ВАРНЕНСКИ СВОБОДЕН УНИВЕРСИТЕТ
„ЧЕРНОРИЗЕЦ ХРАБЪР“

ЮРИДИЧЕСКИ ФАКУЛТЕТ
КАТЕДРА „ОБЩЕСТВЕН РЕД И СИГУРНОСТ“

Д-Р ТЕОДОРА КИРИЛОВА ЛИЧЕВА

ТРАНСФОРМАЦИЯ НА УПРАВЛЕНСКИЯ ЦИКЪЛ В РАЗУЗНАВАНЕТО И КОНТРАРАЗУЗНАВАНЕТО ЧРЕЗ ИНТЕГРАЦИЯ НА СЪВРЕМЕННИ ТЕХНОЛОГИЧНИ РЕШЕНИЯ

А В Т О Р Е Ф Е Р А Т

на дисертационен труд
за придобиване на научна степен
„доктор на науките“,
професионално направление
9.1 „Национална сигурност“

Варна

2026 г.

ВАРНЕНСКИ СВОБОДЕН УНИВЕРСИТЕТ
„ЧЕРНОРИЗЕЦ ХРАБЪР“

ЮРИДИЧЕСКИ ФАКУЛТЕТ
КАТЕДРА „ОБЩЕСТВЕН РЕД И СИГУРНОСТ“

Д-Р ТЕОДОРА КИРИЛОВА ЛИЧЕВА

ТРАНСФОРМАЦИЯ НА УПРАВЛЕНСКИЯ ЦИКЪЛ В РАЗУЗНАВАНЕТО И КОНТРАРАЗУЗНАВАНЕТО ЧРЕЗ ИНТЕГРАЦИЯ НА СЪВРЕМЕННИ ТЕХНОЛОГИЧНИ РЕШЕНИЯ

А В Т О Р Е Ф Е Р А Т

на дисертационен труд
за придобиване на научна степен
„доктор на науките“,
професионално направление
9.1 „Национална сигурност“

Рецензенти:
проф. д.н. Стефан Ангелов Симеонов
проф. д-р Георги Василев Бахчеванов
проф. д.н. Боян Кирилов Медникаров

Варна
2026 г.

Дисертационният труд обхваща 475 страници и се състои от увод, три глави, заключение, приноси и библиография. Отделните глави, представени в съдържанието, са разделени на подглави и завършват с обобщения и изводи. Основният текст съдържа 94 таблици и 34 фигури.

Използваната литература се състои от 514 източника, които включват:

- международни и наднационални актове (4 източника);
- българско законодателство и стратегии (9 източника);
- чуждестранни актове и стандарти (17);
- литература на кирилица (24);
- литература на латиница (61);
- литература на китайски (5);
- интернет източници (394).

За изготвянето на дисертационния труд са използвани основно интернет източници и статии, поради бързата промяна и развитие на информационно-комуникационните комуникации и иновации, и чувствително забавяне на законодактелната рамка в сферата.

Защитата на дисертационния труд пред научното жури ще се проведе на 25.08. 2026 г. от 10,30 ч. в заседателната зала на Варненския свободен университет „Черноризец Храбър“. Материалите за защитата са на разположение в катедра „Обществен ред и сигурност“, както и на сайта на университета www.vfu.bg.

I. Обща характеристика на дисертационния труд

Настоящият дисертационен труд изследва трансформацията на управленския цикъл в сферата на сигурността под въздействието на съвременните технологични иновации. В условията на Четвъртата индустриална революция, средата за сигурност се характеризира с изключителна динамика, сложност и взаимосвързаност на заплахите (Schwab, 2018). Традиционните управленски модели са аналогови, базирани предимно на човешки фактор, експертни оценки и статични процедури. Те все по-често не успяват да отговорят на асиметричните и хибридни предизвикателства (Schwab, 2016), което налага основно преосмисляне на всички етапи от управленски цикъл:

- събиране и анализ на информацията;
- изготвяне на прогнози, прогнозни оценки и варианти за решения;
- взимане на решения и изготвяне на сценарии
- планиране;
- организиране;
- изпълнение;
- контрол и проверка на изпълнението с планираната цел.

Внедряването и използването на големи данни (Big Data), изкуствен интелект (ИИ), облачни технологии, блокчейн, дронове (БЛА) и други съвременни инструменти променя съдържанието и механизмите на управленския цикъл от събиране и обработка на информация (Laney, 2001) до вземане на решения, изпълнение и последващ контрол.

Традиционните, йерархични модели на управление се оказват все по-неадекватни

1. Актуалност и значимост на изследването

Четвъртата индустриална революция (Индустрия 4.0) поставя основата на коренна трансформация в начина, по който функционират институциите за национална сигурност (Радулов, 2019). Разузнаването и контраразузнаването, които са ключови стълбове на държавната архитектура за сигурност, са изправени пред безпрецедентни предизвикателства, породени от бързото развитие на дигиталните технологии, глобализацията и свръхобема на информационните потоци (World

Актуалността на изследването произтича от обективната необходимост за адаптиране на системите за национална сигурност към новата технологична среда.

Интеграцията на технологии като изкуствен интелект, анализ на големи данни, облачни изчисления, блокчейн и автономни системи не е просто техническо усъвършенстване, а стратегическа необходимост за постигане на информационно и оперативно превъзходство. Значимостта на темата се определя от няколко ключови аспекта:

- **Научно-теоретична значимост:** И следването допринася за развитието на теорията на управлението в сигурността, като предлага нов концептуален модел за трансформация на управленския цикъл, който синтезира и адаптира класически управленски принципи с възможностите на дигиталните технологии.
- **Научно-приложна значимост:** Разработените модели, анализи и препоръки имат пряка практическа стойност за държавните институции в разузнаването и контраразузнаването на Република България. Те предоставят методическа основа за модернизация, дигитализация и повишаване на ефективността на разузнавателните и контраразузнавателните структури в съответствие с най-добрите евроатлантически и световни практики.

Темата е изключително актуална предвид ускорената дигитализация на публичния сектор, засилените международни регулаторни изисквания и нуждата от модернизиране на националните институции за сигурност.

2. Обект на изследването

В съответствие с поставената цел и задачи, в дисертационния труд са дефинирани следните обект и предмет на изследване:

- Обект на изследването е управленският цикъл в системите за разузнаване и контраразузнаване – разгледан в неговата цялост от взаимосвързани процеси, включващ фазите събиране и анализ на информацията; изготвяне на прогнози, прогнозни оценки и варианти за решения; взимане на решения и изготвяне на сценарии; планиране; организиране; изпълнение; контрол и проверка на изпълнението с планираната цел. Всички етапи са реализирани в контекста на съвременните предизвикателства за националната и международната сигурност.
- **Предмет на изследването** са процесите на трансформация на управленския цикъл, породени от интеграцията на технологични иновации. Анализът е фокусиран върху начините, по които новите технологии променят дейността на управлението в разузнавателните и контраразузнавателните структури на национално и международно равнище, както и върху възникващите нови управленски модели и стратегии.

. Цели и задачи на дисертацията

Тезата на дисертационния труд е, че съвременните управленски процеси са неизбежно свързани с технологичния прогрес и тяхното развитие по същество е експоненциално, каквото е развитието на съвременните технологии. Управлението и средата на сигурност са адекватни на икономическото развитите, като това определя и тяхната ефективност.

