РАЗДЕЛ III

ФИНАНСОВА СТАБИЛНОСТ, ИКОНОМИЧЕСКИ ПОЛИТИКИ, РЕГУЛАЦИИ И УСТОЙЧИВО РАЗВИТИЕ

ИНФОРМАЦИОННАТА СИГУРНОСТ НА ЛЕЧЕБНИТЕ ЗАВЕДЕНИЯ В БЪЛГАРИЯ[1]

Доц. д-р Веселин Попов
Доц. д-р Петя Емилова
Ас. д-р Искрен Таиров
Докторант Владислав Василев

Резюме

Актуалността на настоящото изследване се определя от нарастване на изискванията и на заплахите за информационната сигурност на лечебните заведения. Целта е изследване на особеностите, състоянието и проблемите на информационна сигурност на лечебните заведения в България. Задачи: проучване и анализиране на състоянието на информационната сигурност на лечебните заведения в България и перспективите за подобряване; очертаване на добри практики; анализ на възможностите на някои нови технологии; дефиниране на концепция за модел за информационна сигурност, подходящ за МБАЛ. Изследователската теза, е че изискванията и заплахите към информационната сигурност нарастват постоянно. Това налага осъществяване на превантивни мерки и високо ниво на сигурност и защита на данни и услуги, както и непрекъснатост на бизнеса и се отнася с особено значение за лечебните заведения, които събират, съхраняват и обработват лични данни и данни за здравното състояние от своите пациенти. Нивото на информационна сигурност може да бъде повишено, посредством прилагането на модел за информационна сигурност.

В студията е направен анализ на състоянието на информационната сигурност на лечебните заведения в България и е дефинирана концепция за модел за информационна сигурност, който се базира на: добри практики; следва препоръките, насочени към техническото изпълнение, изисквани от GDPR; отчита принципа на нивата на защита.

Ключови думи: информационна сигурност, лечебни заведения, модел за сигурност

JEL: D80

[1] Участие на авторите е както следва: доц. д-р Веселин Попов – резюме, т. 2.1, т. 4.1 съвместно с доц. д-р Петя Емилова; доц. д-р Петя Емилова – въведение, т. 2.2, т. 4.1 съвместно с доц. д-р Веселин Попов, заключение; ас. д-р Искрен Таиров – т. 4.2 и т. 4.3; докт. Владислав Василев – т. 1, т. 3.

INFORMATION SECURITY OF HOSPITALS IN BULGARIA

Assoc. Prof. Veselin Popov, PhD
Assoc. Prof. Petya Emilova, PhD
Assist.Prof. Iskren Tairov, PhD
PhD Student Vladislav Vasilev

Abstract

The relevance of this study is determined by the increasing requirements of and threats to the information security of healthcare facilities. The aim of the study is to investigate the state of information security of hospitals in Bulgaria and to define the concept of the model for information security. The following tasks are solved: studying the state of information security of hospitals in Bulgaria and opportunities for improvements; highlighting the good practices; analysing the capability of new technologies. On this basis, a concept for an information security model is developed, taking into account the features of Bulgarian hospitals. The research thesis, which is defended, is that threats and information security requirements have been steadily increasing. This requires precautionary measures and a high level of security and protection of data and services, as well as business continuity and is particular important to hospitals that collect, store and process personal data and health data of their patients. The information security level can be increased by applying an information security model. The studies have analysed the state of information security of medical establishments in Bulgaria and defined a concept for an information security model based on: good practices; following the recommendations for technical implementation required by the GDPR; accounting for the principle of protection levels.

Keywords: information security, hospitals, security model.

JEL: D80.

Въведение

Сигурността на информационните системи (ИС-и) е сред основните обекти на научни изследвания през последното десетилетие. Редица фактори определят **актуалността** на настоящото изследване. На първо място – нарастващите и разнородни заплахи, пред които са изправени ИС-и и поддържащия ги персонал. На второ място е въвеждането на нови технологии и концепции, като Big data, интернет на нещата (IoT), BYOD, облачни услуги, и др., които, освен че предоставят ефективни решения, също увеличават заплахите. Не на последно място са проблемите, свързани с прилагането на политиките, регламентите и процедурите за сигурност.

