Днес, повече от всякога, информационната сигурност придобива първостепенно значение в съвременната държава, която се оказва изправена пред предизвикателството да промени съществуващите механизми за нейното обезпечаване, като съществено условие за успешното си функциониране и запазване на националния си суверенитет. Именно затова органите на държавната власт приоритетно разглеждат ролята на информационната сигурност като ключов фактор за гарантиране на успешното държавно управление, включително и поради усилване на заплахата от използването на тази сигурност като „информационно оръжие“. Това предопределя необходимостта от решаване на проблемите, свързани с нарастващите вероятности за „информационна война“, негативни информационни въздействия върху индивидуалното и общественото съзнание и психика на

[3] По въпроса виж Казаков, К. Управление на системата за защита на националната сигурност. С., „Софттрейд”, 2016.

хората, на комуникационните и информационните системи и други източници на информация.

Актуалността на темата на дисертационното изследване е безспорна и нейната значимост се прояви особено силно в условията на кризисно състояние на обществото и държавата и необходимостта от търсенето на възможности за повишаване на качеството на мениджмънта на информационната сигурност в държавното управление. Това породи необходимостта от настоящото изследване, което е обусловено от следните обстоятелства: На първо място, за успешното решаване на практическите задачи в управлението, повишаването на ефективността на изпълнителната, съдебната и законодателната власт, от изключително значение е системите за държавно управление да разполагат с пълна и достоверна информация, да умеят правилно да я използват и умело да боравят с нея. На второ място, процесите в държавното управление предвид тяхната сложност, могат да бъдат умишлено блокирани посредством различни способи, в това число и политически, с цел да бъдат предизвикани недействителни представи за протичащите в държавата процеси, промените в социално-икономическото, културното, демографското и пр. развитие, състоянието на вътрешната среда и международната обстановка и т.н.

Степен на разработеност на проблематиката: Проучените литературни и нормативни източници в областта на мениджмънта на информационната сигурност сочат за наличието на недостатъчно изследвана ниша, свързана с необходимостта от целенасочена политика по отношение на ефективното управление на информационните процеси в държавата, насочени към повишаване равнището на националната сигурност. Това ни позволява да направим констатацията, че в своята цялост избраният от нас проблем е слабо изследвана тема сред ангажираната научна общност в България. Като водещ приоритет на направените анализи и проучвания са самата информационна сигурност и същността на информацията в различни сфери от обществения живот на страната, а управленските процеси, които всъщност са основните градивни елементи на тази система, са останали встрани от фокуса на изследователите на проблема. Теоретичната и методологична основа за такива изследвания все още не са разработени и разкрити в цялост, което прави разглеждана тема съществено важна от гледна точна на нейния значим, сложен и противоречив характер.

Обект на изследването в дисертационния труд е държавното управление като информационна система.

Предмет на изследването са организационно-правните характеристики на информационната сигурност в системата на държавното управление като елемент от защитата на националната сигурност.

Основната хипотеза на дисертационния труд е, че държавното управление може да бъде разглеждано като система от информационни процеси, които за да функционират безпроблемно, е наложително да бъдат надеждно защитени, за да се гарантира качеството на информацията, използвана за генериране на адекватни управленски решения. Това налага в механизмите за стратегически мениджмънт на държавата да се създаде система за контрол и ефективно управление на информационните процеси, което да гарантира информационната сигурност при управлението на възникнали кризи, като елемент от защитата на националната сигурност на страната, с което ще се постигне ограничаване на негативните им последствия или тяхното пълно неутрализиране.

В Република България досега не е разработена и не се прилага подобна комплексна система за мониторинг и контрол на информационната сигурност при възникването на кризи, в резултат на което съществува сериозна заплаха за качеството на вземаните решения при тяхното управление.

Целта на изследването е да се очертае състоянието на информационната сигурност в държавното управление и да се разработят организационни и правни мерки за повишаване на ефективността на управленските процеси чрез реализирането на интегрирана система за мониторинг и контрол на информационната сигурност при възникнали кризи, като елемент от защитата на националната сигурност на страната.

За постигането на така формулираната цел в дисертационния труд са поставени следните **научноизследователски задачи:**

1. Да се изследват същността, основните понятия, характеристики и елементи на информационната сигурност при формирането на обществените отношения в държавата.

2. Да се анализира ролята и мястото на информационната сигурност в държавното управление, методите и средствата за нейното гарантиране в обществените системи.

3. Да се изследват същността и основните характеристики на стратегическите дейности и обекти при реализиране на държавното управление като елемент от националната сигурност на страната.

4. Да се изследват принципите, характерът и типологията на процесите в управлението на държавните органи и състоянието на информационната

сигурност на страната и да се представят способи и мерки за нейното подобряване в органите на държавната власт при управлението на кризи.

5. Да се предложат препоръки за повишаване качеството на държавното управление при защитата на информационната сигурност като елемент от националната сигурност на страната.

Структурата на дисертационния труд е ориентирана към поставените задачи, като резултатите от изследването са изложени в увод, три глави и заключение.

Методологична база на изследването. В процеса на научното търсене в дисертационния труд е приложена обща и специална методология на изследването. *Общият методологичен апарат* включва разнообразни теоретични методи за изследване, прилагани в теорията на познанието, като системен анализ и синтез, диференциращ, системно-интегриращ, исторически и синергичен подход и др. Използвани са класическите *изследователски методи,* включващи обзор, събиране, обработване, обобщение и анализ на научната литература с цел систематизиране на информацията за основните научни понятия, които кореспондират с дисертационната проблематика и служат за изграждане на теоретичната база на изследването, както и други широко прилагани методи на научното познание - наблюдение, сравнение, анализиране, синтезиране, теоретични обобщения, формализация и др. Поставените хипотези в доказателствената част на дисертационния труд са решени чрез прилагането на SWOT анализ. SWOT анализът е използван като комплексен метод на стратегическия анализ, с помощта на който са изведени общите характеристики и е представено състоянието на мениджмънта на информационната сигурност в държавното управление при функционирането и взаимодействието на ангажираните държавни органи от системата за национална сигурност на страната, като са дефинирани и съответните препоръки за неговото усъвършенстване. За провеждане на емпиричното изследване е използван и функционално-структурният анализ като инструмент за изследване на дейността и взаимодействието на държавните органи от системата за национална сигурност. В резултат на него са определени функциите, процесите, организационните структури и информационните потоци, възникващи при взаимодействието на елементите от разглежданата система. В хода на анализа са използвани теоретични и методологични положения, български и чуждестранен опит при анализиране на протичащите информационни процеси в сигурността на страната и управлението и функционирането на системата за защита на националната й сигурност.

II. ОБЕМ И СТРУКТУРА НА ДИСЕРТАЦИОННИЯ ТРУД

Дисертационният труд е с обем 189 стандартни страници, в т.ч. 12 фигури и 2 таблици. Съдържа списък на използваните съкращения, увод, изложение в три части, заключение и библиография от 160 източника (93 литературни източника на кирилица, 14 на латиница; 38 нормативни документа; 12 източника от Интернет).

Дисертационният труд е структуриран в следната последователност:

УВОД

ГЛАВА ПЪРВА

СЪЩНОСТ И РОЛЯ НА ИНФОРМАЦИОННАТА СИГУРНОСТ
В СЪВРЕМЕННИТЕ ОБЩЕСТВЕНИ ОТНОШЕНИЯ

1. Концептуални основи на информацията в контекста на информационната сигурност

1.1. Основни характеристики на понятието „информация“

1.2. Структурно определящи елементи на информацията

1.3. Функции и качества на информацията като инструмент за въздействие на обществените отношения

2. Основни аспекти в процесите на разпространение на информацията

2.1. Стойност и качествени параметри на информацията

2.2. Материални измерения на информацията

2.3. Пространствени форми за разпространение на информацията

3. Доктринални основи на информационната сигурност

3.1. Същност и място на информационната сигурност в обществените отношения

3.2. Информационна сигурност и защита на обществените системи

3.3. Методи и средства за гарантиране на информационната сигурност

ИЗВОДИ ОТ ГЛАВА ПЪРВА

ГЛАВА ВТОРА

ДЪРЖАВНОТО УПРАВЛЕНИЕ КАТО ЗАЩИТАВАНА СИСТЕМА
В ПРИОРИТЕТИТЕ НА НАЦИОНАЛНАТА СИГУРНОСТ
НА СТРАНАТА

1. Стратегически дейности при реализиране на държавното управление

2. Стратегическите обекти на държавното управление като елемент от Системата за национална сигурност на страната

3. Основни аспекти на държавната политика за гарантиране на информационната сигурност

3.1. Принципи за осъществяване на информационната сигурност в рамките на държавното управление

3.2. Характер и типология на процесите на управлението на държавните органи

3.3. Основни аспекти от състоянието на информационната сигурност на Република България

ИЗВОДИ ОТ ГЛАВА ВТОРА

ГЛАВА ТРЕТА

МЕХАНИЗМИ ЗА ОПТИМИЗИРАНЕ НА ИНФОРМАЦИОННАТА СИГУРНОСТ В ДЪРЖАВНОТО УПРАВЛЕНИЕ

1. Методи и изследвания, приложени при изучаване състоянието на информационната сигурност в държавното управление

1.1. SWOT-анализ на състоянието на информационната сигурност в процесите на управление на държавата

1.2. Преглед и обобщение на резултатите от SWOT анализа

2. Информационната сигурност в процесите на държавното управление при кризи

2.1. Управлението при кризи като елемент от защитата на националната сигурност на страната

2.2. Основни аспекти на политиката за информационна сигурност при управлението на възникнали кризи

3. Оптимизиране на механизмите на държавното управление при защита на информационната сигурност като елемент от националната сигурност на страната

3.1. Способи и мерки за подобряване на информационната сигурност в органите на държавната власт при управлението на кризи

3.2. Мониторинг и контрол на процесите за гарантиране на информационната сигурност при взаимодействието на държавните институции при управлението на възникнали кризи

3.3. Препоръки за подобряване на държавното управление при защитата на информационната сигурност

ИЗВОДИ ОТ ГЛАВА ТРЕТА

ОБЩИ ИЗВОДИ

ЗАКЛЮЧЕНИЕ

ИЗПОЛЗВАНА ЛИТЕРАТУРА

III. СЪДЪРЖАНИЕ И РЕЗУЛТАТИ ОТ ИЗСЛЕДВАНЕТО

УВОД

В увода е представена и обоснована значимостта и актуалността на темата за мениджмънта на информационната сигурност в държавното управление, представени са целта, основният проблем, обектът, предметът, водещата хипотеза, задачите за проверка на хипотезата, подходът и методология на изследването, както и степента на разработване на проблематиката.