Екосистемата за сигурността е по-чувствителна към процесите, които се развиват в политиката икономиката и обществено-социалните процеси, поради което необходимостта от бърз дигитален преход и използване на високотехнологични решения е залог не само за ефективност, но и за справяне със съвременни предизвикателства в сигурността.

С оглед на гореизложеното, ***целта*** на изследването е да се установят тенденциите в развитието и усъвършенстването на елементите и същността на управлението в сигурността при преминаването от аналогово към технологично дигитално управление. На базата на изследването на съществуващата до момента информация предлагам рамки и концепции за модернизиране и повишаване на ефективността на управлението в сигурността. Моделирането на съвременни интензивни сценарии за управление улеснява практическата дейност по ефективно ръководене в сложната екосистема на сигурността и едновременно създава възможност за адекватно реагиране при съвременни заплахи. Предизвикателствата пред сигурността са тясно свързани с развитието на съвременните технологии и съответно противодействието и управлението на кризите, свързани с тях, не могат да бъдат други освен високотехнологични.

За постигането на тази цел поставям следните ***научноизследователски задачи:***

1. Съпоставяне на класическото с дигиталното управление за изясняване на общите моменти и разлики;

2. Извеждане на ролята и значението на всяко едно от новите технологични направления по отношение на елементите на управленския цикъл;

3. Определяне на рамките и сценариите на развитие на всяка една технология по отношение на отделните фази на управленския цикъл;

4. Изследване на синергията на съвременните технологии по отношение на повишената ефективност на дигиталното управление в сигурността.

Методология на изследването

Методологичната рамка на дисертационния труд, е поставена на пресечната точка между управление, национална сигурност и съвременни информационно-комуникационни технологии.

Използваните методи са подбрани така, че да осигурят системен, многопластов и интердисциплинарен анализ на националната система за сигурност, трансформацията на управленските практики и влиянието на иновативните технологии върху тях. Методологичният апарат включва общонаучни, специализирани и приложни методи, които в своята цялост формират интегрирана изследователска рамка, съчетаваща описателни, аналитични и прогностични елементи, както и изготвяне на сценарии и създаване на описателни модели.

Общонаучни методи

Анализ и синтез – при изследването на теоретични постановки и обобщаване на данни от различни източници;

Индукция и дедукция – за формулиране на изводи от частни случаи към общи закономерности и обратно

Специализирани методи и подходи

Системен и структурно-функционален подход – за разглеждане на управленския цикъл като единна система от взаимосвързани елементи

Управленски анализ – за конструиране на матрици и модели, които показват приложимостта на различни технологични решения по етапи на цикъла и по нива на управление (стратегическо, тактическо, оперативно).

Документален и правно-аналитичен метод

Документален и правно-аналитичен похват – изследване на нормативната и стратегическата рамка на системата за сигурност на национално и международно ниво: стратегии и концепции за сигурност, закони и подзаконови актове, регулаторни режими, доклади и документи на международни организации.

Анализ на съдържанието – за извличане на ключови понятия, приоритети и доминиращи концепции.

Исторически и сравнителни подходи

Историко-генетичен метод – за проследяване еволюцията на системата за сигурност и управленските модели в различни исторически периоди.

Историко-сравнителен и сравнителен анализ – за съпоставя развитието на българската система за сигурност с аналогични системи в други държави.

Сравнителният анализ – за сравняване на управленски модели и практики в държави със силно развити разузнавателни структури, водещи в технологично страни и България.

Сценарен и прогностичен анализ, сценарии и описателни модели

Сценарен анализ и изготвяне на сценарии – за разработване на алтернативни възможни развития на системата за сигурност при ускорена технологична еволюция.

Моделиране – за разработване на концептуални модели за трансформация на управленския цикъл

Прогностичен анализ – за очертаване на най-вероятните тенденции в развитието на технологиите, управленските практики и регулаторните режими в средносрочна и дългосрочна перспектива.

Интегрирана методологична матрица

Комбинацията от системен и структурно-функционален подход, управленски анализ, общонаучни методи (анализ, синтез, индукция, дедукция), исторически и сравнителни подходи, анализ на съдържанието, както и сценарен и прогностичен анализ, изготвяне на сценарии и създаване на описателни модели, формира интегриран методологичен модел на дисертацията.

Изследването стъпва на широк кръг от източници – научни публикации, монографии, стратегически документи на национални и международни организации, нормативни актове и доклади от водещи изследователски центрове.

. Приноси

Извършеният анализ в дисертацията, касаещ управленските етапи в сигурността е принос за България, и е на база на изследванията, които показаха, че страната изостава значително по отношение на внедряване и използване на новите технологични възможности в разузнавателната и контраразузнавателната дейност.

Основният принос е формулиране на миграцията на елементите на управленския цикъл, характерни за службите за сигурност, от традиционни и аналогови, към модерни дигитални процеси, включващи спецификите на отделените нива на управление според времевия хоризонт и структурните нива в системата на националната сигурност.

Теоретико-научни приноси

ормулирана е концепция за цифрово управление на сигурността;

азработен е интердисциплинарен модел за интеграция на новите технологии в управлението на сигурността;

зведени са и формализирани матрични модели и шаблони за приложение на ключови технологии;

редложен е нов прочит на развитието на българските служби за сигурност чрез задълбочен историко-институционален анализ;

азработена е етико-правна и управленска рамка на технологичната трансформация в сигурността;

азработена е цялостна концептуална рамка на управленския цикъл в сигурност в контекста на Индустрия 4.0–6.0 и Сигурност 4.0–6.0;

истематизирана и сравнително анализирана е еволюцията на сигурността от Сигурност 1.0 до Сигурност 5.0 (и тенденции към 6.0).

Практическо-приложни приноси

ъздадени са приложими аналитични инструменти за стратегическо планиране и реформи в сигурността;

азработени са рамки за измерване ефективността на управленския цикъл чрез конкретни технологии в разузнаването и контраразузнаването;

пределени са направления и модели за обучение и развитие на човешкия ресурс в контекста на дигиталната трансформация;

редложени са насоки за усъвършенстване на нормативната и етична рамка, свързана с използването на нови технологии в сигурността;

зградена е практическа рамка за поетапен преход от аналогов към цифров управленски цикъл;

ъздадена е референтна рамка за оценка на технологичното изоставане и рисковете за националната сигурност, основа на сравнителни казуси и индикатори за технологична зрялост.

. Практическо значение на изследването

Практическото значение на дисертационния труд е многопластово. То обхваща приложения на национално, институционално и оперативно ниво. Практическото значение е систематизирано в следните основни направления:

Рамки за измерване ефективността на управленския цикъл

В изследването са разработени конкретни рамки и матрични модели за измерване на ефективността на управленския цикъл чрез специфични технологии в разузнаването и контраразузнаването. Тези рамки могат да служат като

практически ръководства при проектиране и внедряване на технологични решения в службите за сигурност, защото показват приложението на различни технологични решения по етапи на цикъла и по нивата на управление – стратегическо, тактическо и оперативно.

Обучение и развитие на човешкия ресурс

Дефинирани са направления и модели за обучение и развитие на служителите в контекста на дигиталната трансформация. Тези модели могат да бъдат използвани при изграждането на учебни програми, вътрешноинституционални обучения и сценарийни тренинги с елементи на виртуална и добавена реалност (AR/VR), включително симулационни среди за подготовка на кадри.