Целта на студията е да се изследват особеностите, състоянието и проблемите на информационна сигурност на лечебните заведения в Бълга-

рия, като се решават следните *задачи*: проучване и анализиране на състоянието на информационната сигурност на лечебните заведения в България и перспективите за подобряване; очертаване на добрите практики, анализ на възможностите на някои нови технологии. *Изследователската ни теза* е, че заплахите и изискванията към информационната сигурност постоянно се увеличават. Това налага превантивни мерки за поддържане на високо ниво на сигурност и защита на данни и предоставяни услуги, както и непрекъснатост на бизнеса (в случая функционирането на лечебните заведения). Това се отнася с особено значение за лечебните заведения, които събират, съхраняват и обработват лични данни и данни за здравното състояние от 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 нормативни и регулаторни изисквания.

Обект на изследване са ИС на лечебните заведения в България, а *предмет* – информационната сигурност на лечебните заведения в България.

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 лечебните заведения са използвани три онлайн инструмента: ThreatInteligence; Whois; 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.

1. Проучване на текущото състояние на информационната сигурност на лечебните заведения в България

За проучването на текущото състояние на информационната сигурност на лечебните заведения в България са използвани: *анкетно проучване* на състоянието на информационна сигурност на лечебните заведения в България и *онлайн проучване* на публично достъпната инфраструктура на лечебните заведения.

1.1. Анкетно проучване

1.1.1. Методика на анкетното проучване

Проучването на състоянието и възможностите за подобряване на информационна сигурност на лечебните заведения в България и идентифицирането на добрите практики за информационната сигурност се базира на

Политиката за развитие на електронното здравеопазване, част от Националната здравна стратегия (2014 – 2020 г.) и конкретно към краткосрочните мерки, които обхващат: утвърждаване на информационни стандарти; системи за сигурност на информацията; публичен регистър на здравните данни и термини; модел на здравно-информационна система; електронно здравно досие; здравен идентификатор; интегрирани болнични ИС-и. Изследването включва *анкетиране чрез електронна форма на анкета* и провеждане на интервюта на място с ИТ специалисти. Изследването обхвана две групи респонденти, за които бяха подготвени две различни анкетни карти.

- ***Първа група респонденти*** *(анкетна карта 1)* – медицинският персонал в качеството му на основен потребител на ИС на лечебните заведения, включваща въпроси за личните данни на пациентите, и всекидневните им задължения, свързани с информационната инфраструктура на организацията. Въпросите в тази анкетна карта са 10 и са обособени в три секции – базова информация, информация за работата на служителите, стратегия и правила за информационна сигурност.
- ***Втора група респонденти*** *(анкетна карта 2)* – специалистите от ИТ отдела в качеството им на персонал, осигуряващ и поддържащ сигурността и защитата (заедно с всички други аспекти) на ИС на лечебните заведения. Въпросите са 26 и са организирани в следните секции: базова информация; поддръжка и достъп до информационната система (ИС); нарушения в сигурността; стратегия и процедури за информационна сигурност; инвестиране в информационната сигурност; наличие на централизирано хранилище за данни; контрол за зловреден софтуер и защитна стена.

1.1.2. Резултати от анкетното проучване

Според Закона за лечебните заведения респондентите попадат в следните две категории:

- *За болнична помощ*, свързана с диагностика и лечение на заболявания, когато лечебната цел не може да се постигне в условията на извънболнична помощ, родилна помощ, рехабилитация, вземане, съхраняване, снабдяване с кръв и кръвни доставки, учебна и научна дейност (чл.11, ал 1, от Закон за лечебните заведения) – МБАЛ (многопрофилна болница за активно лечение); СБАЛ (специализирана болница за активно лечение); УМБАЛ (университетска болница за активно лечение); БПЛ (болница за продължително лечение).
- *За извънболнична помощ*, свързана с извършващи лечение, рехабилитация, лабораторни и други видове изследвания (чл. 11, ал. 1, от Закон за лечебните заведения) – МДЛ (Медико-диагностична лаборатория).

Тук е нужно да отбележим особения статут, според GDPR регламента, на болничните заведения в режима им на събиране и обработване на персоналните данни на пациента.

