СТОПАНСКА АКАДЕМИЯ „Д. А. ЦЕНОВ“ – СВИЩОВ
КАТЕДРА „БИЗНЕС ИНФОРМАТИКА“

Владислав Владимиров Василев

УПРАВЛЕНИЕ НА ИНФОРМАЦИОННАТА СИГУРНОСТ И КОНФИДЕНЦИАЛНОСТТА В ЗДРАВНИТЕ ЗАВЕДЕНИЯ

А В Т О Р Е Ф Е Р А Т

на дисертационен труд за присъждане на образователна и научна степен “Доктор“ по научна специалност „Приложение на изчислителната техника в икономиката“

Докторска програма
„ПРИЛОЖЕНИЕ НА ИЗЧИСЛИТЕЛНАТА ТЕХНИКА В ИКОНОМИКАТА“

Научен ръководител:
доц. д-р Веселин Попов

Свищов
2021 г.

Дисертационният труд е обсъден и предложен за защита от членовете на катедра „Бизнес информатика“.

Дисертацията е в обем 175 стандартни страници и се състои от увод, три глави, заключение, декларация за оригиналност и достоверност, списък на използваните съкращения, библиография от 161 литературни източници (33 български и 128 чуждестранни) и 14 таблици и 23 фигури.

I. ОБЩА ХАРАКТЕРИСТИКА НА ДИСЕРТАЦИОННИЯ ТРУД

1. Актуалност на изследването

Сред най-значимите последствия на развитието на информационните технологии са възможностите за обмен на информация в глобален мащаб, както и генериране и достъп до информация за научни цели. В сферата на здравеопазването, благодарение на технологичния прогрес, днес се развиват теле-медицина, дигитализация на пациентските досиета, подобряване на услугите за пациентите, осигуряване на все повече възможности за натрупване и споделяне на данни за нуждите на фундаменталните и специфичните медицински изследвания. Развитието на тези дейности традиционно се съпътства от рисковете за сигурността. Базирайки се на проучвания, цитирани в дисертационния труд, можем да обобщим следните световни тенденции в информационната сигурност в здравеопазването.

- Необходимо е да се осигури и поддържа висока степен на сигурност на достъпа до информация, предоставяна на пациенти, здравни организации и различни заинтересовани страни;
- Секторът здравеопазване функционира в усложняваща се среда, подложен е на зловредни атаки, които отчасти са провокирани от различното ниво на информационната сигурност в здравните заведения;
- рисковете за информационната сигурност в здравните заведения са постоянно нарастваща величина;
- наблюдава се драстично увеличаване на заплахите към сектора на здравеопазването: около две до три пъти повече в сравнение с други сектори.

Приоритетът на информационната сигурност в здравеопазването в България се регламентира в Националната стратегия за здравеопазване 2014 г. – 2020 г., както и в проекта на Национална здравна стратегия 2021- 2030, в мярка № 4 на Приоритет 4, засягащ развитието на електронното здравеопазване.

2. Цели и задачи на изследването

Основната цел на дисертационния труд е анализ на основните заплахи и проблеми на информационна сигурност на здравните заведения в България и разработване на модел за информационна сигурност, съобразен с особеностите на лечебните заведения, предлагащи болнична помощ тип „многопрофилна болница за активно лечение" (МБАЛ). За постигане на тази цел си поставяме следните задачи:

- анализиране и очертаване на проблемите и специфичните особености на информационната сигурност в здравните заведения;
- изследване на правно-организационните, технологичните и икономическите аспекти на информационната сигурност в здравните заведения;
- анализиране на технологиите за осъществяване на защита на информационната система;
- проучване и анализ на текущото състояние на информационната сигурност на лечебни заведения за болнична и извънболнична помощ в България и перспективите за нейното подобряване;
- разработване на концептуален модел за информационна сигурност на МБАЛ, съобразен с българските условия.

3. Обект и предмет на изследването

Обект на изследването е информационната система на здравните заведения в България.

Предмет на изследването е информационната сигурност на здравните заведения в България, гарантираща тяхното безопасно функциониране и изпълнение на дейностите без прекъсване.

4. Изследователска теза

Изследователската ни теза е, че заплахите и изискванията към информационната сигурност в здравните заведения постоянно се увеличават, което изисква мерки за поддържане на високо ниво на сигурност и защита на данните и предоставяните услуги и за осигуряване на непрекъсваемост на протичащите в тях процеси. Това е от особено значение за лечебните заведения за болнична и извънболнична помощ, които събират, съхраняват и обработват лични данни и данни за здравното състояние на своите пациенти. Нивото на информационна сигурност може да бъде повишено, посредством прилагането на модел за информационна сигурност, базиран на добри практики, отговарящ на стандарти за сигурност и удовлетворяващ нормативните и регулаторните изисквания.

5. Обем и структура на дисертацията

Дисертацията е в обем 175 стандартни страници и се състои от увод, три глави, заключение, декларация за оригиналност и достоверност, списък на използваните съкращения, библиография – 161 литературни източници (33 български и 128 чуждестранни.), както и 14 таблици и 23 фигури.

6. Ограничителни условия

Дисертационния труд има следните ограничителни условия:

- Извършените анкетни проучвания са насочени към лечебни заведения за болнична и извънболнична помощ като най-разпространените видове заведения, обслужващи най-голям относителен дял пациенти; предложеният концептуален модел за информационна сигурност е насочен към МБАЛ, чиято информационна инфраструктура се характеризира като най-сложна сложна и комплексна.
- Многоаспектният характер на информационната сигурност на здравните заведения налага ограничаване на насоката на изследване отнасящо се до

„Електронно медицинско досие/Електронен здравен запис“, както са посочени в Стратегическа цел № 1 на Националната здравна информационна система. С оглед на това ограничение, проблемите свързани с използването на специализирани медицински устройства, IoT, тяхната комуникация и свързаната с тях обмяна на здравна информация не се разглеждат.

7. Методология на научното изследване

За методологическа база на изследването е използван системният подход. Направено е анкетно проучване сред специалисти от практиката и са приложени статистически методи за установяване на текущото състояние на информационната сигурност на лечебните заведения. За тестване на степента на защита на публично достъпната инфраструктура на лечебни заведения са използвани три онлайн инструмента: Threat Inteligence; Whois и Лаборатория за анализ на SSL сертификати. За дефиниране на авторския модел са приложени методите на сравнителния анализ и синтеза по отношение на моделите за информационна сигурност. Приложен е и методът за архитектурно-функционално моделиране на системи и е предложен концептуален модел за информационна сигурност.

II. СТРУКТУРА И СЪДЪРЖАНИЕ НА ДИСЕРТАЦИОННИЯ ТРУД

Дисертационния труд се състои от увод, три глави и заключение. Съдържа и списък на използваните съкращения и използваните източници.