Адаптиране на нормативната и етична рамка

Предложени са насоки за подобряване на нормативната и етична рамка, свързана с използването на нови технологии в сигурността. Те могат да бъдат използвани при подготовка на законодателни промени, вътрешни политики и механизми за независим одит, оценка и мониторинг, като отчитат рисковете от масово наблюдение, алгоритмична пристрастност и нарушаване на личната сфера.

Концептуален модел за цифрово управление на сигурността

Дисертацията предлага конкретен концептуален модел за цифрово управление на сигурността, приложим на практика. Моделът предвижда изграждането на съвременни дигитални платформи, системи за предикативен анализ, дигитални близнаци на критичната инфраструктура, внедряване на архитектура „нулево доверие“ (ROSE et al., 2020) и постквантови криптографски решения.

Принос за България и евроатлантическата интеграция

Особено значимо е практическото приложение в **българския контекст**. Изследването установява, че България изостава значително по отношение на внедряване и използване на съвременни технологични възможности в сферата на сигурността сектор, поради ограничен ресурсен капацитет, остаряла информационна инфраструктура и недостиг на висококвалифицирани кадри. Резултатите от изследването могат да послужат като основа за разработване на национална стратегия за дигитална трансформация, в която науката, държавните институции и частният сектор да действат като партньори и работят в синхрон.

Оперативно предимство и управление на заплахи

Моделирането на съвременни интензивни сценарии за управление улеснява практическата дейност по ефективно ръководене в сложната екосистема на

сигурността. Интеграцията на блокчейн, ИИ и големи данни в оперативния цикъл дава конкретни инструменти за преминаване от реактивно разследване към превантивно прогнозиране на заплахи, в това число и на хибридни и киберзаплахи, което е решаващо за националната сигурност.

Практическото значение на изследването се изразява в предоставянето на приложими рамки, модели и стратегически насоки, чрез които разузнавателните и контраразузнавателните структури могат реално да модернизират своя управленски цикъл и да придобият трайно оперативно предимство в условията на съвременната дигиталната ера.

Ограничения

Изследването има съществени ограничения, които следва да бъдат взети под внимание при интерпретацията на резултатите и формулираните изводи.

На първо място ограниченията, са, че ***сигурността се разглежда в ограничения формат*** на службите за сигурност, а именно:

- Разузнаване;
- Контраразузнаване;

На второ място, ***ограничен е географският и сравнителният обхват***. Анализът е фокусиран върху ограничен набор от държави, подбрани въз основа на тяхната водеща роля в международната система, наличието на достатъчно публично достъпни данни, и България.

На трето място, ***използваната база с източници е главно от публично достъпни документи,*** академична литература, стратегически и нормативни актове, както и специализирани анализи.

Четвърто, ***изследването има времеви хоризонт, ограничен до процеси и данни към 2025 г.***, поради бързото развитие на технологиите и предложените тенденции следва да се възприемат като т.нар. моментна **снимка,** а не като окончателна и непроменлива картина.

Пето, ***по отношение на България изследването среща специфични ограничения в наличието и детайлността на публичните данни.***

На шесто място, част ***от формулираните препоръки и модели са с нормативен и стратегически характер***.

Основно съдържание на дисертационния труд

1. Структура на изследването

Увод

ГЛАВА I. Еволюция на сигурността

Раздел I. Промишлените революции и развитие на сигурността

Раздел II. Управление на сигурността

1. Сравнителен анализ на управлението на сигурността в различни държави

2. Управление на сигурността в България

3. Методи за управление на сигурността

4. Етапи на управленския цикъл в сигурността

5. Трансформация на управленския цикъл в дигиталната среда

6. Управленският цикъл в сигурността: Индустрия 4.0, Индустрия 5.0 и Индустрия 6.0

Изводи

ГЛАВА II. Новите технологии в сигурността

Раздел I. Големите данни

1. Възприемане на големи данни и съвременни предизвикателства

2. Сравнителен анализ: глобални срещу български възможности

Раздел II. Изкуствен интелект

1. Практически казуси

2. Ключови етапи в използването на ИИ в сигурността

3. Международен и български опит. Сравнение

Раздел III. Облачни изчисления

1. Технологично развитие на сигурността

2. Приложение на облачните решения в сигурността. Международен и български опит. Сравнение

3. Периферни изчисления

4. Поверителни изчисления

Раздел IV. Технологията блокчейн

1. Интегриране на блокчейн в сигурността

2. Приложения в световен аспект и България. Сравнение

3. Постквантова защита на блокчейн системи

4. Умни договори в сигурността

5. Служебни е-досиета

Раздел V. Дронове

Раздел VI. Адитивни технологии

Раздел VII. Нанотехнологии

1. Нано-устройства и материали с приложение в сигурността

2. Приложения на нанотехнологиите в сигурността в глобален и български аспект. Сравнение

Раздел VIII. Геотехнологии

1. Геотехнологии в специалните служби – световен и българки контекст. Сравнение

. Национални законодателства и механизми за контрол

Раздел IX. Виртуална и добавена реалност

1. Приложения на виртуалната реалност сигурността

2. Приложения на добавената реалност в полеви операции

3. Сравнителен анализ и казуси: международен опит и България

Раздел X. Космически технологии

1. Приложения на космическите технологии в сигурността

2. Казуси и оперативни задачи в международен аспект и България. Сравнение

Раздел XI. Синергия между технологиите в сигурността

1. Дигитални близнаци

2. Мека роботика

3. Концепция „Нулево доверие”

Раздел XII. Сигурност на данните

Изводи

ГЛАВА III. Цифрово управление на сигурността

Раздел I. Големите данни

1. Събиране, обработка и анализ на информацията

2. Прогнозиране и подготовка на управленски решения

3. Взимане на управленско решение: Процеси и рамки

4. Планиране и организиране на изпълнението на решенията

5. Изпълнение и контрол

Раздел II. Изкуствен интелект

1. Разузнаване

2. Контраразузнаване

Раздел III. Облачни изчисления

1. Събиране, обработка и анализ на информация в облачна среда

2. Прогнозиране и подготовка на управленски решения

4. Планиране и организиране

Описание на главите

Увод

Уводът има за цел да постави рамката на дисертационния труд. В него са обосновани актуалността, предметът и обектът на изследването, целите и задачите на работата, приложената методология. Очертана е рамката на изследването, като се поставя акцент върху практическата приложимост на новите информационни и комуникационни технологии, със стратегически ползи за повишаване на ефективността и сигурността на разузнавателните служби. От поставените в него граници логически произлизат следните 3 глави.

Глава I: Еволюция на сигурността

Първа глава от дисертационния труд представя историко-сравнителен анализ на еволюцията на сигурността, разглеждайки как технологичните трансформации, породени от индустриалните революции, са повлияли на методите и инструментите в разузнаването и контраразузнаването. Анализът проследява развитието от първите механизирани системи до прогностични модели, базирани на квантови технологии и изкуствен интелект.

Глава I е организирана в два основни раздела: **„Промишлените революции и развитие на сигурността“** и **„Управление на сигурността“**, като вторият включва шест подраздела, обхващащи сравнителен анализ на управленските системи в различни държави, институционалното развитие в България, методите и етапите на управленския цикъл, трансформацията му в дигиталната среда и сравнителния анализ на сигурността в контекста на Индустрия 4.0, 5.0 и 6.0.