ПЪРВА ГЛАВА

СЪЩНОСТ И РОЛЯ НА ИНФОРМАЦИОННАТА СИГУРНОСТ В СЪВРЕМЕННИТЕ ОБЩЕСТВЕНИ ОТНОШЕНИЯ

В първа глава са решени първите две научно-изследователски задачи на дисертационния труд – изследвани са същността, основните понятия, характеристики и елементи на информационната сигурност при формирането на обществените отношения в държавата; и са анализирани ролята и мястото на информационната сигурност в държавното управление, както и методите и средствата за нейното гарантиране в обществените системи.

1. Концептуални основи на информацията в контекста на информационната сигурност

1.1. Основни характеристики на понятието „информация“

Понятието „информация“ е едно от най-актуалните, фундаментални и дискусионни понятия в съвременната наука и практика. Някои автори представят информацията като първично понятие, поради което считат, че не е нужно то да се дефинира като такова. До днес за понятието „информация“ няма постигнато единно определение, като в исторически план то продължава да е предмет на дефиниране и формулиране от различни автори още от епохата на отминалото столетие. В научната литература съществуват много опити този феномен да се „облече“ в терминологично определение от философска, лингвистична, математическа и пр. гледна точка. Според някои автори латинският произход на термина „информация“, който означава „налагане на форма“, го представя като налагане на структура на някаква неопределена маса, като информацията съществува във всеки материален обект като многообразие на неговите състояния и може да се създава, унищожава, предава, приема, съхранява и обработва.[4] Ето защо информацията се представя като резултат от отражението на обективната действителност. Според безспорният авторитет в тази област Норберт Винер информацията е обозначение на съдържанието, получено от външния свят в процеса на приспособяване на индивида към него.[5] Друго широко разпространено определение за информацията е дадено от У.Р.

---

[4] Семерджиев, Цв., Н. Митев. Цит. съч., с. 20.

[5] Търкаланов, Ю. Разузнавателният анализ. С., Албатрос, 2003, с. 15.

Ешби (допълнено от А.Д. Урсул), които я разглеждат като отразено (добавено) разнообразие във всички обекти (процеси) на живата и неживата природа.

Същността на информацията е свързана с четири нейни неотменими характеристики. Първата е, че информацията винаги е свързана с определен материален обект и не може да съществува извън него. Според втората характеристика информацията се обменя чрез особени форми и минимални от енергийна и веществена гледна точка „порции", които са такива, че не разрушават системата „информиран – информиращ", което е в основата на втория методологичен извод, че няма информация изобщо, а тя винаги е конкретна и е предназначена за конкретен потребител. Информацията достига до потребителя по начин, при който не се нарушава триединството: източник, среда, потребител. Обстоятелството, че информацията трябва да дава нещо ново на потребителя, да разшири неговия обем от знания, е в основата на изграждане на третата характеристика, описваща разглежданото понятие. Оттук следва изводът, че всякакви данни, факти, сведения и др. са информация тогава, когато съдържат нещо ново за потребителя или потвърждават вече получени в дадената система данни. Четвъртата характеристика на информацията определя съществуването на отношението *„управление – информация"*. За информация се говори само тогава, когато тя се е използвала, използва се в момента или в бъдеще ще се използва за управление на някакви социални процеси или явления. Това управление може да се отнася както само за един индивид, така и за цяла обществена група на базата на допълнително получени знания, което означава, че без информация няма управление и обратното и показва, че същността на управлението се изразява чрез информационни процеси.

Информацията също така представлява снета (или преодоляна) неопределеност, като в процеса на нейното получаване тази неопределеност се намалява или ликвидира напълно.[6] Намаляването на неопределеността свързва информацията с установяване на някаква подреденост, като в този смисъл тя се разглежда като отрицателна ентропия. Според Н. Винер, ако ентропията е мярка за хаоса, то количеството информация е измерение на порядъка.

Можем да обобщим, че информацията представлява дадени сведения за обекти или явления от обкръжаващата среда, техните параметри, свойства и състояния, които намаляват съществуващата за тях степен на неопределеност и непълнота на знанието.[7] Същността на информацията се заключава и в съвкупността на отразените в нея признаци на обектите, системите, явленията и

---

[6] Търкаланов, Ю. Разузнавателният….цит. съч., с. 16. Също там: Според автора К. Шенън, информация съществува при наличието на възможности за избор измежду най-малко два варианта. Колкото по-голям е изборът, толкова по-богата е информацията.

[7] По въпроса виж Тужаров, Хр. Бази данни, 2007.

процесите извън техния контекст и винаги отразява степента на изменение на съществуващите знания.

Понятието информация е неделимо и от функционирането, и успешното развитие на всяка една *организационна система*, като изградена съвкупност от хора и ресурси, обединени чрез вътрешните организационни отношения, определящи правилата на взаимодействие в процесите на функциониране на системата. Управлението на всяка система винаги е свързано с използването на получената информация и създаването на най-благоприятни условия за реализиране на всички управленски функции, които да гарантират конкурентоспособността на организация и постигането на набелязаните цели.

Информацията винаги е свързана с определен материален обект и така се формира същината на информационния поток, който представлява движението на информацията от източника й до другия обект (потребителя), чрез канал за връзка, наречен транспортна информационна среда или преносител. Тези съставни части на информационния поток са в основата на информационните процеси[8], които представляват съвкупност от информационни дейности и стадии, които са свързани с различни аспекти от реалността.

Информацията е най-важният компонент на всеки информационен процес. При информационните процеси се получава информацията, необходима за реализиране на поставената цел, посредством изпълнението на последователни действия (операции), извършвани с данните, първичната информация, сведенията, фактите, хипотезите и т.н. В обобщение може да се твърди, че най-просто основните информационни процеси се съдържат в дейностите по събиране на информацията; нейното преработване, съхранение и разпространение (към потребителите) на информацията.

1.2. Структуроопределящи елементи на информацията

В научната литература терминът „информация“ се свързва с понятията *данни, факти, сведения* и пр., които изграждат нейната същност и са нейни основни информационни характеристики. Изследователите по темата определят най-общо данните (*data* - от лат. „дадена“), като неструктурирани факти за нещо (или за обект), които се съхраняват, без да се използват. При появата на необходимост, тези данни се използват (или обработват) с някаква цел, най-вече за намаляване неопределеността. Вече преобразуваните данни се превръщат в информация. В по-широкия смисъл данните се определят като наблюдаемо или измеримо сетивно възприятие (факти) от научни изследвания, събития от реалния свят, като се записват под формата на числа, думи или изображения.

---

[8] Василев, М. Обработка и анализ на информацията по национална сигурност. С., НСС, 2002, с. 13.

Информацията има съществена роля при формирането на социално-икономическите отношения в обществото, тъй като по своята същност то представлява сложна организационна система. Така например вид социална информация представлява *обществената информация*, която съгласно действащото законодателство е всяка общодостъпна информация, свързана с обществения живот и даваща възможност на гражданите да си съставят собствено мнение относно дейността на различни субекти. Тя се разделя на *официална* (която се съдържа в актове на държавни органи и органи на местното самоуправление при осъществяването на техните правомощия) и *служебна* (която се събира, създава и съхранява във връзка с официалната информация, както и по повод на дейността на органите и техните администрации). Друг специфичен вид информация представлява *класифицираната информация*, която съгласно правните регламенти, е всяка информация, представляваща държавна или служебна тайна, както и чуждестранната класифицирана информация.[9]

Съществена роля при определяне характера и вида на информацията имат източниците, от които тя се получава. Едни от най-широко използваните източници са т.нар. открити източници или означавани още като Open Sources. Също така информация може да се получава и при използването на специфични сили, методи и средства като прийоми на разузнаването или посредством обработката на открити източници.

1.3. Функции и качества на информацията като инструмент за въздействие на обществените отношения

Важно място в изучаването на явлението „информация“ трябва да се отдаде на неговите основни функции: *социална* (или предупредителна), *комуникативна*, която е в основата на отношенията между социалните групи и на релациите между политическата власт и държавното управление, държавите и международни организации; *когнитивна* - свързана с натрупването на ново знание и разширяване на познанието, което е в основата на историческото развитие на човешката цивилизация.