Първа група респонденти

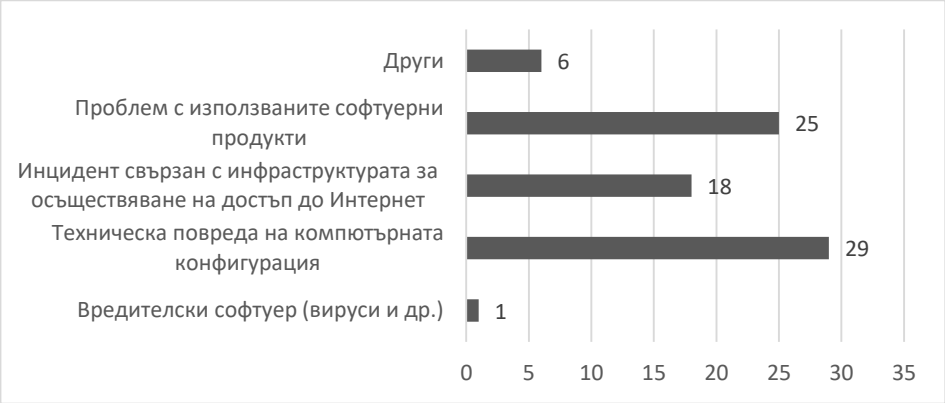
От изпратените 350 покани за попълване на електронната анкетна карта към първата група респонденти – *медицинският персонал на лечебните заведения* – се получиха 49 коректно попълнени анкетни карти. В резултат се очерта следният профил на първата група респонденти: УМБАЛ – 41,66 %; СБАЛ – 29,16 %; БПЛ – 20,83%; МБАЛ – 8,33%. В основната си част – 72,91% от респондентите са 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%.

Изследването показва, че съвременните ИТ се превръщат в основно средство в работата на медицинския персонал. 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.

Основната част (почти половината) от дейностите, в които медицинските служители използват компютърна техника, е работа с конкретен медицински софтуер – 48,97%. Също така съществена част от тези дейности са: обработка на документи – 28,57% и обработка на данни – 22,44%. За тези дейности повече от две трети от респондентите (79,16%) се нуждаят от интернет връзка.

Много голяма част от респондентите – 84,41% се сблъскват с проблеми при работата със софтуерните продукти и/или компютърната техника. Естеството на тези проблеми е различно (вж. фиг. 1). 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. Така на практика съществената част от проблемите възникват от вътрешни фактори.

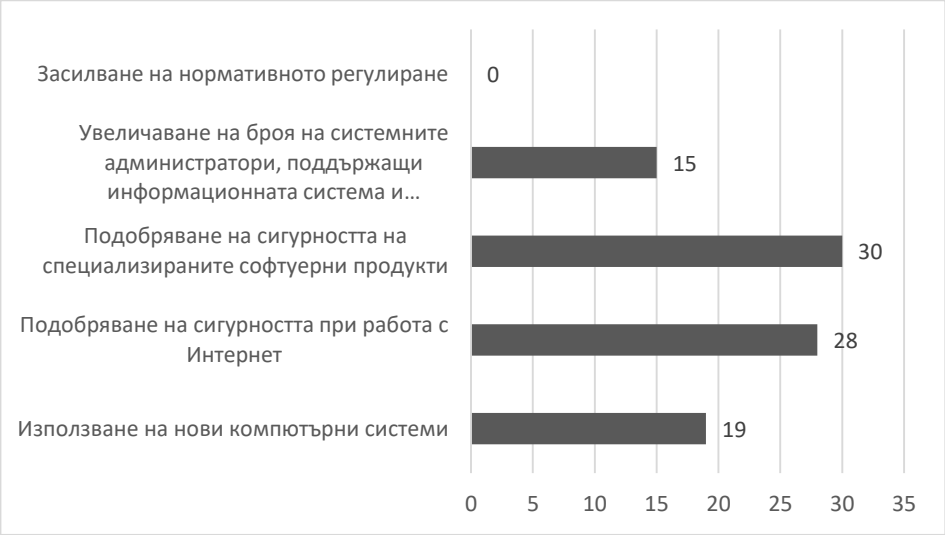
Въпросите в последната секция на анкетната карта за медицинския персонал са свързани с аспекти на информационната сигурност. На въпроса доколко са запознати с *Регламента за защита на личните данни на Европейския съюз (GDPR),* 14,58% от респондентите заявяват, че са подробно запознати с него; 72,91% са запознати само частично; а 12,5% от тях не познават този регламент. Това състояние е тревожно, като се отчита фактът, че медицинският персонал работи с много чувствителни данни, а от 25 май 2018 г. спазването на регламента е задължително. Можем да предположим, че запознаването и внедряването на регламента се изпълнява в движение, т.е. възникнали проблеми ще се решават в процеса на работа.