Основни тези и научни резултати

1. Промишлените революции като движеща сила на трансформацията

Първостепенен изследователски принос на главата е систематизирането на еволюцията на сигурността успоредно с хронологията на индустриалните революции. Авторът доказва, че всяка промишлена революция генерира специфичен тип заплахи и налага съответна трансформация в разузнавателните и контраразузнавателните структури.

Първата индустриална революция (Индустрия 1.0) поставя основите на структурираното разузнаване. В този период се появяват първите агентурни мрежи за наблюдение на работнически движения и зараждат се институциите за защита на промишлените тайни. Парният двигател и железопътният транспорт служат като

инструменти за разгръщане на разузнавателна дейност и прихващане на комуникации.

Втората индустриална революция (Индустрия 2.0) въвежда телефона и телеграфа като стандартни инструменти на разузнаването и контраразузнаването, а индустриалният шпионаж придобива международен характер. Важно е да се отбележи, че фотографията навлиза като средство за събиране на информация.

Третата индустриална революция (Индустрия 3.0) е свързана с появата на електронното разузнаване (SIGINT), анализа на Големи данни и международните мрежи за сигурност. Дигитализацията налага киберсигурността като ключов компонента на контраразузнаването.

Четвъртата индустриална революция (Индустрия 4.0) бележи навлизането на изкуствения интелект (ИИ), Интернета на нещата (IoT) и автономните системи в сигурността. Разузнаването разработва ИИ-базирани инструменти за анализ на масиви от данни, а контраразузнаването се насочва към защита срещу IoT-заплахи и кибератаки (Радулов, 2019).

Петата индустриална революция (Индустрия 5.0) въвежда симбиозата между човека и интелигентните машини. Появяват се нови предизвикателства, свързани с геномния шпионаж, злоупотребата с биометрични данни, невротехнологиите и квантовите компютри.

. Еволюция на концепцията за сигурност – от Сигурност 1.0 до Сигурност 6.0

Представена е систематизирано еволюцията на сигурността в пет последователни рамки, всяка от които отразява специфичните нужди на съответната технологична ера:

- **Сигурност 1.0** – физическа защита, ограничени механични методи;
- **Сигурност 2.0** – стандартизирани индустриални протоколи и процедури;
- **Сигурност 3.0** – защита на ранните информационни системи, криптография и антивирусни програми;
- **Сигурност 4.0** – интегрирана киберсигурност за свързани системи, IoT-защита, блокчейн и машинно обучение;
- **Сигурност 5.0** – човекоцентрична, устойчива и гъвкава защита, при която технологиите служат на човека (Личева, 2024), а не обратното, и при която физическата и цифровата сигурност се сливат в единна система;
- **Сигурност 6.0**, е прогностичен етап, където се анализират както потенциалните заплахи от квантовите изчисления за съществуващите

криптографски системи, така и възможностите, които квантовата криптография предлага за създаване на непробиваеми комуникационни канали.

Ключов теоретичен принос е концептуализирането на Сигурност 5.0 като концепция, при която се изисква: превантивност и предсказуемост чрез ИИ и големите данни; сближаване между физическата и киберсигурността; подобрена публично-частна интеграция; и хуманоцентрични системи, съобразени с етичните стандарти и защитата на личните данни.

Авторът детайлно изследва етапите на управленския цикъл в разузнаването и контраразузнаването, включващи стратегическо планиране, събиране и анализ на информация, прогнозиране, взимане на решения, организиране, изпълнение и контрол. Аргументира се, че с навлизането на дигиталните технологии всеки от тези етапи претърпява качествена трансформация.

Особено внимание се отделя на промяната в ролята на ръководителя – от администратор на рутинни процеси към стратегически лидер, ориентиран към данни и технологично оптимизиране на организацията. Въвеждането на „смарт анализи“, базирани на ИИ, позволява сценарийно планиране и предикативно управление на риска в реално време.

Сравнителен анализ: Сигурност 4.0 – 5.0 – 6.0

В изследването е разработен детайлен сравнителен анализ на управленския цикъл в трите последователни фази на развитие на сигурността:

Таблица 1. Сравнителен анализ на управленския цикъл от Сигурност 4.0-Сигурност 6.0

Управленски етап	***Сигурност 4.0***	***Сигурност 5.0***	***Сигурност 6.0***
Събиране на информация	IoT/SCADA, човешки анализ	ИИ, биометрия, автоматично валидиране	Автономни агенти, квантово криптиране
Прогнозиране	Исторически данни, шаблони	Машинно обучение, невронни мрежи	Самонастройващи се ИИ модели, квантови симулации
Взимане на решения	Центриран около човека	ИИ препоръки, валидирани от човека	Автономни решения, човешка намеса само при гранични случаи

Планиране	Твърдо, годишно	Динамично, реалновременно	Самокоригиращо се, адаптивно
Организиране	Йерархично, статично	Хибридно, гъвкаво	Самоуправляващи се мрежови структури
Контрол	Изцяло човешки	Интерактивен ИИ, автоматизация	Напълно автономен, самовъзстановяващ се

Управление на сигурността в България

В рамките на историко-институционалния анализ се проследява развитието на българските служби за сигурност – от централизирания апарат на Държавна сигурност (ДС) в периода на Студената война до реформирането и създаването на ДАНС и ДАР след 1989 г. Констатира се постепенен, но последователен преход към архитектура, съвместима с евроатлантическите стандарти, съпроводен с нарастващи инвестиции в технологична модернизация и киберсигурност.

Изводи на главата

Изводите от Глава I могат да бъдат обобщени в три ключови констатации.

Първо, управлението на сигурността представлява сложна, многопластова и динамично развиваща се система, в която се пресичат исторически наследства, правни и етични рамки и технологичен прогрес.

Второ, устойчивостта и ефективността на разузнавателните служби вече не могат да се мислят извън контекста на внедряването на информационни системи, изкуствения интелект, киберсигурността и мрежовата свързаност на критичната инфраструктура.

Трето, технологичната интеграция трябва да бъде съпроводена от устойчиви нормативни, етични и институционални механизми с ясни режими на отговорност, системи за одит и независим надзор, за да се гарантира баланс между ефективност и защита на гражданските права.

Основният извод безспорно доказан е, че бъдещето на управлението на сигурността зависи от успешното съчетаване на три взаимозависими измерения: технологична иновация, демократичен контрол и стратегическа визия за интегриран, устойчив управленски цикъл, адекватен на предизвикателствата на XXI век.

Глава II: Новите технологии в сигурността

Глава II е най-обемната и технологично насочената част в дисертационния труд. Тя обхваща дванадесет раздела:

- ✓ Големите данни;
- ✓ Изкуствен интелект;
- ✓ Облачни изчисления (включително периферни и поверителни изчисления);
- ✓ Технологията блокчейн;
- ✓ Дронове;
- ✓ Адитивни технологии;
- ✓ Нанотехнологии;
- ✓ Геотехнологии;
- ✓ Виртуална и добавена реалност;
- ✓ Космически технологии;
- ✓ Синергия между технологиите в сигурността (цифрови близнаци, мека роботика, архитектура „Нулево доверие“);
- ✓ Сигурност на данните.