На информацията е отредена и ролята на специфичен фактор на производството. В основата на това е схващането, че съвременната икономика се основава на знанието, а информацията участва в основните стопански процеси, както на национално, така и на международно равнище. В условията на протичащата глобализация информацията се превръща в стратегически

[9] Чл.2 от Закона за достъп до обществена информация (ЗДОИ), обн. ДВ, бр. 55 от 07 юли 2000 г., изм. ДВ, бр. 85 от 24 октомври 2017. Също виж чл.1, ал.3 от ЗЗКИ, обн. ДВ, бр.45 от 30.04.2002 г., изм. и доп. ДВ, бр. 81 от 14.10.2016.

ресурс, а нарастващата зависимост на икономиката и социалната стабилност от информационните процеси я превръщат в мощен инструмент на въздействие.

Друг аспект от социалната роля на информацията е нейното *информационно въздействие*, което има за цел постигането на изменения в процесите, протичащи в информационните системи в съответствие със замисъла на субекта и неговото прилагане. Качествата на информацията като инструмент на въздействие я правят приложима към процеси, пряко свързани със сигурността на държавата, като чрез нея може да се окаже въздействие както върху вътрешната, така и върху външната среда. За повишаване социалната роля на информацията е създадена концепцията за *информационната война*, разбирана като борба за установяване на световно господство. Контролът върху знанието ще завърши епохата на завоевателните войни, чието бойно поле според Алвин Тофлър е невидимо, „виртуално" материализирано в глобалните информационни системи на човешката цивилизация и борбата в него е борба за контрол върху информационните ресурси на човечеството.

2. Основни аспекти в процесите на разпространение на информацията

2.1. Стойност и качествени параметри на информацията

В обществените системи количествените характеристики на информацията определят и части от нейната стойност. Качествените характеристики на информацията се класифицират основно в две групи - първата е според съдържанието, което на практика показва начина на отразяване на обекта, за който се отнася. Към качествата на информацията се отнасят: *достоверност* и *пълнота,* като в някои литературни източници се употребява понятието „достатъчност на информацията", т.е. степента, в която информацията сваля неопределеността. Втората група е според отношението на получателя на информация, като в този случай информацията има следните качества: *ценност* (значимост) и *своевременност* (актуалност) на информацията

Срещат се и някои „отклонения" на информацията, като съществуването на сто процента значима и достоверна информация е идеалното състояние, особено при развитието на социалните процеси, което не може да се постигне винаги. Ето защо се приема схващането, че всяка работа с информация е манипулация, т.е. действителността се моделира субективно и информационно. Субективният момент на отражението намира израз в трите форми на отклонение от реалността, като *девиация* (изкривяване); *аберация* (отклоняване); и *дезинформация*.

Друга качествена характеристика на информацията е свързана с преноса на данни от източника до потребителя, като се различават два вида информация:

първична (директна, пряка), която потребителят придобива за даден обект при непосредствените си контакти с него; и *вторична* (косвена, непряка), която е придобита по косвен път по схемата „източник – междинен носител – потребител“.[10]

Информацията се подразделя според съдържателната си натовареност, според обхвата, формата и обвързаността си, според времевите й свойства, но е необходимо да отбележим, че каквито качества и характеристики да притежава информацията, основно изискване към нея, особено при потреблението й в дадена социална система, е нейната *защитеност*. В технически смисъл защитеността на данните се характеризира със свойството „недостъпност“, което отразява защитеността им от неоторизиран достъп, а в социално-психологически аспект това означава конфиденциалност, с която се определя състоянието на секретност на информацията и достъпа до нея само на оторизирани потребители. Смисълът на прилагане на дейности и мероприятия по реализиране на изискванията за сигурност и защита на информацията в социалните системи е осигуряване на способността им да гарантират запазване на качествата на обработваната и съхранявана информация.[11]

2.2. Материални измерения на информацията

Съществен момент при определяне и оценка на ролята и значението на информацията при функционирането на дадена система е нейното разглеждане като ресурс, който позволява да се реализират социалните функции и да се осъществят икономическите дейности при постигане на целите на организацията, вкл. на държавната. Подобно на останалите ресурси, информационните ресурси също се явяват обект на покупко-продажба, конкуренция, политическа и икономическа експанзия и др.

По своята същност *информационните ресурси* могат да бъдат информация или знание, съхранени на материални носители или продукт на информационни системи. Като икономическа категория информационните ресурси формират своя цена, стойност, разход, печалба и др. Така най-общо за информационните ресурси може да се генерализира, че те представляват цялата натрупана информация, фиксирана на материални носители (както и във всяка друга форма), които осигуряват предаване през времето и пространството на информацията между различни потребители и служат за решаването на конкретни научни, управленски, социални и др. задачи и имат две основни характеристики –*неизчерпаемост* и *нематериалност*

В зависимост от вида на събраната информация, информационните ресурси се делят на класове, като спрямо първично събраната информация те се

[10] Захариев, А. Управление на информационните услуги. С., „Софттрейд”, 2011, с. 13.
[11]Пак там, с. 38.

систематизират като естествени, производствени, социално-икономически и др. Другият клас информационни ресурси образуват сведения и данни, получавани в процеса на творческата дейност, като към този клас ресурси се отнасят и обекти, създавани като авторски произведения в областта на литературата и изкуството. Информацията в този клас ресурси се явява вторична, получавана в резултат на интелектуалната дейност на човека и възникваща на база вече съществуваща информация. Тук също се отнасят различни научни открития, прогнози в областта на различни природни и социални процеси и др.

Друг вид материализирано изражение на информацията е нейното представяне във вид на *информационен продукт*, предоставен на даден потребител. В резултат на събиране, обработка, систематизиране и отчитане на информацията в отделните организации, се извършва нейното натрупване в различни *бази данни*, които са колекция от логически свързани данни в конкретната предметна област и са структурирани по определен начин.

Информацията може да съществува в много форми, но независимо от приетата форма, информацията винаги следва да бъде и *надеждно защитена*. Това дава възможност да се избегнат или намалят рисковете за нейното компрометиране и позволява ефективното използване на информационните ресурси, като краен резултат, чрез който се осъществяват и постигат целите на дадената организация.

2.3. Пространствени форми за разпространение на информацията

С настъпването на съвременната епоха информационните технологии навлизат все повече във всички сфери на обществения живот, предизвиквайки глобална интеграция на информационното пространство на човечеството, в което се появяват нови средства на труда и се създават нови обществени отношения. Информацията и базираните на нея знания определят главните черти на човешката цивилизация, която на съвременния етап на развитие се нарича информационно общество със своите характерни особености, които намират проявление във все по-засилващата се роля на ИТК във всички сфери на човешката дейност, като съществуването и функционирането на обществото вече е немислимо без използването на информацията. От друга страна, нарастването на броя на заетите специалисти в областта на информационните технологии и комуникациите води до увеличаването на дела на информационните продукти и услуги в БВП на държавите. Разширеният и улеснен достъпът до комуникации, СМИ и Интернет увеличава тяхното влияние в обществото, а създаващото се глобално информационно общество, което осигурява на хората по-ефективно взаимодействие и достъп до световните информационни ресурси, все по-често започва да се идентифицира като източник на рискове и заплахи.

В новата фаза в развитието на човешката цивилизация – *информационното общество* (*Information society*), главни продукти са информацията и знанието. Основните движещи сили на информационното общество, които оказват съществено влияние върху неговото развитие, са цифровата революция, информационната супермагистрала и глобализацията, в резултат на което планетата се превръща в място, където всеки има достъп до общите информационни ресурси.

Когато представяме информационното общество, трябва да отбележим и съществената роля и мястото в него, което заемат *информационните системи*, тъй като в основата на тяхното функциониране е производството на нужната за дадената социална организация информация с цел осигуряване на ефективно управление на всичките й ресурси и създаване на информационна и техническа среда за осъществяване на това управление. Под „информационна система“ следва да се разбира средата, осигуряваща целенасочената дейност на субектите и трябва да се разглежда в по-широк смисъл, а не само в технически аспект, тъй като тези системи включват в себе си и държавата, и обществото. В условията на информационно общество, информационните системи се явяват най-важният клон в класификационната схема на системите, като те участват и играят съществена роля във всички останали обществени системи.[12] Мястото, където се осъществяват тези процеси на създаване и разполагане на информацията и получаването и интерпретирането й от съответния потребител, се определя като *информационно пространство* (*Information space*). То се определя и като системообразуващ фактор, активно влияещ на състоянието на обществената сигурност във всички направления в развитието на обществото. Информационното пространство се дефинира и като съвкупност от бази данни, технологии за техния трансфер и използване, информационни и телекомуникационни системи, функциониращи на основата на общи принципи и осигуряващи информационното взаимодействие на организациите и гражданите и удовлетворяването на техните информационни потребности. Основни негови компоненти са: информационните ресурси, средствата за информационно взаимодействие и информационната инфраструктура.

3. Доктринални основи на информационната сигурност

3.1. Същност и място на информационната сигурност в обществените отношения

Динамичното развитие на науката и информационните технологии в началото на XXI век водят след себе си множество дълбоки промени в

[12] По въпроса виж Тужаров, Хр. Бази данни, 2007.