Структурата на изложението:

Списък на използваните съкращения

Увод

Глава I. Проблеми за информационната сигурност в здравните заведения

1.1. Принципи и концепция за информационна сигурност

1.1.1. Необходимост от архитектура за информационна сигурност

1.1.2. Подходи за изграждане на архитектура за информационна сигурност

1.1.3. Контрол при защитата на информацията

1.2. Оценяване и управление на риска за информационната сигурност

1.3. Специфика на информационната сигурност в здравните заведения

1.4. Съвременни тенденции в осигуряването на информационната сигурност

Глава II. Анализ на правно-организационните, технологичните и икономическите аспекти на информационната сигурност в здравните заведения

2.1. Политики, стандарти и процедури регулиращи информационната сигурност

2.1.1. Важни стандарти за информационна сигурност на здравните заведения

2.1.2. Политики, регулиращи информационната сигурност

2.1.3. Процедури, спомагащи за повишаване на за информационната сигурност

2.2. Сравнителен анализ на технологиите осигуряващи защита на информацията

2.2.1. Класифициране на технологиите за защита

2.2.2. Оценяване на информационните ресурси

2.2.3. Организационни аспекти на информационната сигурност

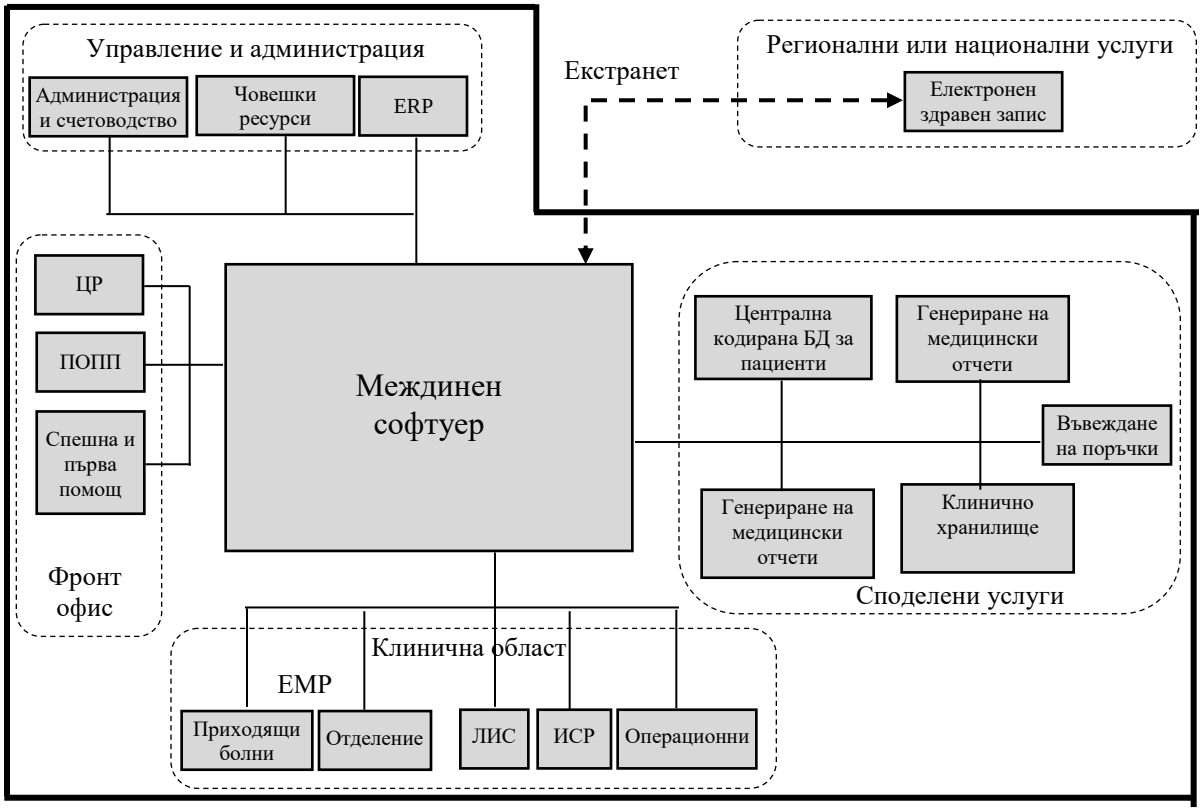
III. СИНТЕЗИРАНО ИЗЛОЖЕНИЕ НА ДИСЕРТАЦИОННИЯ ТРУД

В увода на дисертацията са изяснени актуалността на проблема, обект, предмет, цел, задачи на разработката и е представена научната теза, която следва да бъде доказана.

ГЛАВА I.
ПРОБЛЕМИ ЗА ИНФОРМАЦИОННАТА СИГУРНОСТ В ЗДРАВНИТЕ ЗАВЕДЕНИЯ

Първа глава е с теоретична насоченост. В нея са представени принципите и концепцията на информационната сигурност, изследвано е оценяването и управлението на риска за информационната сигурност, акцентирано е на спецификата на информационната сигурност в здравните заведения и са посочени съвременните тенденции в осигуряването на информационната сигурност.

В параграф**1.1. Принципи и концепция за информационна сигурност** се представя ***концептуална архитектура на ИС на болнично заведение*** (фиг. 1), предложена от Locatelli, Restifo, Gastaldi и Corso, която е изходна точка за анализиране на информационната сигурност на здравните заведения. Обосновава се необходимостта от архитектура за информационна сигурност, представят се мненията на автори, поддържащи използването на архитектурен подход за осигуряване на информационна сигурност.



Фиг.1. Концептуална архитектура на информационна система в МБАЛ

Проучени и представени са ***дефинициите за информационна сигурност***, на база на които е синтезирано авторово мнение че „*информационната сигурност е комплексен процес, който съчетава в себе си управлението на риска, оценката и използването на управленски механизми за осигуряване на информационната сигурност*“.

Проучването на успешните практически решения показва, че успешното справяне с този проблем изисква цялостна архитектура за информационна сигурност.

В следващата част на параграфа се акцентира на ***подходите за изграждане на архитектура за информационна сигурност.*** На база представени мнения на различни автори се стига до заключението, че внедряването на информационна сигурност е комплексен, отнемащ време и скъпоструващ процес, което отдалечава възможността за прилагане на унифициран подход. В тази насока се добавя мнението, че в момента не съществува единна, цялостна концепция за архитектура

на системата за информационна сигурност. Затова са анализирани множество научни публикации, които са посветени на разработването на *подходи за управление на информационната сигурност*. Разгледани са рамки, архитектури, стандарти, концепции, модели на подходи, политики и решения за осигуряване на информационна сигурност.

От представените решения, най-голямо значение имат моделите на Boehm и Wei-Ming (Табл.1) и моделът на Pulkkinen, Naumenko и Luostarinen (Табл. 2).

Таблица 1.