Основни тези и научни резултати

1. Големи данни — от реактивен анализ към предикативно разузнаване

Авторът категорично доказва, че интегрирането на Големи данни представлява структурна трансформация на управлението на специалните служби. Преходът от реактивно проучване на конкретни случаи към проактивно, предикативно разузнаване, задвижено от непрекъснат анализ на масивни обеми от разнородни данни в реално време, е очертан като стратегическа цел. Ключовите характеристики на Големите данни – обем (Volume), скорост (Velocity), разнообразие (Variety), достоверност (Veracity) и стойност (Value) са анализирани в контекст на конкретните предизвикателства пред разузнавателните структури

Сравнителният анализ между глобалните разузнавателни способности (NSA на САЩ обработва над 1,7 млрд. комуникации дневно) и българските структури категорично показва структурно изоставане по технологичен капацитет, финансиране и нормативна готовност.

2. Изкуствен интелект – ключово технологично ядро на сигурността

ИИ се очертава като двигател на съвременното разузнаване. Авторът на изследването систематизира историческото му развитие в четири ключови етапа — от ерата на експертните системи (1970–1980-те г.), през биометрията и разпознаването на образи (1990-те г.), до дълбокото обучение и генеративния ИИ (2020-те г.).

Ключовите приложения включват: автоматизиран OSINT анализ; обработка на естествен език (NLP) за засичане на пропаганда и заплахи в киберпространството; компютърно зрение за анализ на сателитни и дронови изображения; и машинно обучение за откриване на аномалии във финансови трансакции и мрежов трафик.

Поставят се и **критични ограничения**: проблемът с „черната кутия“ на ИИ решенията, риска от алгоритмична пристрастност, уязвимостта на тренировъчните данни към „отравяне“, и нарастващата трудност при анализ на криптирани комуникации. Законодателната рамка (вкл. ЕС Регламент 2024/1689 за ИИ) е разгледана като задължително условие за легитимна и демократично контролирана употреба (Европейски парламент и съвет на ЕС, 2024).

В дисертацията са систематизирани четири ключови направления с перспективи до 2030 г. – обясним ИИ, генеративен и мултимодален ИИ, федеративно обучение за сигурност на системите и консолидирани международни регулации.

3. Облачни изчисления, периферни и поверителни изчисления

Облачните технологии са определени като критична инфраструктурна основа за съвременното управление на сигурността.

В изследването са анализирани три взаимодопълващи се концепции са анализирани в синергия:

Облачни изчисления предоставят мащабируемо съхранение и бърза обработка на петабайтни масиви от разузнавателни данни, улесняват международната оперативност между агенции и съюзници и позволяват бързо внедряване на ИИ модели.

Периферни изчисления (Edge Computing) изместват критичните функции към „ръба“ на мрежата. Те са близо до физическия източник на данни или заплаха, като елиминират закъсненията при обработка на чувствителна информация в реално време. Разглеждат се ключови проекти по държави, включително приложения в охрана и наблюдение.

Поверителни изчисления (Confidential Computing), базирани на Доверени среди за изпълнение (TEE), позволяват обработка на класифицирана информация дори в публична облачна среда, без компрометиране на поверителността. Поверителните изчисления са ключова технология за съвместни операции с партньорски служби.

4. Блокчейн – децентрализирано доверие и неизменимост на данните

Блокчейн е анализиран като основополагаща промяна в управлението на разузнавателна информация. Четири са фундаментални характеристики на технологията (Nguyen et al., 2021) – неподправеност на данните, прозрачност на операциите, децентрализирана защита и умни договори. Те са приложени конкретно към всеки етап на управленския цикъл в сигурността.

Авторът поставя особен акцент е върху постквантовата защита на блокчейн системите като неотложен стратегически приоритет (量子密钥分发密码协议, инструмент за информационна сигурност, оперативна ефективност и защита на в

е

р В разработката е представен сравнителният анализ, който показва, че докато и световен мащаб се наблюдава активно внедряване, **България се намира в начален, предимно изследователски етап** без доказателства за оперативно в внедряване в разузнавателните структури.

т **5. Дронове, Адитивни технологии и Нанотехнологии**

а **В изследването дроновете** са систематизирани като инструмент с двойна функция: разузнавателна (наблюдение, IMINT, картографиране) и к контраразузнавателна (засичане и неутрализиране на враждебни БЛА). А Анализирани са правните и оперативни предизвикателства, включително рискът от употребата им от престъпни организации.

д **Адитивните технологии** (3D, 4D, 5D печат) трансформират управленския ц цикъл чрез бързо прототипиране и децентрализирано производство по заявка на к критични активи. Същевременно разпространението им създава сериозна к контраразузнавателна заплаха, като производство на нелегални оръжия и в вкимиращи устройства.

а **Нанотехнологиите** са анализирани като стратегическа кооперативна технология на оперативните способности на разузнавателните служби – от е свръхчувствителни сензорни мрежи и нанодоспехи до изчезваща електроника и к квантова криптография с нанокристали. В дисертацията се констатира, че д държавите без системна интеграция на нанотехнологии рискуват не просто технологично, а структурно разузнавателно изоставане.

в

а

6. Геотехнологии, VR/AR и Космически технологии

Геотехнологиите. Това са ГИС, сателитно разузнаване, ГНСС и БЛА с геопространствен анализ. Те са утвърдени като ключов и незаменим ресурс на разузнавателните служби. Анализирани са националните законодателства и механизмите за контрол.

Виртуалната (VR) и добавената реалност (AR) коренно променят методите за обучение на служителите, полевите операции и ситуационната осведоменост за предоставяне на контекстуална информация в реално оперативно пространство

Космическите технологии са определени като гръбнак на съвременното разузнаване, защото осигуряват несравними възможности за глобално и постоянно наблюдение. Анализирани са конкретни приложения по всички седем фази на управленския цикъл – от сателитно IMINT и сигнализиращо разузнаване (SIGINT) до навигация и сигурни комуникации.

7. Синергия и системна интеграция на технологиите

В дисертацията се представени и анализирани три синергични концепции:

Цифровите близнаци (Digital Twins) позволяват симулиране на атаки, предварително тестване на защити и предикативен анализ на сложни системи, без риск за реалните инфраструктури. Очаква се до 2030 г. да станат стандартен инструмент за националната сигурност в развитите страни (Gartner, 2024).

Меката роботика предлага гъвкави роботизирани системи за наблюдение и защита на инфраструктура в труднодостъпна среда.

Концепцията „Нулево доверие“ (Zero Trust Architecture) е анализирана и определена от автора като съвременен стандарт за киберсигурност. Тя се основана на принципа „Не вярвай никому, проверявай всичко“ (NIST, 2020) (Gartner, 2023). Концепцията е приложена към разузнавателната и контраразузнавателна среда и анализът доказва, че при успешно внедряване намалява риска от вътрешни атаки с

8. Сигурност на данните

Последният раздел от Втора глава на изследването систематизира цялостния жизнен цикъл на данните – от генерирането им до унищожаването, като структурира защитата около три ключови признака: поверителност, цялост и наличност. Разгледани са методите за класификация, криптиране (симетрично и асиметрично), маскиране, архивиране (стратегия 3-2-1) и технологиите за

предотвратяване на загуба на данни (DLP). Принципите на GDPR (Европейски парламент и съвет на ЕС, 2016) са представени като регулаторна рамка за отговорна обработка на лични данни от службите за сигурност.