стратегическата среда[13], които на свой ред засягат почти всички аспекти на дейност на социалните системи. Днес факт са нови реалности, като усложняване на международната обстановка, нарастване на обхвата и темпото на промените, появата на нови заплахи и рискове, пораждащи нетрадиционни кризи и конфликти, които се разрастват мигновено и засягат големи територии и многочислено население. Причините за това се коренят в нарастването на ролята на информацията в обществените процеси в съвременния свят - глобалното разпространение на информационните инфраструктури, ръстът на информационния обмен и комуникационната интеграция в световен мащаб, свързват в една мрежа цялото човечество. Тази информационна интеграция създава множество нови възможности за възход и просперитет на социалните общности, като обединява всички аспекти на обществената активност в едно световно информационно пространство, което днес е системообразуващ фактор на човешката еволюция.[14]

Според изследователите истинската същност на понятието *информационна сигурност* следва да се търси в съставните му части – *информация* и *сигурност*, като същността и основните характеристики на информацията бяха представени в по-горните съждения на научното дирене. В случая ще отделим по-специално внимание на второто понятие – *сигурност*. В контекста на разглеждания проблем ще представим и някои теоретични аспекти на понятието *национална сигурност*, като ключов елемент от реализирането на държавните политики.

Сигурността има смисъл и се разглежда само в контекста на обществената организация. Социологизирането на сигурността е възможният правилен подход, който дава много от отговорите на въпросите, които се търсят при нейното изучаване, защото тя съществува за човека единствено и само в условията на социалната организация. Това е довело до фундаментална промяна на характера и структурата на обществените отношения и е предизвикало радикални изменения в схващанията за *националната сигурност* на съвременната държава.

Необходимостта да се удовлетвори основната човешка потребност от сигурност е и главната причина в съвременното българско общество да се

---

[13] Национална отбранителна стратегия на Република България, приета с Решение № 283 от 18 април 2016 г. на МС, в която се описва стратегическата среда за сигурност като сложна, динамична и с трудно предвидими измерения. Основното дестабилизиращо влияние върху формирането й оказват глобализацията, забавянето на икономическото развитие и неблагоприятните явления във финансовата сфера, вътрешни и регионални конфликти, енергийни, демографски, екологични и климатични проблеми, заплахи за информационната сигурност и пр.

[14]Семерджиев, Цв., Н. Митев. Цит. съч., с. 15.

създаде Системата за национална сигурност (СНС), която да гарантира сигурността на българските граждани и да осигурява защитата на интересите на гражданското общество, териториалната цялост и суверенитета на държавата във всички сфери на човешката дейност – политическа, икономическа, социална, екологична, военна, информационна и др.

В контекста на изследвания проблем информационната сигурност е един от най-важните компоненти на националната сигурност, защото информационното пространство е мястото, където се извършват основните социални дейности в съвременното общество – управленски, икономически, културно-образователни, информиране, свободно време и др. Свободният и безопасен достъп до информационното пространство, гарантираната сигурност на циркулиращите в обществото и отделните организации информационни потоци, са от жизнено значение при осигуряването на възможности за развитие и просперитет на гражданите, организациите и обществото като цяло.[15]

В този смисъл *информационната сигурност* е защитеността на държавата на стратегическо, оперативно и тактическо равнище. Схващанията за същността на информационната сигурност се прилагат най-вече при формиране на държавната политика в информационната сфера, за усъвършенстване на нейното правно, методическо, научно-техническо и организационно гарантиране и за разработка на целеви програми в тази област. Представата за информационна сигурност е стратегически възглед, обединяващ схващанията за интересите на личността, обществото и държавата в информационната сфера, от една страна, и заплахите за тези интереси и пътищата и средствата за тяхната защита, от друга страна. Също в рамките на този възглед се анализират: стратегическата среда, видовете заплахи и техните източници, задачите и методите за гарантиране на сигурността, основните положения на държавната политика и системата за гарантиране на информационната сигурност.

3.2. Информационна сигурност и защита на обществените системи

Сигурността на комуникационните и информационни системи и тяхната достъпност все повече ангажират общественото внимание. Причината за това са високите рискове и заплахи за ключовите информационни системи, дължащи се на тяхната сложност, или поради повреди, грешки и атаки над физическата инфраструктура, които могат да се окажат критични за благосъстоянието на гражданското общество.[16] Ето защо за успешното реализиране на

---

[15]Семерджиев, Цв., Н. Митев. Цит. съч., с. 16-17.

[16] Европейска агенция за мрежова и информационна сигурност (ENISA), Подход за създаване на ЦДКСКС стъпка по стъпка, документ за справка WP2006/5.1(CERT-D1/D2), 2006, с. 3.
По въпроса също виж CERT Bulgaria – Национален център за действие при инциденти в информационната сигурност (НЦДИИС) // https://govcert.bg/BG/Pages/default.aspx- посетен на 23.03.2020.

информационната сигурност в обществените отношения информационната среда трябва да бъде добре изучена, субектите, и обектите, които си взаимодействат в нея и формират протичащите явления и процеси, както и да се познават добре съществуващите възможности за развитие и поява на рискове и заплахи за информацията в дадената обществена система.

Днес сигурността на всяка държава може да се гарантира само чрез изграждане на еволюционно развиваща се комплексна автоматизирана информационна система за стратегическо управление, в която на основата на анализа да се определят всички действащи фактори и да се осигури възможност за вземането на ефикасни решения. Разработването и използването на тази система изисква ясна и адекватна информационна стратегия и ресурсно осигуряване на жизненият й цикъл, съгласувани с общата концепция за национална сигурност и развитието на страната. Националната автоматизирана информационна система за стратегическо ръководство, командване и управление обединява организационно всички системи, които участват в провеждането на политиката и с които се гарантира сигурността в различните сфери на обществения живот на страната. Тя се използва от всички държавни органи, които съгласно вменените им по Конституция функции, осъществяват националната информационна политика. Тяхна е и отговорността за провеждане на национална политика за сигурност и отбрана в информационното пространство.

Друг важен момент, който има съществена роля при функционирането на обществените системи, са съществуващите заплахи за информационната сигурност, които се подразделят на *външни* и *вътрешни*. Външните източници продуцират враждебни действия на чужди организации, групи от хора и отделни личности в световното информационно пространство, водещи до последствия спрямо националната сигурност. Към вътрешните източници на заплахи за информационната сигурност се отнасят враждебни действия в националното информационно пространство от отделни лица, групи от хора или организации, водещи до застрашеност на националната сигурност.

Гарантирането на информационната сигурност се извършва посредством *правни, организационно-технически* и *икономически методи*. Същевременно за гарантиране на информационната си сигурност, държавата провежда държавна политика, която дефинира основните направления в дейността на органите на държавната власт и местното самоуправление в тази област, реда за определяне на задълженията им в рамките на тяхната компетентност при защита на националните интереси в информационната сфера.

Самата информационна сигурност също оказва силно влияние на държавното управление, тъй като последното се осъществява от органите на

държавната власт и местното самоуправление, при които протичащите информационни процеси образуват затворен цикъл. Те касаят получаването от управляващите субекти на информация, нейната преработка и анализ, приемането на управленски решения, привеждането им в изпълнение, контрол и получаване на информация за резултатите от управлението. Тези процеси по свята същност не се извършват само с помощта на компютъризирани и автоматизирани информационни системи, но са подкрепени и от организационно-правното осигуряване на информационната сигурност, което представлява съвкупността от решения, закони, нормативни актове, регламентиращи както общите дейности по осигуряването на информационната сигурност, така и създаване и функциониране на системите за защита на информацията на конкретни обекти.

3.3. Методи и средства за гарантиране на информационната сигурност

Реализирането на информационната сигурност на дадената система се извършва в няколко *направления,* които могат да се разпределят в следните категории:

1. *Законодателно-правно обезпечаване*.
2. *Организационно-техническо осигуряване*.
3. *Застрахователно обезпечаване*.

За защита на информацията в дадената система се прилагат различни *способи и средства.* Един от основните способи за защита на информацията е *управлението на достъпа* до нея в дадената система. Това се постига чрез регулиране на всички ресурси на системата (технически и програмни средства, бази данни и др.)

Друг характерен начин за защита на информацията е нейното *криптиране* (маскировка). Този способ се приема от специалистите по темата за ефективен както от гледна точка на собствената защита, така и от гледна точка на ползвателя на информация.

Информацията може да се защити и посредством разработването на комплексни мероприятия, въвеждащи ясна *регламентация* при обработката и съхраняването на информация, при които нерегламентираният достъп би бил минимален или дори невъзможен. Не на последно място като способ за защита на информацията в дадената организация могат да се прилагат и различни *мерки от действащото законодателство* – административни, материално-финансови или наказателни мерки при извършване на умишлени злонамерени действия и др.

Важно е да се подчертае, че различните способи за защита на информацията се реализират и посредством различни средства, които могат да

бъдат *технически, програмни, организационни, законодателни* и *морално-етични средства*. Те от своя страна, могат да се класифицират като *формални* (изпълняват защитни функции по строго определени процедури, без непосредственото участие на човека) и *неформални* (определят се или от целенасочената човешка дейност или регламентират косвено или непосредствено тази дейност).

Не на последно място при защитата на информацията в съвременното информационно общество място трябва да се отдаде на основната роля на държавата, която функционално трябва да обезпечава решаването на задачите в тази сфера.