Сравнение на моделите на Boehm и Wei-Ming

Модел на Boehm	**Модел на Wei-Ming**	**Изводи**
Модел за използване на архитектура на информационна сигурност,който се базира на управлението на риска. Той се разделя на контролиране на риска и оценяване на риска. Контролирането на риска включва: следене на риска, осъществяване на риска, планиране и управление на риска. Оценяването на риска включва: начини за приоритизиране и управление на риска, анализирането му и неговата идентификация.	Представлява архитектурно ориентиран модел за оценяване и контролиране на риска. Авторите подчертават ролята на редуцирането на риска, неговото избягване, прехвърлянето му, приемането на риска, както и на взаимодействието на различните отдели на дадената организация, външни експерти и правораздавателни органи и правоприлагащи органи в цялостния процес.	Стигаме до извода, че управлението на риска е важна част от създаването и изграждането на архитектура за информационна сигурност. Можем да определим модела на Wei-Ming, като продължение на този на Boehm, което оказва влияние на организационната структура при създаването и внедряването на архитектура за информационна сигурност.

Според Pulkkinen и съавтори, при управлението на информационната сигурност е необходимо да се *използва широк спектър от политики и решения*. В предложеният от тях модел (Табл. 2) има обособени няколко основни нива в архитектурата за информационната сигурност, които са: стратегическо, концептуално, логическо и технологично.

Таблица 2.

Модел на Pulkkinen, Naumenko и Luostarinen

	Бизнес архитектура	**Информационна архитектура**	**Системна и/или програмна архитектура**	**Технологична архитектура**
Ниво на предприятието (стратегическо планиране)	Решения, свързани със стратегията и визията	Стратегическо управление на вземането на решения	Портфолио с приложенията, свързани със стратегическите системи	Стратегически връзки между организацията и нейните партньори
Ниво на домейн (управление на операциите, процеси и др.)	Процеси, свързани с всекидневните бизнес процеси	Информационно управление на всички прилежащи програмни продукти	Потвърждаване за оперативна съвместимост	Инфраструктурата на използваните технологии
Ниво на системата(управление на информационната система)	Изискванията, насочени към предоставяне на информация към информационната система	Насочено към складирането на типовете данни	Самата архитектура на информационната система, логика на осъществяване на операциите	Архитектура на използваната система и политики за внедряване

В края на параграф 1.1. е формулирано *заключението*, че архитектурата за информационна сигурност е основополагаща за защитата на информационната система на здравните заведения. Тя може да съдържа в себе си управленски политики и технологически мерки. Главните дейности за нейното осъществяване са: анализиране на риска за дейностите и информационните ресурси на организацията; включване на всички отдели в процеса на изграждане на архитектурата; определяне на ролите и достъпа на потребителите, които ще извършват различните дейности.

Архитектурата за информационната сигурност трябва да се разглежда като част от стратегическата управленската политика на здравното заведение. Тя може да се изгради на базата на вече приети в организацията политики и чрез прилагането на различни стандарти и добри практики, като винаги трябва да се следят, отчитат и адекватно прилагат възможностите, предоставяни от новите технологии.

Последната част на параграфа е посветена на ***контрола при защита на информацията***. Представени са авторови мнения, регулаторни рамки и стандарти, третиращи тази дейност. В края е формулирано *заключението*, че използването на организационни средства за контрол е важна дейност за осигуряване на информационната сигурност и тяхното прилагане може да се извърши чрез използването на различни правни рамки, управленски и технически решения. Като основни правни рамки, които могат да се използват при избора на организационни средства за контрол, се посочват NIST, ISO/IEC 27001.

В параграф ***1.2. Оценяване и управление на риска за информационната сигурност*** се представят основните стъпки в неговото управление. Първо се разглеждат *принципи за идентифициране на риска*. Базирайки се на представени авторови идеи и становища се стига до заключението, че правилното дефиниране на рисковете, насочени към информационните ресурси на организацията включва намирането на вече съществуваща уязвимост и в изградената информационна система и определяне на заплахите към информационните ресурси на организацията. След това се посочват различни методи за *оценяването на риска.* Представя се следващата стъпка – *определяне на действията за намаляване на риска*. В тази насока се прави обобщението, че мониторингът на риска е

определена система от наблюдения, оценки и прогнози на състоянието и развитието на информационните ресурси и/или процесите. Той включва проследяване на състоянието и развитието на тези обекти и процеси, а така също в предупреждаване за възникването на заплахи, опасности и критични ситуации. Тази система може да съдържа различни технически решения и дефинирани правила и политики.

В параграф ***1.3. Специфика на информационната сигурност в здравните заведения*** се обръща внимание на специфичните особености, които съпътстват осигуряването на информационната сигурност в здравните заведения. За целта е представена нормативната база в Закона за лечебните заведения в България, значението на навлизащите нови технологии в здравеопазването и тяхното влияние в изграждането на информационните системи и последствията, които те имат за създаване на законодателни рамки в различни държави като САЩ, Европейския съюз, Бразилия, Нова Зеландия и Япония и България.

В параграф ***1.4. Съвременни тенденции в осигуряването на информационната сигурност*** се очертават нейните основни насоки на развитие, които са: преминаването към електронно здравеопазване; развитието на политиките за информационна сигурност и по-точно на ISO27000; посочват се увеличаващите се заплахи към информационните инфраструктури на здравните заведения в САЩ и най-честите инциденти; акцентира се на възможностите за използването на изкуствен интелект за осигуряване на информационната сигурност; очертават се някои важни приоритети за осигуряване на информационната сигурност в сектора на здравеопазването и др.

Анализът на изложението в **глава I** на дисертационния труд, води до следните **изводи:**

1. Информационната сигурност постоянно се развива, обхващайки правни регулации, технически, процедурни и човешки фактори. Очертава се тенденцията развитието и усъвършенстването на технологиите да влияе върху развитието на законовите рамки. На тази база се откроява необходимостта от съчетаване и съгласуване на дефинираните законови рамки и тяхното съгласуване с развиващите се технологии.

2. Архитектурата за информационната сигурност трябва да бъде всеобхватна, да синхронизира всички организационни средства за контрол, да включва цялостно управление на риска за информационна сигурност и да следва доказали се в практиката подходи и стандарти.
3. Прилагането на организационни средства за контрол осигурява сигурността на информационните ресурси и помага за управлението на риска. Управлението на риска включва в себе неговото идентифициране и оценяване, което спомага за прилагане на правилни и навременни действия за намаляване на риска от зловредни деяния. Оценяването на риска има съществено значение. То е част от неговото управление, което подпомага изграждането и изпълняването на защитната стратегия на организацията.
4. Подобряването на качеството на предоставяните услуги в сферата на здравеопазването изисква внедряване на нови технологии, включващи нови устройства, софтуерни продукти с изкуствен интелект, безжични комуникации и високоскоростни мрежи. Те имат позитивни ефекти върху дейността на здравните заведения, но тяхното прилагане задължително изисква внедряването на допълнителни технологии за защита като криптиране, филтриране на трафика, и други подобни.
5. Като сериозно предизвикателство в тази сложна среда се очертава синхронизирането на регулаторните рамки с технологичните фактори, както и на определени дейности на медицинския и ИТ персонал.

ГЛАВА II

Анализ на правно-организационните, технологичните и икономическите аспекти на информационната сигурност в здравните заведения

Втора глава е посветена на правно-организационните, икономическите и технологичните аспекти на процесите по осигуряване на информационната сигурност. Тя съдържа три основни части, като първата обхваща анализирането и разглеждането на политики, стандарти и процедури, регулиращи информационната сигурност, втората – технологиите, осигуряващи защита на информацията, а трета обхваща SWOT анализ на използваните технологии.