Изводи на главата

Обобщеният анализ на Глава II доказва, че сигурността навлиза в етап на пълна технологична трансформация, при която всички процеси се реорганизират около интегрираното внедряване на разнородни, но взаимодопълващи се технологии.

Три са ключовите теоретични констатации.

Първо, ИИ и Големите данни се очертават като ядро на новата концепция за сигурност, позволявайки преминаване от традиционен анализ към предикативно управление на риска.

Второ, блокчейн, поверителните изчисления и архитектурата „нулево доверие“ (Taylor, 2022) не са само инструменти за по-висока ефективност, но и за по-голяма проверимост, проследимост и демократичен контрол върху употребата на мощни инструменти за наблюдение, балансирайки разузнавателните методи с гражданските права.

Трето, технологичната модернизация на сигурността не може да се разглежда изолирано от правната, етичната и организационната среда. Рисковете от масово наблюдение, алгоритмична пристрастност и автоматизирано взимане на решения изискват устойчиви нормативни рамки, ясно разпределена отговорност и независим институционален надзор.

Авторът поставя особено важен акцент за структурното изоставане на България: то е пагубно и се задълбочава от хроничен недостиг на финансиране, квалифицирани кадри, остаряла нормативна рамка и доминираща ориентация към минимизиране на рисковете, вместо към превантивни дейности и технологично изпреварване.

Глава III: Цифрово управление на сигурността

Глава III е синтезиращата и приложна кулминация на дисертационния труд. Тя съдържа десет раздела, всеки от които проследява конкретна технология, а именно Големи данни, Изкуствен интелект, Облачни изчисления, Блокчейн, Дронове, Адитивно производство, Нанотехнологии, Геотехнологии, Виртуална и

добавена реалност и Космически технологии, като анализира нейното специфично въздействие върху всеки от седемте управленски етапа в разузнавателния и контраразузнавателния цикъл.

Концептуална рамка на главата

Авторът формулира изходната теза в увода: **съвременните технологични трансформации променят в дълбочина всички етапи на управленския цикъл в сигурността** – от анализ и планиране, през взимане на решения, до изпълнение и контрол. Новите технологии не надграждат само отделни процеси, а **налагат качествена системна промяна**, при която цифровизацията, ИИ, Големите данни, облачните услуги и киберсигурността превръщат традиционната последователност от управленски дейности в динамична, автоматизирана система, ориентирана към данните в реално време.

За аналитична рамка авторката въвежда **матричен модел**, структуриран по двете оси – **седем управленски етапа** (събиране на информация; прогнозиране; взимане на решение; планиране; организиране; изпълнение; контрол) и **три нива** на управление (стратегическо, тактическо, оперативно).

Таблица 2. Шаблон за създаване на рамка за влияние на новите технологии върху етапите на управленския цикъл и нивата на управление в сигурността

Етапи на управленски цикъл / **Нива на управление**	***Събиране и анализ на информация***	***Изготвяне на прогнози, прогнозни оценки и варианти за решения***	***Взимане на решение и изготвяне на сценарии***	***Планиране***	***Организиране***	***Изпълнение***	***Контрол и проверка на изпълнението с планираната цел***
Стратегическо управление							
Тактическо управление							
Оперативно управление							

Всяка разгледана технология е картографирана към тази матрица поотделно за разузнаването и за контраразузнаването.

Основни тези и научни резултати по раздели

Големи данни - преход от реактивен анализ към проактивно управление

Приложението на Големите данни коренно преобразува традиционните, реактивни процеси в проактивен и силно автоматизиран управленски цикъл. На етапа на събиране и анализ на информацията интегрираните платформи позволяват едновременна обработка на разнородни, масивни потоци от данни, от SIGINT, OSINT, биометрика и финансови трансакции, като значително ускоряват с

и На етапа на прогнозиране инструментите генерират динамични оценки и т предикативни сценарии в реално време, заменяйки интуитивните и статистически у прогнози с машинно учене. При взимане на решения авторът идентифицира преход о от колегиален, опитно-базиран избор към **данни-управлявани решения, подкрепени от аналитични рамки и инструменти за оценка на въздействието** (к класификационни матрици, ситуационни таблици, примерни структури за о междуструктурни екипи).

н На етапите на изпълнение и контрол автоматизираните системи за м мониторинг и проследяване на резултати осигуряват по-тясна връзка между а планирани цели и реално изпълнение.

т **2. Изкуствен интелект – дигитализация на управленския цикъл в р разузнаването и контраразузнаването**

Тази част е базирана на детайлна сравнителна матрица на три паралелни у управленски модела: традиционен (аналогов), дигитализиран без ИИ и д дигитализиран с ИИ. Тя систематизира приносите и рисковете на изкуствения и интелект на всеки от седемте управленски етапа.

е

д

о

м

е

н

о

с

т

Таблица 3. Миграция от аналогови към дигитални процеси в управленския цикъл на сигурността

Елемент на цикъла	*Традиционен (аналогов) подход*	*Дигитализиран подход без ИИ*	*Дигитализиран подход с ИИ (състояние/тенденция)*	*Основни ползи от ИИ*	*Ключови рискове/ограничения*
Събиране и анализ	Ръчно събиране, хартиени носители, човешки анализ	Електронни бази данни, ръчен анализ от специалисти	Автоматизиран OSINT/SIGINT, биометрия, клъстеризация и аномалийно откриване	Скорост, обхват, откриване на скрити зависимости	Зависимост от данни, „черна кутия“, уязвимост към манипулации
Прогнозиране	Интуитивни оценки, експертни съвети	Статистически прогнози	Предикативно разследване, прогнозиране на кибератаки, симулации	Проактивност, оптимизация на ресурси	Алгоритмична пристрастност, свръхдоверие към моделите
Взимане на решения	Колегиален/индивидуален експертен избор	Подкрепени с електронни информационни системи	Решения, подпомогнати от обясним ИИ и прогнозни модели	По-добра осведоменост, многофакторен анализ	Прехвърляне на отговорност към „машината“
Планиране и организиране	Текстови планове, йерархични разпореждания	Софтуер за планиране, електронни работни потоци	Интелигентни системи за оптимизация, адаптивно преразпределяне на ресурси	Гъвкавост, синхронизация между служби	Сложност на интеграцията със стари системи
Реализация	Тактически екипи, радиовръзка, ръчни отчети	Цифрови комуникации, GPS, базови сензори	Автономни системи, дронове, интелигентни сензори, киберзащита чрез ИИ	Реагиране в реално време, намален човешки риск	Технически откази, компрометиране на ИИ системи
Контрол	Постфактум отчети, инспекции	Работни дъски, KPI без ИИ	Непрекъснат мониторинг, автоматичен анализ на изпълнение и рискове	Ранно откриване на отклонения, учене от опита	Непрозрачност на основанията за „оценките“ на ИИ

В разузнаването ИИ трансформира събирането на информация чрез автоматизиран OSINT/SIGINT и аномалийно засичане; прогнозирането — чрез

предикативен анализ и симулации на кибератаки; взимането на решения — чрез системи за препоръки с обясним ИИ. На етапа на реализация автономните агенти задействат автоматично защитни мерки при засичане на атака.

В контраразузнаването ИИ се прилага за анализ на вътрешни заплахи, профилиране на рискови лица и звена, биометричен контрол на достъп, автоматизирано засичане на дезинформационни кампании и динамични „рискови профили“ на персонала. Съществен акцент е поставен върху предизвикателствата: алгоритмична пристрастност при профилирането, опасност от „легитимиране“ на погрешни модели и непрозрачност на ИИ решенията при контраразузнавателен надзор.