В заключение от направеното дотук по научното дирене може да посочим, че информационната сигурност в съвременната информационна епоха е един от най-важните компоненти на националната сигурност на държавата, защото информационното пространство е мястото, където се извършват основните социални дейности (управленски, икономически, образователни, информиране, свободно време и т.н.) в съвременното общество. Свободният и безопасен достъп до информационното пространство, сигурността и безопасността на циркулиращите в обществото и отделните организации информационни потоци, са от жизнено значение за осигуряване на възможностите за развитие и просперитет на отделните личности, организации и обществото като цяло.[17]

Изводи от глава първа

- Информацията е стратегически актив от първостепенно значение, който е в основата за вземане на решения на всички равнища и етапи от развитието на отделните общества и държави, която трябва да бъде надеждно защитена, независимо от нейната форма на съществуване.

- Всички значими социални дейности в съвременното общество (управленски, икономически, образователни, политически, отбранителни и т.н.) се осъществяват в информационното пространство.

- Сигурността и безопасността на циркулиращите в обществото и организациите информационни потоци са гарантирани единствено при осигуряването на свободен и безопасен достъп до информационното пространство.

- Като стратегически възглед и един от най-важните компоненти на националната сигурност информационната сигурност е защитеност във всеки един момент на държавата и нейните интереси в информационната сфера на стратегическо, оперативно и тактическо равнище от всякакви опити за

[17]Семерджиев, Цв., Н. Митев. Цит. съч., с. 17.

злоумишлени посегателства и влияния върху информационната й инфраструктура и информационни ресурси.

- При защитата на националните интереси в информационната сфера държавата провежда държавна политика за гарантиране на информационната си сигурност, която дефинира основните направления в дейността на органите на държавната власт и местното самоуправление и реда за определяне на задълженията им в рамките на тяхната компетентност.

ГЛАВА ВТОРА
ДЪРЖАВНОТО УПРАВЛЕНИЕ КАТО ЗАЩИТАВАНА СИСТЕМА В ПРИОРИТЕТИТЕ НА НАЦИОНАЛНАТА СИГУРНОСТ НА СТРАНАТА

Във втора глава е представена и анализирана същността на държавното управление като сложна политико-правна категория, която по същество се свежда до организирано ръководство на държавата. В нея са реализирани трета и четвърта научно-изследователски задачи на дисертационния труд, като са изследвани същността и основните характеристики на стратегическите дейности и обекти при реализиране на държавното управление като елемент от националната сигурност на страната; и са анализирани принципите, характера и типологията на процесите в управлението на държавните органи и състоянието на информационната сигурност на страната.

Под мениджмънт на информационната сигурност в държавното управление ние разбираме как тази специфична дейност се реализира за описаните в Постановление № 256 от 17 октомври 2012 г[18]. дейности и обекти, свързани с държавното управление, поради това, че именно те са определени като приоритетни за националната сигурност на страната. Терминът „критична инфраструктура" се въвежда в българското законодателство през 2005 г. с приемането на Закона за управление при кризи[19]. Според закона *критична инфраструктура* е система от съоръжения, услуги и информационни системи, чието спиране, неизправно функциониране или разрушаване би имало сериозно негативно въздействие върху здравето и безопасността на населението, околната среда, националното стопанство или върху ефективното функциониране на държавното управление. Съществува пряка връзка между информационната сигурност и защитата на обектите на критичната инфраструктура. Навлизането на информационните и комуникационни

[18] Постановление № 256 от 17 октомври 2012 г. за приемане на Наредба за реда, начина и компетентните органи за установяване на критичните инфраструктури и обектите им и оценка на риска за тях.

[19] По въпроса виж Закон за управление при кризи, обн. ДВ, бр.19 от 1 март 2005 г., отм. с §2, т.3 от ЗОВС.

технологии в държавните обекти прави критичните инфраструктури атрактивни цели за атака.

Значимостта на проблема за сигурността на информацията в обектите от критичната инфраструктура е ясно формулиран, като според изследванията възпрепятстването или унищожаването на критичната инфраструктура има пагубно въздействие върху националната сигурност и/или икономическото и социалното благосъстояние на една нация.[20] От друга страна, нарушаването на критичната инфраструктура може да генерира социални промени на много високо и сложно равнище или обхват.[21] Непредвидените и негативни последствия за инфраструктурата могат да бъдат много повече в количествено и качествено изражение от ползите, за чието създаване тази инфраструктура е проектирана.

1. Стратегически дейности при реализиране на държавното управление

✓ *Гарантиране на демократичните устои на държавното управление*

Процесите на глобализация, разгърнали се от 70-те г. на XX век водят до ограничаване на суверенитета на националната държава и до упадък на социалната държава в условията на неолиберален глобален капитализъм. Това води до трансформация на държавата, изразяваща се в делегиране на части от нейния суверенитет „нагоре“ – към наддържавни организации, и „надолу“ – към местни органи на властта и организации на гражданското общество. Свидетели сме на споделяне на национално-държавния суверенитет с други играчи (в т.ч. вето-играчи, каквито са транснационалните корпорации), при което националната държава все още остава ключов играч. Това се дължи на много причини, но една от най-важните е, че държавата чрез своя правов ред е незаменима в създаване на условия за реализация на основните права на своите граждани, като държавното управление е неразривно свързано с двете родови понятия – *конституционен ред* и *обществен ред*, които са подложени на детайлен сравнителен анализ в работата.

✓ *Охрана на държавната граница и отбрана на територията, териториалното море и въздушното пространство на страната*

✓ *Правораздавателна дейност*

✓ *Сигурност*

---

[20] По въпроса виж Dunn, M. and I. Wigert. *AnInventory and Analysis of ProtectionPoliciesinFourteenCountries*, International CUP Handbook 2004, ed. A. Wengerand J.Metzger, Institute of Technology Zurich.

[21] По въпроса виж Weijnen, M. *CriticalInfrastructures at Risk – The Need for Innovation*. Powerpointpresentation, December 2005 // http://www.lsa.ethz.ch/news/Zurich_ETH_220605.pdf - посетен на 01.12.2019.

- ✓ *Защита от природни бедствия и кризи*
- ✓ *Управление и поддържане на Националната система за спешни повиквания с единен европейски номер 112 (НССПЕЕН 112)*
- ✓ *Съхранение и управление на стоки, материали и суровини, представляващи държавните резерви и военновременните запаси*
- ✓ *Дейности, осъществявани от Специалната куриерска служба във връзка с изпращане, предаване, пренасяне и приемане на материали, съдържащи КИ*

2. Стратегическите обекти на държавното управление като елемент от Системата за национална сигурност на страната

В изпълнение на политиките по гарантиране сигурността на страната в задълженията на компетентните държавни органи попада установяването на критичните инфраструктури и техните обекти, както и извършването на оценка на риска за тях. Установяването на критичните инфраструктури и обектите се извършва с цел намаляването на риска от бедствия и защита на населението.[22]

Съгласно действащото законодателство, под определението „критична инфраструктура“[23] се разбира система или части от нея, които са от основно значение за поддържането на жизненоважни обществени функции, здравето, безопасността, сигурността, икономическото или социалното благосъстояние на населението и чието нарушаване или унищожаване би имало значителни негативни последици за Република България в резултат на невъзможността да се запазят тези функции. От своя страна, под „обект на критична инфраструктура“[24] се разбира организационно и/или икономически обособена част от критичната инфраструктура, която е ключова за нормалното функциониране, непрекъснатостта и целостта ѝ. Един обект може да се отнася към критичната инфраструктура на един или повече сектори.

В българската теория и практика се използва терминът „стратегически обект“, без това понятие да има легално определение. Затова приемаме, че понятията „стратегически обект“ и „обект на критичната инфраструктура“ са тъждествени. Съгласно българското законодателство като приоритетни обекти на критичната инфраструктура са определени Народното събрание, Президентството, Министерски съвет и Комплекс „Бояна“[25]. За нуждите на настоящото дисертационно изследване подробно са разгледани първите три обекта през призмата на мисията и функциите на институциите, които са

[22] Постановление № 256 от 17 октомври 2012 г. за приемане на Наредба за реда, начина и компетентните органи за установяване на критичните инфраструктури и обектите им и оценка на риска за тях.
[23] Виж пак там, допълнителна разпоредба.
[24] Виж пак там, допълнителна разпоредба.
[25] Виж раздел VIII, т.2 на приложението към Постановление № 181 от 2009 г. на МС.

разположени в тях и в качеството им на основни субекти в Системата за защита на националната сигурност на страната. Съгласно принципа за разделение на властите, заложен в Конституцията на Република България, главната отговорност за националната сигурност на страната е възложена на Народното събрание, на Президента на републиката и на Министерския съвет. Тяхна отговорност е и формирането на държавната политика за национална сигурност.[26]

3. Основни аспекти на държавната политика за гарантиране на информационната сигурност

3.1. Принципи за осъществяване на информационната сигурност в рамките на държавното управление

Държавната политика за гарантиране на информационната сигурност дефинира основните направления в дейността на органите на държавна власт и органите на местното самоуправление в тази област, както и реда за определяне на задълженията им (в рамките на тяхната компетентност) за защита на националните интереси в информационната сфера. Тази държавна политика се базира на спазването на баланс на интересите на личността, обществото и държавата в информационната сфера. В процеса на осъществяване на тези свои функции държавата провежда обективен, всестранен анализ и прогнозира заплахите в областта на информационната сигурност. На следващо място, се включва разработването на комплекс от мерки за нейното гарантиране, който е насочен към предотвратяване, отблъскване и неутрализиране на заплахите за информационната сигурност. Прилагането на мерките се осъществява чрез правилното организиране на дейността на законодателните и изпълнителните органи на държавната власт.