Параграф **2.1. Политики, стандарти и процедури, регулиращи информационната сигурност започва** с представяне на ***важните стандарти за информационна сигурност.*** Описани са отделните стандарти и са представени процесите по стандартизация, базирайки се на Българския институт по стандартизация, които организациите могат да използват в процеса на преход към осигуряване на информационната сигурност на своите информационни ресурси. Това включва и процеса по стандартизация, който организациите трябва да преминат. Като отправна точка е използван ISO 27001:2013. Представени са и други действащи стандарти в областта на информационната сигурност, като серията ISO/IEC 27000 – Системи за управление на сигурността на информацията. Акцентира се на Наредбата за минималните изисквания за мрежова и информационна сигурност, която има съществено значение за регулиране на информационната сигурност в България, както и на мненията на няколко различни автори, работещи в тази област.

Следва представяне на ***политиките, регулиращи информационната сигурност.*** Базирайки се на представените мнения на автора са формулирани следните изводи:

- Политиката за информационна сигурност включва решения, взети от ръководството на организацията и насочени към защита на информационните ресурси, в зависимост от използваните информационни и комуникационни технологии и свързаните с тяхното използване рискове;
- Цялостната политика за осъществяване на мрежова и информационна сигурност в организацията може да представлява набор от нормативни документи, правила и политики, които определят как организацията защитава обработката, съхранението и разпространението на информацията;
- Политиките за информационни сигурност трябва да осигуряват защитата на специфичната медицинска информация;
- Политиките може да се базират на вече утвърдени и приети стандарти.

В края на параграфа е обърнато внимание на ***процедурите, спомагащи за повишаване на информационната сигурност***. Въз основа на стандартите ISO/IEC 27001:2013 и цитирани публикации, третиращи тази материя, е направено заключението, че процедурите за осигуряване на информационната сигурност

включват в себе си действия и правила, които подпомагат всекидневните операции на организацията. Процедурите могат да включват различни способи за прилагането в действие на вече приетите политики за информационна сигурност.

Параграф **2.2. Сравнителен анализ на технологиите, осигуряващи защита на информацията** започва с ***класифициране на технологиите за защита.*** За целта са представени мнения и становища на автори относно нуждата от класификация и становища за нейното съдържание. В резултат на представеното е формулиран изводът, че правилното идентифициране на информацията помага за селектирането на нужната технологията за осъществяване на защита. Предложена е следната класификация на технологиите за защита, които са технологии за:

- осигуряване на мрежовата сигурност;
- осигуряване на сигурността на приложенията и устройствата, които работят с достъп до мрежата;
- управление на уязвимостите им;
- управление на достъпа и предоставянето му на оторизирани потребители;
- контролиране на потока от информация;
- използване на криптиране.

Следва ***оценяване на информационните ресурси***, обяснява се понятието „информационен ресурс“, съгласно действащото законодателство и се представят мнения на автори и се представят подходи за идентифициране на: ресурсите, заплахите и уязвимостите на информационните ресурси.

Параграфът продължава с представянето на ***организационните аспекти на информационната сигурност***. Посочва се, че организационните аспекти, в това число и персоналът, се определят като най-рисковото звено по отношение на сигурността на информацията. В заключението се посочва, че хората, които оперират с информацията трябва да познават рисковете, които произлизат от това. Ясното и точното дефиниране на задълженията и изясняване на приетите политики

за информационната сигурност е друг важен фактор, осигуряващ тяхното спазване и прилагане.

Относно ***осигуряването на физическата сигурност и сигурността на средата*** е посочено, че това е задължително условие за осигуряване на комплексната информационна сигурност. За тяхното осъществяване е препоръчително да се спазват представените: Наредба за минималните изисквания за мрежова и информационна сигурност, ISO, NIST и планиране на непрекъснатостта на бизнеса.

По отношение на ***обезпечаването на сигурността на комуникациите*** е направено заключението, че осигуряването на защитата на комуникациите представлява начинание, което включва синхронизиране на различни технически мерки и изпълнението им от персонала. Техническите мерки могат да бъдат разнообразни, но е важно да следват предварително създадена процедура, за тяхната дейност и внедряване. Подчертава се, че част от посочените методи за осигуряване на комуникациите са използвани в концептуалния модел на МБАЛ, представен в трета глава.

Следва описание на ***действията при управление на инцидентите***, за което са използвани няколко правни рамки, мнения на автори и препоръките на ISO 27001. На тази база се стига до заключението, че управлението на инцидентите изисква синхронизация между различни технически мерки и спазването на вече приетите процедури и политики.

В края на тази част са представени и ***други технологии, използвани за защита на информационните системи***, които не са описани по-горе, които организацията може да приложи за осигуряване на защитата на своята информационна система. Тези технологии включват филтриране на трафика, забрана за използване на устройства, за които потребителят не е оторизиран, криптография и управление на достъпа.

В параграф **2.3. SWOT анализ на използваните технологии** е посочено, че всяка една от прилаганите технологии за защита на информацията има своите предимства и недостатъци, като основно те зависят от естеството и дейността на организациите. Информационните технологии, осигуряващи защита на

информацията, разгледани комплексно, като съвкупност, използвана заедно, имат силни и слаби страни, предоставят възможности, но също така крият и опасности от възникване на рискове.

В резултат от направеното сравнение се вижда, че силните страни от използването на технологиите за защита са значително повече от слабите страни, и те предоставят значителни възможности на фона на потенциални опасности. Липсата на технологии за защита може да доведе до големи финансови загуби за организацията.

В края на **втора глава** са направени следните **изводи:**

1. Стандартите, политиките и процедурите са изключително важни фактори за осигуряването на информационната сигурност. Стандартите можем да определим като гръбнака, върху който се гради основата за осъществяване на дейностите по защита. Политиките включват в себе си мениджърски решения на различните управленски нива за защита на разнообразни информационни ресурси. Те обхващат регулирането на правната рамка, а стандартите събират в себе си добри практики, технически спецификации и критерии за информационна сигурност. Процедурите обхващат способите за защита, прилагани във всекидневните дейности на организацията и включват в себе си различни организационни средства за контрол, които регулират процеса, осигуряващ информационната сигурност. И трите фактора имат обща цел и допирни точки, свързани с осигуряването на информационната сигурност и различните начини за нейната реализация.

2. Технологиите за защита, можем да определим като динамични и да ги класифицираме като технологии за осигуряване на: мрежовата сигурност; сигурността на приложенията и устройствата, които работят с достъп до мрежата и управляване на уязвимостите им; управлението на достъпа; контролирането на информационния поток и криптиране.

3. Трябва да отбележим, че развитието на информационните технологии води до промени в различни законодателни и нормативни рамки. Внедряването на технологиите за защита, от една страна предоставя предимства и нови възможности, а от друга води до възникване на рискове при тяхното приложение.