Перспективите до 2030 г. са очертани четири стратегически направления: обясним ИИ, федеративно обучение, мултимодален генеративен ИИ и консолидирани международни регулации.

3. Облачни изчисления – мащабируемост и непрекъснатост на управлението

Облачните технологии са анализирани като инфраструктурен гръбнак на модерния управленски цикъл в сигурността. На етапа на събиране и обработка на информация облачните платформи позволяват мащабируема обработка на петабайтни масиви (Rashid и Chaturvedi, 2019), интегрирайки множество разнородни разузнавателни източници. На прогностичния етап те предоставят изчислителен ресурс за ИИ модели и симулации в реално време.

На етапите на планиране и организиране облачните решения обезпечават централизиран контрол и споделяне на информация в реално време, допълнени от блокчейн за гарантиране на прозрачност. Особено важен е раздела за контрол, одит и постоянен мониторинг, където облачните среди позволяват автоматизирани одитни следи, непрекъснат мониторинг и бърза реакция при инциденти.

4. Блокчейн – децентрализирано доверие в управленския цикъл

Авторът анализира приложението на блокчейн като инфраструктура за гарантиране на интегритет, проследимост и автоматизация на процесите в разузнаването и контраразузнаването (中国信息通信研究院, 2020). На прогностичния етап и взимане на решения неизменимите исторически регистри дават достъп до по-надеждни данни за сценарийно моделиране, а умните договори автоматично сигнализират при определени комбинации от рискови индикатори.

Критичен акцент е поставен върху етичните и правни дилеми: масовото профилиране и изграждането на динамични „рискови профили“ посредством

блокчейн изисква строга сегментация на достъпа, криптографски защити и ясни правни рамки, за да не се стигне до злоупотреби с основни права.

5. Дронове, Адитивно производство и Нанотехнологии

Дроновете са систематизирани по двете направления.

В разузнаването те обезпечават непрекъснато наблюдение, IMINT и координация на реализацията в реално време, докато в контраразузнаването се прилагат за засичане и неутрализиране на враждебни БЛА, охрана на периметри и защита на критичната инфраструктура.

Адитивните технологии трансформират управленския цикъл чрез бързо прототипиране и децентрализирано производство, като дигиталните близнаци и системите за управление на производството позволяват прогнозиране на дефекти, оптимизиране на ресурсите и автоматизиране на работни процеси. В контраразузнаването са въведени специализирани рамки за сигурност, базирани на мониторинг на странични канали за засичане на саботаж и кражба на интелектуална собственост.

Нанотехнологиите в управленския цикъл са представени от гледна точка на взимането на решения за инвестиции в защитни технологии, като криптография, сензорни мрежи, нанозащитни материали и квантово-сигурни комуникационни канали. Авторът категорично подчертава, че тези решения имат не само техническо, но и политическо и етично-правно измерение.

6. Геотехнологии – пространственото измерение на управленския цикъл

Геотехнологиите са представени чрез две детайлни матрични, картографиращи приложенията им по всеки управленски етап в разузнаването и контраразузнаването. В разузнаването те осигуряват организирането на изпълнението на решенията чрез прецизно позициониране и картографиране на оперативното пространство. В контраразузнаването геотехнологиите се прилагат за засичане на аномалии в движението, защита на границите и наблюдение на критичната инфраструктура.

7. Виртуална и добавена реалност – съвременно дигитално обучението и оперативния контекст

VR/AR технологиите са определени като фактор за измеримо подобрение в оперативната готовност от 15% до 50%. Те трансформират управленския цикъл чрез системна интеграция на виртуални технологии: VR за обучение, симулация на кризисни сценарии и предварителна оценка на решенията; AR за предоставяне на

контекстуална информация и данни в реално оперативно пространство, повишаваща ситуационната осведоменост на изпълнителите.

8. Космически технологии - надграждаща архитектура на разузнаването

Космическите технологии са концептуализирани като напълно и систематично интегрирани във всичките седем фази на управленския цикъл, от сателитно IMINT и SIGINT за събиране на информация, до прецизна навигация, сигурни комуникации и космически базиран контрол върху изпълнението. Авторът изгражда аналитичен модел, демонстриращ как тяхната всеобхватна интеграция е преобразувала управлението на сигурността от набор от отделни функции в динамичен, информационно-центриран процес, позволяващ проактивно оформяне на средата за сигурност.

Изводи на главата

Обобщеният анализ на Глава III потвърждава три основни теоретични констатации.

Първо, иновацията в предложената концептуална рамка не се крие в самия модел на управленския цикъл, а в коренната му технологична трансформация. Традиционната последователност на управленски дейности се превръща в динамична, данни-ориентирана система, при която преходът от реактивно към проактивно и предикативно управление на сигурността е не перспектива, а оперативна реалност за водещите световни служби.

Второ, предложеният модел обхваща едновременно трите управленски нива, стратегическо, тактическо и оперативно, постигайки по-тясна връзка между стратегически цели и реални оперативни действия. Технологиите като блокчейн и усъвършенстваните системи за управление на данни предоставят по-надеждна и сигурна среда за одит и оценка на управленските решения.

Трето, технологичното превъзходство и способността за системната му интеграция в целия управленски цикъл се очертават като ключов и определящ фактор за националната сигурност. Държавите и разузнавателните структури, успели да превърнат тези технологични направления в част от управленския си модел, ще разполагат с ясно информационно и оперативно предимство. Обратно – изоставането в тази интеграция се превръща в стратегическа уязвимост, излагаща на риск цялостната стабилност в сферата на сигурността.

Финалният и основополагащ извод е, че модерното управление на сигурността изисква паралелно развитие на правната, етичната и организационната

рамка, която да гарантира баланс между ефективност и защита на правата и свободите на обществото. Без такъв баланс концентрацията на критични данни и зависимостта от сложни алгоритми пораждат специфични нови уязвимости, потенциално по-опасни от тези, срещу които е насочена самата система за сигурност.

Заключение

Основна теза и обобщение на приноса

Заключението на дисертационния труд на д-р Теодора Личева „Трансформация на управленския цикъл в разузнаването и контраразузнаването чрез интеграция на съвременни технологични решения“ е синтез на изследователските постижения, който формулира стратегически насоки и очертава бъдещите предизвикателства пред сигурността в дигиталната ера.

Основната теза, която се потвърждава и в заключението, е категорична: **управлението на сигурността не може повече да се основава на аналогови, традиционни и предимно реактивни модели.** То изисква цялостна трансформация на управленския цикъл, която е основана на данни, автоматизация и предикативни технологии, както се спазва върховенството на закона, демократичния контрол и етичните стандарти. Сигурността е концептуализирана не само като институционална функция, а като интегрирана система от технологии, хора, правила и ценности, в която технологичната модернизация и управленската култура са взаимно зависими и неразривно свързани.

Ключови изводи от изследването

Заключението обобщава три взаимосвързани констатации, преминаващи като червена нишка през целия дисертационен труд.