В изпълнение на държавната политика за гарантиране на информационната сигурност държавната власт трябва да поддържа дейността на обществените обединения, насочена към обективно информиране на населението за социално значими явления в обществения живот на страната и към предпазване на обществото от изопачавания и предоставяне на недостоверна информация.

Друго приоритетно направление на държавната политика в областта на гарантиране на информационната сигурност е усъвършенстването на правните механизми за регулиране на обществените отношения, които възникват в информационната област.

Не на последно място, държавното управление трябва да насочи усилията си към приемане и осъществяване на държавни програми, в които се предвижда

[26] Казаков, К. Управление на системата…цит. съч., с. 29.

създаването на общодостъпни архиви от информационни ресурси на държавните органи и органите на местното самоуправление.

Важен елемент от държавната политика за информационна сигурност е развитието на системата за подготовка на кадри, използвани в областта на информационната сигурност и хармонизирането на националните стандарти в областта на информационната сигурност с тези на международната общност.[27]

3.2. Характер и типология на процесите в управлението на държавните органи

Протичащите в сферата на държавното управление процеси по своя характер са *информационни* и образуват затворен цикъл. Към основните параметри на тези процеси се отнасят получаването на информация (от управляващите субекти); преработката и анализа на получената информация; вземането на управленски решения; привеждането на решенията до изпълнителите; контрол на изпълнението и получаване на обратна информация (обратна връзка) за резултатите от изпълнението. Част от изброените процеси се реализират с помощта на компютъризирани, автоматизирани информационни системи – бази данни, фондове и др. Това са организационно-технически системи, които представляват съвкупност от редица взаимосвързани елементи, като технически средства за обработка и предаване на данни (дигитални технически устройства и средства за свръзка), различни методи и алгоритми за обработка под формата на съответното програмно осигуряване, информация (масиви, бази данни) на различни носители и не на последно място, персоналът и ползвателите на системите, обединени по организационно-структурен, тематичен, технологичен или друг признак за изпълнение на автоматизирана обработка на информацията с цел удовлетворяване на информационните потребности на субектите на информационните отношения.

3.3. Основни аспекти на състоянието на информационната сигурност в Република България

В отговор на предизвикателствата в динамичното развитие на съвременна информационна епоха и промените в средата за сигурност, през последните години в Република България беше осъществен комплекс от мерки за усъвършенстване и гарантиране на информационната сигурност при

---

[27] Виж Наредба за общите изисквания за мрежова и информационна сигурност (загл. изм. ДВ, бр.5 от 2017 г., в сила от 01.03.2017 г.), приета с ПМС № 279 от 17.11.2008 г.
Виж пак там, §1, т.3 от доп. разпоредби – „Мрежова и информационна сигурност" е способност на мрежите и информационните системи да се противопоставят на определено ниво на въздействие или на случайни събития, които могат да нарушат достъпността, автентичността, интегритета и конфиденциалността на съхраняваните или предаваните данни и на услугите, свързани с тези мрежи и системи.

управлението на държавните органи. В тази връзка се формира се солидна правна база, като бяха приети редица закони и нормативни актове, регламентиращи обществените отношения в информационната сфера. На второ място, на различни нива в системата на държавното управление бяха създадени институции, които да отговарят за регулирането на тези отношения. Като едни от най-важните в тази посока правно-нормативни актове могат да се посочат: КРБ, ЗЗЛД, ЗДОИ, ЗМВР, ЗОВС, ЗЕС, ЗУФСЗНС, Националната отбранителна стратегия (2016 г.), Доктрината на въоръжените сили на Република България (2017 г.), Актуализираната стратегия за национална сигурност на страната и др.

Един от най-важните закони, уреждащи обществените отношения в информационната сфера е Законът за защита на класифицираната информация и съпътстващите го поднормативни актове. С него се въведоха ефективни механизми за гарантиране на информационната сигурност по отношение на всички субекти, които създават, обработват, съхраняват и пренасят класифицирана информация, в т.ч. и в автоматизирани информационни системи (АИС) и мрежи. Също така за успешното решаване на въпросите за гарантиране на информационната сигурност на Република България функционират държавната система за защита на класифицираната информация, системата за опазване на държавната и служебна тайна и системата за лицензиране и сертификация на средствата за защита на информацията.

Постигнатите успехи и положените усилия за хармонизиране на българското законодателство с европейското са безспорни, но равнището на информационна сигурност в страната все още несъответства в пълна степен на потребностите на обществото. Въпреки регистрирания напредък и несъмнени постижения в областта на гарантирането на информационната сигурност на Република България, все още има редица слабости и нерешени проблеми, които изискват предприемането на комплекс от мерки и механизми, насочени към постигането на едно по-високо равнище на сигурност и защита на интересите на личността, обществото и държавата в информационното пространство, като същевременно се създават предпоставки за установяване на култура на прозрачност, която води до осигуряване на гарантиран свободен достъп до обществената информация, даващ възможност на различните субекти в обществото да формират и вземат обосновани решения.

Изводи от глава втора

- Защитата на органите на държавното управление от информационни рискове, заплахи и опасности има непосредствено значение за тяхното добро функциониране и осъществяване на техните цели и задачи. Това определя важната роля и формирането на актуална държавна информационна политика.

- Значимостта на проблема за сигурността на информацията в обектите от критичната инфраструктура на страната е ясно формулиран, като са конструирани параметрите на връзката между информационната сигурност и защитата на тези обекти като елемент от системата за защита на национална сигурност.

- Информационната сигурност се оценява като стратегически проблем на политиката и управлението на националната сигурност на страната. Акцентира се върху идеята за определяне на информационната сигурност като критична инфраструктура на сигурността, както и ролята на информацията в останалите дефинирани критични инфраструктури.

- В Република България се изпълнява комплекс от мерки за усъвършенстване и гарантиране на информационната сигурност при управлението на държавните органи. Формирана е солидна правна база и на различни нива в системата на държавното управление са създадени институции, които отговарят за регулирането обществените отношения в информационната сфера.

- Въпреки ясно формулираните критерии за мястото и ролята на държавата при управлението и защитата на дейностите и обектите от критичната й инфраструктура, е необходимо в законодателната рамка да се дефинира по-добре понятието „критична информационна инфраструктура", което би повишило капацитета на нейната защита.

ГЛАВА ТРЕТА

МЕХАНИЗМИ ЗА ОПТИМИЗИРАНЕ НА ИНФОРМАЦИОННАТА СИГУРНОСТ В ДЪРЖАВНОТО УПРАВЛЕНИЕ

В трета глава са анализирани състоянието на информационната сигурност в процесите на управление на държавата и на основата на SWOT анализ са представени способите и мерките за нейното подобряване в органите на държавната власт при управлението на кризи; изведени са препоръки за подобряване на държавното управление при защитата на информационната сигурност като елемент от националната сигурност на страната. По този начин е реализирана последната научно-изследователска задачи на дисертацията.

1. Методи и изследвания, приложени при изучаване състоянието на информационната сигурност в държавното управление

1.1. SWOT анализ на състоянието на информационната сигурност в процесите на управление на държавата

За да се разкрие по-добре състоянието на информационната сигурност в процесите на управление на държавата при защита на националната й сигурност, осъществявани от ангажираните държавни органи и институции възприемаме използването на методите на стратегическия анализ. По наше

мнение тези методи са подходящи за прилагане в дисертационното изследване, защото чрез анализ и оценка на възникнали ситуации и заплахи в дадената система най-добре може да се прогнозира нейното развитие и да се изработят варианти за целенасочено поведение на субектите, което е необходимо и достатъчно условие при вземането на решения за избор на най-подходящия измежду тях вариант[28]. По своята същност стратегическият анализ е комплексен анализ на средата за сигурност, на максималното въздействие на заплахата или риска, на максималния обем от необходимите ресурси или необходимостта от вземането на решение на най-високо ниво с цел преодоляването на несигурността.[29] *Това налага в механизмите на държавния мениджмънт да се създаде система за контрол и ефективно управление на информационните процеси, което ще гарантира информационната сигурност при управлението на възникнали кризи като елемент от защитата на националната сигурност на страната, за да се постигне намаляване на негативните им последствия или тяхното пълно неутрализиране*. Предвид характерните особености на изследваната система, за нейното подробно анализиране и представяне приложихме като комплексен метод за стратегически анализ SWOT анализа.

Всяка държавна дейност трябва да бъде подлагана на анализ с цел контролиране и запазване на приемливите параметри, необходими за ефективното и добро функциониране и управление на държавата като цяло. В тази връзка считаме, че изследваната система може да бъде разгледана чрез задълбочен анализ на протичащите в органите на държавното управление информационни процеси. Това ни позволи да разкрием в дълбочина характерните особености от състоянието на информационната сигурност при защита на националната сигурност в процесите на управление, осъществявани от ангажираните държавни органи и институции В съставните части в матрицата на SWOT анализа са описани факторите, които имат най-голямо влияние върху изследваната система като силни и слаби страни, както и прогнозирането на тяхното развитие в краткосрочен и дългосрочен план.