ГЛАВА III.
Анализ на състоянието на информационната сигурност в здравните заведения

В по-голямата си част трета глава има практически характер. В нея са представени резултатите от проведени анкетни проучвания и онлайн проучване на сигурността на публично достъпната инфраструктура на лечебни заведения. Разгледано е и състоянието на законодателната и нормативната база, регламентираща информационната сигурност в сектора на здравеопазването в България и света. Предлага се авторов концептуален модел за информационна сигурност на МБАЛ. Главата се състои от три параграфа.

В параграф **3.1. Изследване на състоянието на информационната сигурност в здравеопазването** се ***изследва състоянието на законодателната и нормативната база, регламентираща информационната сигурност в сектора на здравеопазването в България и света.*** Представени са законодателните инициативи, целящи регламентиране на информационната сигурност. В резултат на извършено проучване на нормативните актове и документите, като най-важни и универсални регулатори, помагащи за осигуряване на информационната сигурност на световно, регионално и локално ниво, са посочени следните:

- Общ регламент за защита на личните данни (Регламент (ЕС) 2016/679);
- Закон за здравните информационни технологии за икономическо и клинично здраве от 2009 г.;
- Бразилският общ регламент относно защита на личните данни LGPD;
- Поправка за поверителност, задължаваща за изискване на информация при успешен пробив;
- Японският регламент за защита на личните;
- Южнокорейският закон за защита на персоналната информация.

Представят се и специализирани нормативни документи, засягащи различни аспекти на информационната сигурност в областта на здравеопазването:

- ISO 27799:2008 (ISO, 2008), ревизиран през 2016: ISO 27799:2016;
- ISO 17090:2008 (ISO, 2008), ревизиран през 2021 г. на ISO 17090-3:2021;
- NIST SP 1800-1.

Посочват се нормативните документи, които регламентират информационната сигурност в България:

- Закон за защита на личните данни;
- Правилник на вътрешни правила за правата и задълженията на потребителите;
- Наредбата за минимални изисквания за мрежова и информационна сигурност;
- БДС ISO/IEC 17799:2006 - Кодекс на добри практики за управление на сигурността на информацията.

Параграфът продължава с ***преглед на състоянието на информационната сигурност в глобален мащаб,*** извършен на база проучвания от консултантската компания EY през 2018 г. и Обществото на американски здравни организации (HIMSS) през 2018 и 2020 г., в които се изследват: посоките, в които организациите трябва да насочат своите усилия; трудностите и предизвикателствата, с които трябва да се справят организациите, предоставящи медицински услуги; констатациите, свързани с най-значимите инциденти в областта на сигурността. В заключението се посочва, че рисковете за информационната сигурност на дигиталното здравеопазване се увеличават постоянно, факт, който изисква постоянно търсене на начини за справяне с тях. Използването на нови технологии за сигурност е начинание, което ще изисква допълнителни изследвания за сферите и начините за прилагане.

В края на тази част се представя ***състоянието на информационната сигурност в здравеопазването в България.*** В този параграф се отбелязва, че на фона на предизвикателствата и нарастващите заплахи пред информационната сигурност в здравните заведения, научните публикации и изследвания в тази насока в България са малко на брой. На базата на тези изследвания се определят настъпили промени, както и предположения за развитие на информационната сигурност по отношение на прехода към електронно здравеопазване. Използвани са: анкетно проучването, насочено към актуалното състояние на електронните системи в лечебните заведения, проведено през 2012 г. от Шишманов и съавтори; публикация на CIO България; публикация на Деливерски от 2016 г.; публикация на Каракънева от 2018 г.

Направени са следните изводи:

- Българските лечебни заведения са в процес на доизграждане на техническата база, необходима за техните информационни системи;
- Изискването за по-високо ниво на информационната сигурност се налага като важен аспект за осигуряването на качествено електронно здравеопазване в България;
- Представените научни изследвания, разгледани в хронологичен аспект, показват, че електронното здравеопазване в България се развива с добри темпове.

В параграф **3.2. Проучване на текущото състояние на информационната сигурност на лечебните заведения в България** е анализирано ***състоянието на информационната сигурност в лечебни заведения*** в България на база проучване, направено през 2019 г. в рамките на научноизследователски проект „Изследване на състояние на информационната сигурност в лечебните заведения в България“ със значително участие на автора на дисертационния труд. Изследването включва *анкетиране чрез електронна форма на анкета* и провеждане на интервюта на място с ИТ специалисти. Изследването обхваща две групи респонденти, за които са създадени две различни анкетни карти и онлайн проучването, извършено с помощта на инструментите **ThreatInteligence**, **Whois**, **Лаборатория за анализ на SSL сертификати.**

Групите на респондентите са както следва:

1. ***Първа група респонденти***– медицински персонал в качеството му на основен потребител на ИС на лечебните заведения.
2. ***Втора група респонденти*** – специалисти от ИТ отдела в качеството им на персонал, осигуряващ и поддържащ сигурността и защитата (заедно с всички други аспекти) на ИС на лечебните заведения.

Резултати от анкетното проучване, за първата група от респонденти са както следва: В общия профил, те работят в следните -УМБАЛ - 41,66 %; СБАЛ - 29,16 %; БПЛ - 20,83%; МБАЛ - 8,33%. В основната си част - 72,91% от респондентите са от средно големи организационни структури с персонал повече от 250 души. Останалите са както следва: по-малко от 10 души – 2,16%, от 10 до 49

души 2,08%, от 50 до 250 души 20,83%. Като за съществена част от ежедневната си работа респондентите използват компютърна техника като 60,94% от тях прекарват повече от 2 часа в работа с нея, 20,83% - до 1 час на ден, а 18,75% - до 2 часа.

Много голяма част от респондентите (84,41%) се сблъскват с проблеми при работата със софтуерните продукти и/или компютърната техника. Почти две трети от респондентите (59%) имат технически проблеми, т.е. с повреда на компютърната конфигурация; половината (51%) имат проблеми с използваните софтуерни продукти; повече от една трета (37%) са имали проблеми с инцидент, свързан с инфраструктурата за осъществяване на достъп до Интернет. Интересно е, че само 2% от респондентите отчитат проблеми със зловреден софтуер.

Въпросите в анкетната карта за медицинския персонал са свързани с аспекти на информационната сигурност, като до колко са запознати с *Регламента за защита на личните данни на Европейския съюз (GDPR),* 14,58% от респондентите заявяват, че са подробно запознати с него; 72,91% са запознати само частично; а 12,5% от тях не познават този регламент.

На въпроса за наличието на разработени собствени правила за защита на информацията за здравето на пациентите, повече от две трети (68,75%) от респондентите отговарят положително.

Всички респонденти смятат, че са необходими действия за повишаване на сигурността на информацията в лечебните заведения в България. На фиг. 2 е представено мнението на респондентите по отношение на сферите, в които трябва да бъдат полагани усилия, за да се повиши сигурността на информацията. Според повече от половината (61%) от тях е необходимо подобряване на сигурността на специализираните софтуерни продукти, т.е. усъвършенстване на защитата на ниво приложения; за 57% - подобряване на сигурността при работа с Интернет, т.е. усъвършенстване на мрежовата защита; 39% смятат, че е нужно използване на нови компютърни системи; а за 31% - увеличаване на броя на системните администратори, поддържащи ИС и инфраструктура, т.е. усъвършенстване на защитата на ниво инфраструктура. Нито един от респондентите не смята, че са

необходими повече нормативни регулатори.