Първо, традиционният управленски цикъл в сигурността е вече функционално несъстоятелен в условията на дигиталната ера. Реактивният, бавен и бюрократизиран управленски модел е заместван от динамична, данни-ориентирана система, при която всеки от седемте управленски етапа от събиране и анализ на информация, прогнозиране, взимане на решения, планиране, организиране до изпълнение и контрол, претърпява качествена трансформация. Изкуственият интелект, Големите данни, облачните изчисления, блокчейн, дроновете, нанотехнологиите, геотехнологиите и космическите технологии не са просто

инструменти за ефективност – те са архитектурни елементи на нов управленски модел, характеризиращ се с проактивност, предикативност и автоматизация.

На второ място, технологичното превъзходство и способността за неговата системна интеграция в целия управленски цикъл се очертава като ключов и определящ фактор за националната сигурност в XXI век. Разузнавателните структури, които успеят да превърнат технологичните иновации в органична част от своя управленски модел, придобиват измеримо информационно и оперативно предимство. И обратно – изоставането в тази интеграция се превръща в стратегическа уязвимост, излагаща на риск цялостната стабилност и надеждност в сферата на сигурността.

Трето, технологичната трансформация е устойчива само при паралелно развитие на правната, етичната и организационната рамка. Концентрацията на огромни масиви от чувствителни данни, зависимостта от сложни алгоритми и автоматизираното взимане на решения пораждат нови, специфични уязвимости, от киберзаплахи и алгоритмична пристрастност до ерозия на гражданските права и правото на неприкосновеност. Без ясен баланс между ефективност и защита на правата на обществото, самата система за сигурност може да се превърне в заплаха.

Изводи за България

Значително внимание в заключението е отделено на специфичния български контекст, като се констатира структурно изоставане, което рискува да се задълбочи. Въпреки позитивните институционални и нормативни реформи след 1989 г. и създаването на ДАНС и ДАР, приемането на специализирано законодателство и въвеждането на механизми за демократичен контрол, системата за сигурност остава изправена пред комплекс от предизвикателства.

Те включват: ограничен ресурсен и технологичен капацитет; фрагментирана информационна инфраструктура; недостатъчно интегриране на съвременни технологии на оперативно ниво; хроничен недостиг на висококвалифицирани кадри с дигитални компетентности; и забавено въвеждане на иновативни управленски модели.

Авторът подчертава, **че изоставането на България е не само технологично, но и концептуално,** защото доминира ориентацията към минимизиране на рискове и реагиране на вече настъпили заплахи, вместо към превантивна, предикативна и технологично-изпреварваща дейност.

Предложен концептуален модел

На основата на изследването дисертацията предлага концептуален модел за цифрово управление на сигурността, интегриращ трите управленски нива – стратегическо, тактическо и оперативно в единна, технологично-задвижвана система. Моделът предвижда конкретни стратегически мерки, обединени в следните направления:

- Изграждане на съвременни дигитални платформи и системи за предикативен анализ за всички фази на управленския цикъл;
- Въвеждане на дигитални близнаци на критичната инфраструктура за безрискова симулация и оценка на заплахи;
- Внедряване на архитектура „нулево доверие“ като стандарт за киберсигурност в разузнавателните и контраразузнавателните структури;
- Разработване и внедряване на постквантови криптографски решения като отговор на нарастващата заплаха от квантови изчисления.

Всичко това трябва да бъде съпроводено от единна нормативна и стратегическа рамка, по-добра координация между институциите, стандартизиране на процесите и гарантиране на баланс между националната сигурност и гражданските права и свободи.

Ролята на човешкия фактор

Особено значение в заключението се отдава и на човешкия фактор, концептуализиран като незаменима константа в процеса на технологична трансформация. Основна констатация е, че технологичните иновации могат да бъдат трайно ефективни единствено ако са съпроводени с развитие на компетентностите, организационната култура и ценностите на служителите в системата за сигурност. Ръководителите трябва да еволюират от администратори на рутинни процеси към стратегически дигитални лидери, способни да вземат информирани, данни-базирани решения в условия на постоянна несигурност и технологична турбулентност.

Дисертационният труд завършва с фундаментално стратегическо послание: ***технологичната трансформация на управлението на сигурността е не само необходимост, но и стратегическо предимство***, при условие, че е водена от ясна визия, обезпечена от адекватни ресурси, правно регулирана и ориентирана към устойчивост. Само при тези условия тя ще се превърне в трайно конкурентно предимство за националната сигурност, а не в нов и по-сложен източник на нестабилност и уязвимости.

V. Публикации по темата на дисертацията

ичева, Т. „Технологиите между индустрия 4.0 и 5.0”, В. Сб. док. IX Международна научна конференция „Industry 4.0” – 26 – 29 юни 2024 г., стр.65-67, ISSN 2535-0161

ичева, Т. „Сигурност на данните”, В. Сб. XII Международна научна конференция „Техника. Технологии. Образование. Сигурност” – 2 – 5 сеп. 2024 г., стр. 54-56, ISSN

ичева, Т. „Правила и елементи за сигурност на данните“, В сп. „Сигурност и отбрана, 2024, година III, бр. 2, стр. 188-200, ISSN 2815-388X

icheva, T.„ Artificial Intelligence and data security, В. Сб. Док. от VIII Международна научна конференция по сигурност „CONFSEC 2024” –9-12 дек. 2024 г., стр. 69-71,

ичева, Т. „Блокчейн в разузнаването”, в Сб. док. научнотеоретична конференция „Българско разузнаване и контраразузнаване – предизвикателства, проблеми, п

еТ. “Digital twins in security”, В сб. Док. от X Международна научна конференция р

ıдулов, Н, **Личева, Т.,** „Екосистема на сигурност 5.0”, В сб. Док. от X Международна N

ичева, Т. „Сигурност на е-досиета с блокчейн”, В сп. „Сигурност и отбрана, 2025, **у**одина IV, бр. 1, стр. 114-128,https://doi.org/10.70265/NKYH9976, ISSN 2815-388X– **б**тчетени за доцент

ичева, Т. ”Технологиите в управленския цикъл – съвременен и традиционен метод”, **В**. Сб. XIII Международна научна конференция „Техника. Технологии. Образование. **С**игурност” – 1 – 4 септ. 2025 г., стр. 41-43, ISSN 2535-0323

ıдулов, Н, **Личева, Т**., „Взаимодействие на блокчейн с високите технологии в **е**косистемата на Сигурност 5.0”. В. Сб. XIII Международна научна конференция „Техника. Технологии. Образование. Сигурност” – 1 – 4 септ. 2025 г., стр. 111-113, **0**

ıдулов, Н, **Личева, Т.,** „Smart contract in security”. В. Сб. XIII Международна научна **к**онференция „Техника. Технологии. Образование. Сигурност” – 1 – 4 септ. 2025 г., стр. **2**

ичева, Т. „Виртуална и добавена реалност в сигурността”. В. Сб. Док. от IX **М**Международна научна конференция по сигурност „CONFSEC 2025” 8 – 11 дек. 2025 **2**, стр. 76-78, ISSN 2603-2953

ичева, Т. „Меката роботика в сигурността.“ В сп. „Сигурност и отбрана, 2025, година I

ичева, Т. „Изкуствен интелект в управлението на контрараузнаването“. В. Сб. Док. от Международна научна конференция „Изкуствен интелект“ 23-26 март 2026

ичева, Т. „Изкуствен интелект в управлението на разузнаването“, В. Сб. Док. от Международна научна конференция „Изкуствен интелект“ 23-26 март 2026

р
0
2
8

ю
н
р