1.2. Преглед и обобщение на резултатите от SWOT анализа

От представените елементи в матрицата на SWOT-анализа могат да бъдат представени следните ***изводи***:

- В държавата съществуват законодателна и институционална рамка, чрез която ясно са регламентирани обществените отношения в информационната сфера като елемент от защитата на националната сигурност на страната.

---

[28] Семерджиев, Цв. Стратегическо ръководство…цит. съч., с. 109-110.

[29] Гюров, Р. Към анализа на сигурността. С., Ф-я „Национална и международна сигурност“, 2011, с. 128.

- За гарантиране и защита на информационната сигурност в държавното управление е необходимо въвеждането на ефективен контрол върху изпълнението на информационните процеси в държавните органи и качествено управление на човешките ресурси.

- За изпълнение на приоритетите и практическото противодействие на рисковете и заплахите за националната сигурност на страната е необходима актуализирана законодателна рамка, вкл. и изработването и приемането на нови законодателни регламенти в областта на овладяването на възникнали кризи от различен характер.

2. Информационната сигурност в процесите на държавното управление при кризи

2.1. Управлението при кризи като елемент от защитата на националната сигурност на страната

Чрез SWOT анализа е установено, че държавата е изградила добра законодателна и институционална рамка за управление на процесите при защита на информационната сигурност като елемент от националната сигурност на страната. Въпреки отчетените положителни аспекти в матрицата на анализа е видно, че едни от най-сериозните проблеми за държавното управление са наличието на слабости в прилагането на сегашните методи за гарантиране на информационната сигурност в органите на държавната власт. Липсата на качествен контрол при изпълнението на информационните процеси в държавните органи може да доведе не само до загуба на информационни ресурси и вземане на грешни управленски решения, но и в пробив в информационната сигурност на страната. Не на последно място анализът извежда и някои слабости в законодателната рамка на държавното управление при процесите за гарантиране защитата на националната сигурност на страната и в частност в управлението на възникнали кризи като елемент от тази сигурност.

За да разкрием в цялост същността и основните аспекти на държавната власт в управлението на страната, за нуждите на дисертационния труд бяха разгледани някои основни процеси на държавното управление при възникнали кризи като елемент от защитата на националната сигурност на страната и възможностите за гарантиране на информационната сигурност при тяхното протичане.

2.2. Основни аспекти на политиката за информационна сигурност при управлението на възникнали кризи

В резултат на динамиката на развитие на информационните и комуникационни технологии в световен план на дневен ред в българското общество се появяват нови проблеми, свързани с укрепването на националната

сигурност на страната в условията на глобализация. Това означава също, че устойчиво развитие на държавата може да се постигне чрез осигуряване на високо равнище на информационната ѝ сигурност. В този контекст за държавното управление при кризи следва да се отбележи, че политиката за информационна сигурност е съществен градивен сегмент от цялостната държавна политика за национална сигурност на страната.

Политиката за информационна сигурност е система (комплекс) от четири основни елемента, които се дефинират при отчитане на националните интереси. Към тях се отнасят: условията за осигуряването на държавната политика за информационна сигурност; развитието на националната информационна инфраструктура; защитата на националните информационни инфраструктури и ресурси. Успешната реализация на политиката за информационна сигурност в рамките на управлението на държавата при възникнали кризи зависи от ресурсите, информираността за ситуациите и заплахите, подготовката и поведението на ангажираните държавни органи и институции. Когато разпределението на ресурсите е пропорционално на управлението на дейностите, най-благоприятният очакван изход е в посока решаване на възникналите критични ситуации и ограничаване на последиците от тях в краткосрочен план, с минимални ресурси и разходи.

3 . Оптимизиране на механизмите на държавното управление при защита на информационната сигурност като елемент от националната сигурност на страната

3.1. Способи и мерки за подобряване на информационната сигурност в органите на държавната власт при управлението на кризи

За защитата на информационната сигурност в държавното управление трябва да се полагат особени грижи. В постановление № 186 от 19 юли 2019 г. за приемане на Наредба за минималните изисквания за мрежова и информационна сигурност Чл. 2. (1) и (2) са посочени мерките за мрежова и информационна сигурност. В теорията и практиката съществуват различни по вид и предназначение информационни средства за защита на информацията в зависимост от компютърните и комуникационни възможности за първоначално събиране на информация, за представяне на информация, за архивиране, за статистика, контрол, комуникация и др. Важен елемент от управлението на държавата при кризи е своевременното, надеждно, защитено и достъпно използване на източниците на информация и управлението на информационните потоци.[30]

---

[30] Павлов, Г. Проблеми на сигурността и защитата на класифицираната информация в автоматизираните информационни системи и мрежи. С., УНСС, „Икономически алтернативи“, бр.5, 2005, с. 27-40.

3.2. Мониторинг и контрол на процесите за гарантиране на информационната сигурност при взаимодействието на държавните институции при управлението на възникнали кризи

В контекста на проведеното изследване и формулираните от SWOT анализа изводи считаме, че усилията на държавното управление трябва да се насочат в посока преодоляване на констатираните пропуски и отстраняване на възникналите проблеми при гарантирането на информационната сигурност в процесите на защита на националната сигурност на страната, с което ще се постигне благоприятен ефект върху функционирането на цялата държавна система и отделните й елементи, а от друга страна и не на последно място ще се повиши и общественото доверие в държавните институции.

Разгледаните процеси могат да бъдат обхванати и представени в една обща *Система за мониторинг и контрол на информационните процеси при взаимодействието на държавните органи в управлението на възникнали кризи*, чрез която се показва една по-широка картина на механизма на действие на протичащите в системата процеси, тяхното управление и начините за контрол над основните й елементи. Ето защо считаме, че прилагането на системата за мониторинг и контрол на информационните процеси в органите на държавата при управление на възникнали кризи ще гарантира по-високо ниво на информационната сигурност при изпълнението на дейностите, които ангажираните държавни институции, органи и ведомства осъществяват в това управление. Това е важно, тъй като динамиката на протичащите процеси е голяма, средата, в която те се извършват се отличава с променливост и динамичност и подреждането и обхващането на отделните елементи от системата в единен общ организъм със стройно изградени връзки, начини за комуникация, отчетност, управление, механизми за наблюдение и проверка и пр., ще позволи по-доброто им наблюдение, контрол, организиране на работата и постигане на поставените цели.

3.3. Препоръки за подобряване на държавното управление при защита на информационната сигурност

Представената система ясно дефинира и показва мястото, компетенциите, координацията и начините за контрол между държавните структури и субекти при управлението на кризи. Разкрити са функциите, връзките и начините за осъществяване на взаимодействие между ангажираните държавни органи и институции при управлението на кризи, начините на осъществяване и протичане на информационните процеси в рамките на това управление и механизмите за контрол на взетите решения. Правомощията, отговорностите и дейностите, които органите на държавната власт изпълняват при възникнали

кризи, са съгласно устройствените закони и правно-нормативните регламенти на действащото законодателство.

В контекста на представеното изследване, в съответствие с императивите на приетите стратегически документи в осъществяването на политиката за национална сигурност на страната, за ефективното подобряване на държавното управление при защитата на информационната сигурност в процесите на управление на страната като цяло трябва да бъдат взети под внимание и следните ***препоръки***:

- Възприемане на единна, завършена държавна политика за осигуряване на защитени и надеждни комуникации в областта на държавното управление и националната сигурност на страната;
- Периодичен анализ и мониторинг на правно-нормативната уредба, необходима за качественото осигуряване на информационните дейности и защита на информационната сигурност в държавата;
- Създаване на механизми за повишаване информираността на обществото и гражданите по проблемите на информационната сигурност на страната и мерките по нейната защита като елемент от националната сигурност.

Днес информационната сигурност е сред новите аспекти на сигурността, превърнала се в основен субект на националната сигурност и запазване на националните интереси и суверенитет на страната. Съвременните предизвикателства пред демократичните държави обуславят и въвеждането на нови моменти при формирането на политиката по защита на информационната сигурност като част от цялостната политика по национална сигурност в контекста на европейската политика в тази област[31]. Процесите на глобализация засилват ролята на сигурността на информацията, както и необходимостта от международно сътрудничество в тази област. Въвеждането на адекватни направленията и механизми на държавното управление при осъществяването на политиката за информационна сигурност е сложен процес, свързан с оценка и анализ на генерираните нови рискове и заплахи за сигурността на страната. Информационното пространство има глобален характер, затова защитата на

---

[31] В заключенията на ЕС относно изграждането на цифровото бъдеще на Европа от 09.06.2020 е записано: „Пандемията от COVID-19 и последиците от нея за живота и икономиките ни акцентираха върху значението на цифровизацията във всички области на икономиката и обществото в ЕС. Новите технологии ни помогнаха да запазим свързаността си, да работим от дома си и да улесним дистанционното обучение на нашите деца. Те изиграха ключова роля за продължаването на стопанската дейност и обществените услуги. Цифровата трансформация не само ще спомогне за преодоляване на настоящата здравна криза, но ще бъде и основна движеща сила за икономическото възстановяване, екологосъобразния растеж и стратегическата автономност на ЕС.”. https://www.consilium.europa.eu/bg/press/press-releases/2020/06/09/shaping-europe-s-digital-future-council-adopts-conclusions/ - посетен на 10.06.2020.

информационната сигурност е невъзможно да се осъществи от отделната личност, общество или отделната държава, което налага обективната необходимост от консолидиране на сили и средства на национално, регионално и международно равнище.