Фиг.2. Насоки за повишаване на сигурността на информацията в лечебните заведения в България

Резултатите от втората група респонденти имат следния профил МБАЛ - 40%; УМБАЛ - 30%; СБАЛ - 10% - БПЛ - 10%, - МДЛ - 10%. Най-голямата част – 40% от респондентите са средно големи организационни структури с персонал повече от 250 души. Останалите са както следва: с по-малко от 10 души – 0%, от 10 до 49 души 30%, от 50 до 250 души 30%. Въпросите са в следните направления: нарушенията в сигурността;поддържаното ниво на сигурността, оценяване на информационната сигурност като мениджърски проблем и познаване на Регламента за защита на личните данни на Европейския съюз (GDPR); прилагани политики и процедури за сигурност.

За Нарушения в сигурността: половината (50%) от респондентите в изследването декларират, че през последната година инциденти, свързани с информационната сигурност, са се случвали рядко; на 20% такива инциденти са се случвали често, а на почти една трета (30%) такива инциденти е имало рядко. Видовете инцидентите в информационната сигурност на лечебните заведения, които са декларирали такива (70% от всички респонденти). Всички респонденти (100%) декларират наличието на атаки от външни лица. Съществена част от тях (86%) декларират инциденти поради физически проблеми, свързани с хардуера.

Също толкова заявяват за проблеми с инциденти от зловреден софтуер. Една трета от респондентите посочват, че са имали и други инциденти, свързани с персонала.

Поддържаното ниво на сигурността: 70% от поддръжката на ИС на изследваните лечебни заведения се осъществява от ИТ отдел, 20% от един администратор, а 10% е аутсорсвана към външен изпълнител. Всички респонденти (100%) отбелязват, че в техните системи достъпът на външните потребители се контролира, като се имплементират различни потребителски роли. Подобен е и отговорът (100% от респондентите) относно съществуването на обратна връзка с администратора и/ или ИТ отдела. При определяне на правилата за регламентиране на ролите за достъп респондентите заявяват, че 60% имат такива или че се водят от предварително определени правила. При останалите 40% от респондентите правата за достъп се предоставят по преценка на системния администратор.

Оценяване на информационната сигурност като мениджърски проблем и познаване на Регламента за защита на личните данни на Европейския съюз (GDPR) - само половината от респондентите (50%) приемат информационната сигурност като задача с висок приоритет, докато за 40% от респондентите информационната сигурност е задача със среден приоритет. Най-тревожното е, че за 10% тази задача все още е с нисък приоритет. На въпроса относно познаването на Регламента за защита на личните данни на Европейския съюз, 80% от респондентите отговарят, че са подробно запознати, докато останалите (20 %), че само отчасти са запознати с него.

Прилагани политики и процедури за сигурност - всички респонденти (100%) използват защитната функционалност на специализиран софтуер и хардуер, както и оторизиране на използването на мрежови услуги. Почти всички респонденти (90%) имат и провеждат политика за управление на чувствителни данни. Много голяма част от респондентите (80%) прилагат процедури за отдалечен достъп до локалите мрежи на лечебните заведения; използване на корпоративен e-mail, интранет и Интернет; управление на паролите. Малко повече от половината (60%) респонденти осигуряват отговор и управление на инцидентите, свързани със сигурността, а по-малко от половината (40%) декларират наличие на политика и използване на стандарти за криптиране.

За проучване на степента на защита на публично достъпната инфраструктура на лечебните заведения – порталите предоставящи услуги на пациенти (фронт-енд на системите) са използвани три онлайн инструмента за тестване: ThreatInteligence; Whois; Лаборатория за анализ на SSL сертификати сме избрали 20 болнични заведения на случаен принцип. В табл. 3 са представени крайните резултати от това изследване. За оценка е използвана скала от 1 до 5 със следните значения: от 1 до 2 - слаба степен на защита; от 3 до 4 - средна степен на защита, 5 - висока степен на защита. По отношение на Whois протокол е отбелязано наличието или липсата на такъв. Опцията „Да“ означава, че порталът е истински и принадлежи на лечебното заведение.

Таблица 3.

Резултати от онлайн тестовете

Лечебно заведение	Threat Inteli-gence оценка	Whois про-токол	Лаб.за анализ (SSL)	Издател на сертификата	Вид на сертификата – алгоритъм
Обект 1	4	Да	5	Let's Encrypt Authority X3	SHA256withRSA
Обект 2	4	Да	4	cPanel, Inc. Certification Authority	SHA256withRSA
Обект 3	5	ДА	5	Let's Encrypt Authority X3	SHA256withRSA
Обект 4	4	Да	4	RapidSSL RSA CA 2018	SHA256withRSA
Обект 5	4	Да	4	cPanel, Inc. Certification Authority	SHA256withRSA
Обект 6	4	Да	4	cPanel, Inc. Certification Authority	SHA256withRSA
Обект 7	4	Да	5	cPanel, Inc. Certification Authority	SHA256withRSA
Обект 8	4	Да	5	Let's Encrypt Authority X3	SHA256withRSA
Обект 9	5	Да	1	Няма наличен сертификат	Няма сертификат
Обект 10	4	Да	5	Let's Encrypt Authority X3	SHA256withRSA
Обект 11	5	Да	5	RapidSSL RSA CA 2018	SHA256withRSA
Обект 12	5	Да	4	cPanel, Inc. Certification Authority	SHA256withRSA
Обект 13	4	Да	5	Let's Encrypt Authority X3	SHA256withRSA
Обект 14	5	Да	5	Let's Encrypt Authority X3	SHA256withRSA
Обект 15	5	Да	1	Няма наличен сертификат	Няма сертификат
Обект 16	4	Да	4	cPanel, Inc. Certification Authority	SHA256withRSA
Обект 17	5	Да	5	Let's Encrypt Authority X3	SHA256withRSA
Обект 18	4	Да	5	Let's Encrypt Authority X3	SHA256withRSA
Обект 19	5	Да	1	Няма наличен сертификат	Няма сертификат
Обект 20	5	Да	5	Let's Encrypt Authority X3	SHA256withRSA

Следват ***изводите за състоянието на информационната сигурност,*** които са:

1. Основните проблеми, с които се сблъсква медицинския персонал в качеството му на основен потребител на ИС на лечебните заведения имат вътрешно естество и са свързани с използването на софтуерни продукти и/или компютърната техника. За проблеми със зловреден софтуер съобщават едва 2% от респондентите. Проблем се вижда във факта, че основната част от този персонал познава само частично регламента за защита на личните данни на Европейския съюз (GDPR).

2. Според специалистите в ИТ отделите на българските лечебни заведения в качеството им на персонал, осигуряващ и поддържащ сигурността и защитата (заедно с всички други аспекти) на ИС на лечебните заведения, през последната година проблеми със сигурността на ИС са имали всички лечебни заведения, като при една пета от тях тези проблеми са се случвали много често. Основните инциденти са свързани с атаки от външни лица, инциденти от зловреден софтуер и хардуерни проблеми.

3. Типът на поддръжка на информационната сигурност в лечебните заведения в България зависи от големината на лечебното заведение и основно се осъществява от собствен специализиран ИТ отдел. Информационната сигурност към момента се постига основно чрез техники като: контрол на достъпа на външните потребители; обратна връзка; система за докладване на грешки в ИС; система за регистриране на нарушенията; отдалечен достъп на служители и пациенти и др.

4. За висшия мениджмънт осигуряването и поддържането на информационна сигурност все още не е задача с висок приоритет. За такава към момента я приемат малко повече от една трета от мениджърите на лечебни заведения. Все пак положителен е фактът, че основната част от лечебните заведения имат бюджет, който е специално определен за осигуряване и поддържане на информационна сигурност. В преобладаващия случай тези разходи не са задоволителни, т.е. са между 2% и 5 % от общия бюджет за ИТ.

5. На текущия етап около една пета от ИТ специалистите не познават в подробности Регламента за защита на личните данни на Европейския съюз (GDPR). Позитивен е фактът, че в много голяма част от лечебните заведения все пак са

дефинирани и се спазват собствени правила за работа с здравната информация на пациентите.

6. Политиките и процедури за сигурност, които основно се прилагат в българските лечебни заведения са: използване защитната функционалност на специализирания софтуер и хардуер; оторизиране на използването на мрежови услуги; процедури за отдалечен достъп до локалите мрежи на лечебните заведения; използване на корпоративен e-mail, интранет и Интернет; управление на паролите и др.

7. Прилаганите към момента техники за противодействие на атаките лечебните заведения в България са: централизирано хранилище за данни; контрол на достъпа до дневниците за сигурността; наблюдение на сигурността и на нарушенията по отношение на наличните приложения и мрежови услуги и др.

8. Тестовете на степента на защита на публично достъпната инфраструктура на лечебните заведения (порталите предоставящи услуги на пациенти) с онлайн инструменти показват, че са налице слабости и потенциални точки на пробив в системите.

9. Използването на външен хостинг от 85% от лечебните заветния крие рискове за ефективния контрол върху медицинската информацията за здравното състояние на техните пациенти.

В параграф **3.3. Концептуален модел за информационна сигурност на МБАЛ** се представят ***модели за инвестиции в информационната сигурност.*** Обяснява се, че за подпомагане на вземането на решение за инвестиране в информационна сигурност може да се използват специално дефинирани модели за оценка на необходимите инвестиции. Те представят различни подходи за оптимално инвестиране в информационна сигурност. За тяхното използване се дефинират критерии за избор на модел за инвестиция от гледна точка на бизнес организацията (табл. 4).

Таблица 4.

Сравнение на моделите за инвестиции за осигуряване на информационна сигурност

Критерии	**Модел на Гордон-Лоеб**	**Модел на Соненрич**	**Модел на Креморини и Мартини**	**Модел на Боджанк, Блазис и Текавкик**
Финансова рамка	Представя се оптимална инвестиция от 37 % от нетните приходи.	Представя се финансова рамка, която се базира на ценността на информацията и не може да се определи с точност.	Представя се рамка базирана на годишен финансов план, предвиждайки потенциални загуби променяща се на база на атаките.	Представя се финансова рамка, която се базира на ценността на информацията и уязвимостта на системата.
Начин за инвестиция	Фиксиран начин за инвестиция, с точни и ясно дефинирани параметри.	Фиксиран начин за инвестиция, който се определя още в началния стадий за изграждане на информационна сигурност.	Фиксиран начин за инвестиция, базирайки се на годишните очаквания от загуби и възвръщаемостта на инвестициите след успешна атака.	Фиксиран, предлагащ възможност за продължителна инвестиция, базирайки се на анализите за риска на информационните ресурси.
Ползи	Ползите се изразяват в защита на ресурсите с по-голям риск за причиняване на вреда и изграждане на защита за тях с фиксиран размер на инвестиция.	Моделът предлага ползи акцентирайки вниманието към смекчаването на загубите и отбелязване на връзката между продуктивността и сигурността на бизнес организацията.	Моделът предлага анализ на атаките, които постоянно застрашават сигурността на информацията.	Ползите произлизат от дефинирането и оценяването на риска и предложените политики за информационна сигурност, базирани на добри практики.
Негативи	Не се обръща	Не се вземат под	Постоянното	Възможността за

	внимание при малка вероятност за пробив, от което се възползват атакуващите.	внимание постоянно еволюиращите заплахи. При такава възможност и смекчаването на загубите може да не е ефективно.	излагане на риск от пробив, може да бъде нерентабилно и потенциално опасно.	претърпяване на промени при определянето на финансовите параметри, базирайки се на анализирането и оценяването на риска.

В параграфа ***Подход за информационната сигурност, базиран на модел*** се акцентира върху необходимостта от подход за информационна сигурност, базиран на модел, и се очертават ключовите компоненти на информационната сигурност, обосновани от изследователския колектив, осъществил посочения по-горе научен проект.

В параграфа ***Концептуален модел за информационна сигурност на МБАЛ*** е предложен от автора на дисертационния труд на концепция за модел за сигурност на ИС на лечебно заведение, тип МБАЛ. МБАЛ е избрано като най-разпространен тип лечебно заведение и такова с най-много пациенти (в сравнение с останалите). Поради ограничения обем на настоящото изследване, в концептуалния модел се отделя внимание само на софтуерните и хардуерните системи, информационните потоци и администрирането на потребителите като най-важни и специфични компоненти и ресурси на ИС на МБАЛ. За обезпечаване на сигурността на ИС на МБАЛ е предложен **концептуален логически модел** на организация на информационната инфраструктура и осъществяване на защитени комуникации. **Първата стъпка** в концептуалния модел е да се **очертае обхвата на информационната инфраструктура**: вътрешни и външни ресурси. Логическата структура трябва да се базира на стандартите за сигурност. Те предполагат изграждане на мрежа и свързаните с това политики за регулиране на достъпа. **Логическата архитектура** на модела за информационна сигурност на МБАЛ може да бъде дефинирана на три нива: външно; средно; вътрешно.

Външното ниво включва главния маршрутизатор, който управлява трафика от и към компонентите, разположени на другите нива. *Средното ниво* включва

хардуерно устройство, което ще управлява защитната стена. Защитна стена към настоящия момент може да се реализира с хардуерно устройство, софтуерно или чрез съвместно използване на двете устройства. Функциите, които изпълняват тези устройства е контролиране на получаваните по мрежата информационни пакети за съответствие на предварително дефинираните правила. Изисква се ограничаване на достъпа до публични (външни) адреси с изключение на най-необходимите приложения. Това се отнася за външни адреси, които не са от важно значение за изпълнението на задълженията на служителите на МБАЛ.