Изводи от глава трета

- Рисковете и заплахите за информационната сигурност на Република България са следствие на глобалните промени във всички аспекти на сигурността, като навлизането на новите информационни и комуникационни технологии ще доведат до появата на новите типове рискове и заплахи за националната и в частност за информационната сигурност на страната.

- Изпълнението на стратегическата цел на политиката за управление при кризи се основава на изграждане на устойчива, комплексна и гъвкава Национална система за управление при кризи, която осигурява необходимите институционална рамка и инструменти за координиране и междуведомствено сътрудничество на държавното управление при кризи.

- Управлението при кризи изисква ясно представена цел и пълна готовност да се преодолеят всякакви трудности и критични ситуации чрез прилагането на Система за мониторинг и контрол на информационните процеси при взаимодействието на държавните органи в управлението на възникнали кризи на всеки един етап от протичането на процесите между ангажираните държавни органи и институции.

- Изпълнението на политиката за защита на информационната сигурност на страната може да се осъществи най-ефективно чрез правилното разпределение на задачите и координация на държавните институции чрез разработване на система от методи за нейната оценка.

ОБЩИ ИЗВОДИ:

1. Информацията е стратегически актив, който е в основата за вземане на решения на всички равнища и етапи от развитието на отделните общества и държави, тъй като всички значими социални дейности в съвременното общество (управленски, икономически, образователни, политически, отбранителни и т.н.) се осъществяват в информационното пространство, а това поставя императива за гарантиране на сигурността на циркулиращите в обществото и организациите информационни потоци посредством осигуряването на свободен и безопасен достъп до информационното пространство.

2. Като един от най-важните компоненти на националната сигурност информационната сигурност е защитеност на държавата и нейните интереси в информационната сфера на стратегическо, оперативно и тактическо равнище от всякакви опити за злоумишлени посегателства и влияния върху

информационната инфраструктура и информационни ресурси, която се реализира чрез провежданата от държавата политика, която дефинира основните направления в дейността на органите на държавната власт и местното самоуправление и реда за определяне на задълженията им в рамките на тяхната компетентност.

3. Постигането на високо равнище на информационната сигурност е стратегически проблем на политиката и управлението на националната сигурност. Определянето на информационната сигурност като критична инфраструктура на сигурността, както и значимата роля на информацията в останалите дефинирани критични инфраструктури, предпоставя конструираните параметрите на връзката между информационната сигурност и защитата на тези обекти като елемент от системата за защита на националната сигурност на страната.

4. Комплексът от мерки за усъвършенстване и гарантиране на информационната сигурност при управлението на държавните органи на Република България, основан на солидна правна база, включва институции на различни нива в системата на държавното управление, които отговарят за регулирането обществените отношения в информационната сфера. Ефективното управление на дейностите и обектите от критичната инфраструктура на държавата изисква в законодателната рамка по-точно дефиниране на понятието „критична информационна инфраструктура”, което би повишило капацитета на нейната защита.

5. Глобалните промени във всички аспекти на сигурността, вкл. навлизането на новите информационни и комуникационни технологии водят до появата на нови типове рискове и заплахи за националната и в частност за информационната сигурност на страната. Изпълнението на стратегическата цел на политиката за управление при кризи изисква изграждане на устойчива, комплексна и гъвкава Национална система за управление при кризи, която осигурява необходимите институционална рамка и инструменти за координиране и междуведомствено сътрудничество на държавното управление при кризи.

6. Управлението при кризи предполага пълна готовност за преодоляване на всякакви трудности и критични ситуации чрез прилагането на Система за мониторинг и контрол на информационните процеси при взаимодействието на държавните органи в управлението на възникнали кризи на всеки един етап от протичането на процесите между ангажираните държавни органи и институции, което е възможно да се осъществи ефективно чрез правилното разпределение на задачите и координация на държавните институции чрез разработване на система от методи за нейната оценка.

ЗАКЛЮЧЕНИЕ

Информационната революция и възникването на обществото на знанието, в което информацията е основен ресурс, налагат преосмисляне на понятията сигурност, национална сигурност и информационна сигурност. Случващото се по своята същност предлага многопосочни и разнообразни възможности за развитие и прогрес, но едновременно с това генерира и нов тип рискове и заплахи за националната сигурност на държавите – рисковете и заплахите за тяхната информационна сигурност.

Това разбиране бе водещо в работата по настоящото научно изследване и ни позволи да изпълним *целта и основните научно-изследователски задачи на дисертационния труд* - да представим състоянието на информационната сигурност в държавното управление към сегашния момент и да предложим организационно-правни мерки за повишаване на ефективността на управленските процеси чрез реализирането на интегрирана система за мониторинг и контрол на информационната сигурност при възникнали кризи като елемент от защитата на националната сигурност на страната.

В процеса на изследователската работа бяха получени *резултатите* в областта на изследваната материя - ново знание за състоянието на информационните процеси в системата на държавното управление, като са систематизирани и категоризирани възможностите за тяхното адекватно управление и са предложени нови подходи за тяхната защита в аспекта на националната сигурност.

В резултат на извършените изследвания в научното дирене е *защитена основната хипотеза* на дисертационния труд, че държавното управление може да се разглежда като система от информационни процеси, които за да функционират безпроблемно, е необходимо да бъдат надеждно защитени, за да се гарантира качеството на информацията, използвана за генериране на адекватни управленски решения. Понятията „държавно управление” и „информационна сигурност”, анализирани през фокуса и в контекста на националната сигурност, придобиват ново и актуално звучене, а изведените механизми на държавното управление при реализирането на политиките за информационна сигурност на страната намират своето приложение чрез Системата за защита на националната й сигурност. Само компетентните държавни органи в условията на действащото законодателство могат ефективно да гарантират и защитават националните интереси, териториалната цялост и суверенитета на държавата, посредством провежданата от държавата политика в защита на стабилността на институциите при компетентно управление на процесите, елиминиращи рисковете и заплахите за сигурността на държавата и запазването на икономическия и социален просперитет на страната.

IV. СПРАВКА ЗА ПРИНОСИТЕ В ДИСЕРТАЦИОННИЯ ТРУД

Научни приноси

1. Разширени и допълнени са съществуващите и са синтезирани нови научни знания, свързани с мениджмънта на информационната сигурност и информационните процеси в държавното управление, в частта за възможностите за повишаване ефективността на управлението на информационната сигурност на страната.

2. Обогатена е теорията за определяне на състоянието на информационните процеси в системата на държавното управление, като е разработена и предложена концептуална рамка на Система за мониторинг и контрол на информационните процеси при възникнали кризи.

Научно-приложни приноси

1. Разработена и предложена е информационна органиграма на структурата, дейностите и функциите на Съвета по сигурността към Министерски съвет, представяща йерархичните равнища и взаимовръзките в системата, обединяваща държавните органи и институции, специализирани в осъществяването на дейностите при овладяване и разрешаване на възникналите кризи.

2. Изведени са препоръки за повишаване на ефективността на мениджмънта при защитата на информационната сигурност в държавното управление в съответствие с императивите на приетите стратегически документи и осъществяваната политика за национална сигурност на страната.

V. ВНЕДРЯВАНЕ НА ДИСЕРТАЦИОННИЯ ТРУД

Резултатите от изследването имат както научно-теоретично, така и практическо приложение.

В *научно отношение* резултатите могат да допринесат за обогатяване и развитие на знанието в две големи научни области - управление и сигурност и по-конкретно в сферата на мениджмънта на информационната сигурност в държавното управление, както и за допълване и уточняване на основни термини и понятия от изследваната област, което като цяло води до нарастване на научния капацитет.

В *практическо отношение* се очаква приложимостта на разработката да е значима, тъй като осигурява добра платформа за системното разбиране и натрупване на познание от страна на държавните институции с цел повишавате на качеството на извършваните от тях дейности за защита на националната сигурност, и на организациите от публичния и частния сектор при осъществяването на техните мисии при защита на правата и свободите на гражданите.

Резултатите могат да послужат за усъвършенстване на учебния процес във ВА „Г. С. Раковски“, Академията на МВР, както и в други висши училища и научноизследователски организации, свързани с обучение, образование и научни изследвания в областта на националната сигурност.

VI. НАУЧНИ ПУБЛИКАЦИИ, СВЪРЗАНИ С ДИСЕРТАЦИЯТА

1. Хинова, Боряна, *Основи на информационната сигурност в обществените отношения,* В: Сборник доклади от Научни четения посветени на 140-тата годишнина от приемането на Търновската конституция, ПУ „Паисий Хилендарски“, Юридически факултет, Пловдив, 19 април 2019.
2. Хинова, Боряна, *Принципи и механизми на държавното управление като защитавана система* – В: Сборник доклади от годишна университетска научна конференция, 27-28 юни, 2019, т. 4 „Сигурност и отбрана”, НВУ „Васил Левски”, ИК, 2019.
3. Хинова, Боряна, *Доктринални основи на информационната сигурност* – В: Годишен сборник с доклади. Велико Търново: Национален военен университет „Васил Левски“ (под печат).

VII. ДЕКЛАРАЦИЯ

Декларирам, че дисертационният труд „Съвременни измерения на сигурността на информацията в държавното управление“ е изцяло авторски. При неговото разработване не са ползвани чужди публикации и разработки в нарушение на авторските права. Посочени са всички използвани литературни източници, статии, публикации, документи и информация.