По-горе са посочени главните компоненти на информационната инфраструктура, като има опции за включване на допълнителни приложения (когато те са необходими) и тяхната настройка. Препоръчва се всички вътрешни отделения и структурни звена, включени в състава на *вътрешното ниво,* да използват вътрешни мрежи с частни адреси. Към основните функции на външното ниво се отнасят осъществяването на комуникация с други организации като: болници; лаборатории; медицински университети; НЗОК; НОИ; НАП. В тези случаи връзката най-често се осъществява чрез използване на:

- електронен портал за достъп;
- контролиране на достъпа чрез потребителски роли;
- използването на стандарти за шифриране.

Друг важен елемент от инфраструктурата за информационна сигурност е **електронният подпис**, използван за потвърждаване на самоличността, като това включва **потребителски роли** и определяне на **правата за достъп** на регистрираните потребители. След успешно преминаване и авторизация от защитната стена, може да бъде осъществен достъп до ресурси като онлайн портала на лечебното заведение. Те са разположени в слоя на средното ниво, в състава на което влиза защитната стена като преграда, защитаваща вътрешната част на мрежата. *Централизираното хранилище за данни* е основен компонент на вътрешното ниво. То може да бъде съставено от различни физически база данни, които могат да са хетерогенни и да се различават по типа, структурата, модел на данните и модел на складиране на данните. Базите данни складират различната информация, като едновременно предоставят и достъп до нея на потребителите и на софтуерните продукти, които ще ги използват. Те са базирани на конфигуриран

сървър за бази данни. Препоръчително е всички бази от данни да са централизирани, разположени на сървъра в централизираното хранилище за данни. При осигуряване на защитата на личните данни трябва да отчетем и изискванията на GDPR. Към *вътрешното логическо ниво* на защита може да се добави *ниво за физическа защита на достъпа*. Това ще осигури ограничаване на достъпа до помещенията на централното хранилище за данни и на специализираните компютърни конфигурации, свързани със специфична медицинска апаратура само на хора с права за това.

Предложеният концептуален модел има за цел да осигури оптимално ниво на защита на информацията в лечебните заведения, като се базира на:

- добри практики;
- следване препоръките насочени към техническото изпълнение, предоставени от GDPR;
- спазване принципа на нива на защита, като се стреми да намали щетите от евентуален пробив;
- отвореност към модификации и разширение на мрежата осигуряваща достъпа;
- ненарушаване на достъпа до ресурсите на мрежата в случай на разширение и/или на повреда;
- осигуряване на свързаност между вътрешните мрежи за продължаване на работата дори и при загуба на връзката с Интернет.

Заключението систематизира проблемите, решенията, които се предлагат в дисертационния труд, и приносите му за науката и практиката.

Най-важните от тях са:

Заплахите, а съответно и изискванията към информационната сигурност на здравните заведения в България постоянно се увеличават. Това обстоятелство изисква мерки за поддържане на високо ниво на сигурност и защита на данните и предоставяните услуги и за осигуряване на непрекъсваемост на протичащите процеси в здравните заведения.

Осигуряването и поддържането на информационната сигурност в здравните заведения е комплексен процес, който трябва да се базира на законови и нормативни регулации, да включва разработване на стратегии и политики на различните мениджърски нива, на своевременното оценяване и внедряване на иновации и др.

Технологичните решения имат ключово значение за осигуряване на съответно ниво на информационната сигурност. Те включват широк набор от технологии, които могат да бъдат класифицирани в следните групи: за осигуряване на мрежовата сигурност; за осигуряване на сигурността на приложенията и устройствата, които работят с достъп до мрежата и управляване на уязвимостите им. Техните силни и слаби страни, опасности и нови възможности трябва да бъдат основа за критична оценка при тяхното внедряването в информационните системи.

Текущото състояние на информационната сигурност на здравните заведения в България показва, че те имат проблеми със сигурността на ИС, като при една пета от тях тези проблеми са се случвали много често. Основните инциденти са свързани с атаки от външни лица, инциденти от зловреден софтуер и хардуерни проблеми. Политиките и процедури за сигурност, които основно се прилагат в българските лечебни заведения са: използване защитната функционалност на специализирания софтуер и хардуер; оторизиране на използването на мрежови услуги; процедури за отдалечен достъп до локалите мрежи на лечебните заведения; използване на корпоративен e-mail, интранет и Интернет; управление на паролите и др.

На базата на извършеното теоретичното проучване на литературните източници и проведените емпирични изследвания е предложен концептуален модел, който има за цел постигането на оптимално ниво на защита на информацията в лечебно заведение от тип МБАЛ. Концептуалният модел се базира на добрите практики и следва препоръките, насочени към техническото изпълнение, дефинирани в регламентите и стандарти, използвани за защита на информацията и личните данни, също така отчита принципа на нивата на защита. Концептуалният модел се характеризира с това, че е: отворен към модификации и разширение на мрежата, осигуряваща достъпа; гарантира защита на достъпа до ресурсите на мрежата в случай на разширение и/или на повреда; осигурява

вътрешна свързаност за продължаване на работата, дори и при загуба на достъп до Интернет.

IV. СПРАВКА ЗА ОСНОВНИТЕ ПРИНОСИ В ДИСЕРТАЦИОННИЯ ТРУД

Теоретичната и практическа значимост на труда и неговите **основни приноси** се изразяват в следното:

- анализирани и очертани са проблемите и особеностите на информационната сигурност в здравните заведения;
- изследвани са правно-организационните, технологичните и икономическите аспекти на информационната сигурност в здравните заведения;
- анализирани са технологиите за осъществяване на защита на информационната система;
- извършено е проучване и е анализирано текущото състояние на информационната сигурност на МБАЛ в България и са очертани перспективите за нейното подобряване;
- разработен е концептуален модел за информационна сигурност на МБАЛ, съобразен с българските условия.

V. СПИСЪК НА ПУБЛИКАЦИИТЕ, СВЪРЗАНИ С ДИСЕРТАЦИОННИЯ ТРУД

СТУДИИ:

1. Попов, В. Емилова, П., Таиров, И. Василев, В. (2020). Информационната сигурност на лечебните заведения в България. Алманах научни изследвания. СА Д. А. Ценов - Свищов, стр. 211-242.

СТАТИИ:

2. Василев, В. Добри практики и модели за информационната сигурност в бизнес организациите // Годишен алманах. Научни изследвания на докторанти на СА Д. А. Ценов - Свищов, бр. 10 , 2017, с. 446-458.

ДОКЛАДИ:

1. Василев, В. Заплахи за информационната сигурност и нива на защита., Юбилейна научна конференция Предизвикателства пред информационните технологии в контекста на „Хоризонт 2020“, 2016. Свищов. с.343-348.
2. Tairov, I., Vasilev, V. Perspectives on mobile devices adoption in healthcare sector. International Conference Information and communication technologies in business and education, Varna, 2019, p. 257-262.
3. Vasilev, V. Good practices and models for information security in business organizations. Securitatea informationala 2018, Academia de studii economice a Moldovei, p. 141-145.