Фигура 1. Проблеми на медицинския персонал със софтуера и компютърната техника

Друг въпрос, касаещ информационната сигурност на лечебните заведения, в които работят респондентите, се отнася до наличието на разработени собствени правила за зашита на информацията за здравето на пациентите. Повече от две трети (68,75%) от респондентите отговарят положително на този въпрос, което означава, че съществен, макар и недостатъчен дял от лечебните заведения, са дефинирали и спазват свой собствен правилник за боравене с информация за здравното състояние. Това ни дава основание да предположим, че е налице сериозно отношение към проблематиката и синхронизирането с европейския регламент ще бъде реализирано. Трябва да отчетем и възможността, част от респондентите да са медицинските служители, които нямат съществен достъп до чувствителните данни или до използваните ИС-и.

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. За 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 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.



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

Втора група респонденти

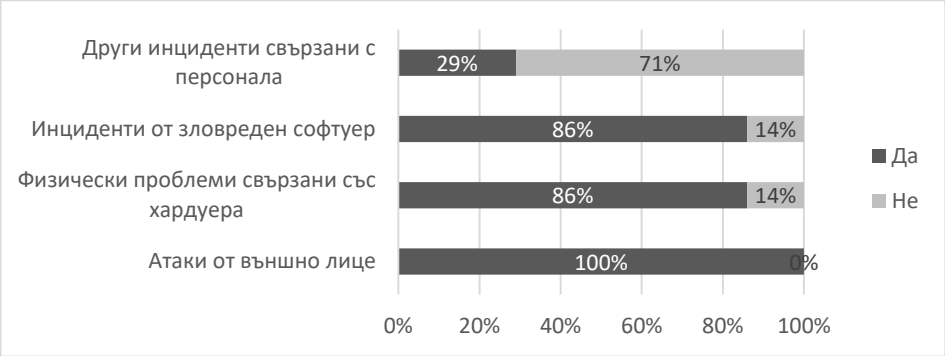
От изпратените 100 покани за попълване на електронната анкетна карта към втората група респонденти – *специалистите в ИТ отделите* на лечебните заведения – се получиха 10 коректно попълнени анкетни карти. Сравнително ниският процент респонденти може да се обясни с чувствителността на проучваната област: информационна сигурност на информация за здравното състояние на пациенти.

В резултат се очерта следният профил на втората група респонденти: 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%.

Изследвано е състоянието на ИС на респондентите 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.

Нарушения в сигурността и възможностите за противодействие

Половината (50%) от респондентите в изследването декларират, че през последната година инциденти, свързани с информационната сигурност, са се случвали рядко, за 20% такива инциденти са се случвали често, а за почти една трета (30%) такива инциденти е имало рядко.



Фигура 3. Видове инциденти с информационната сигурност

Видовете инцидентите в информационната сигурност на лечебните заведения, които са декларирали такива (70% от всички респонденти), са показани на фиг. 3. Всички респонденти (100%) декларира наличието на атаки от външни лица. Съществена част респонденти (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. Определено атаките от външни лица, зловредният софтуер, както и инциденти поради физически проблеми, свързани с хардуера, се очертават като основен проблем за информационната сигурност на лечебните заведения в България.

Впечатление прави разминаването в позициите на двете групи респонденти (медицински персонал и ИТ специалисти) по въпроса за инцидентите със зловреден софтуер. Въпреки че съпоставянето е условно, разликите са съществени. Само 2% от медицинския персонал декларира проблеми със зловреден софтуер срещу 86%, деклариран от ИТ персонала. За това вероятно има основателна причина, свързана с гледната точка. Медицинският персонал няма нужните познания, за да разпознае осъществяваща се атака от външни лица, а от друга страна, тези атаки се прихващат на ниво защитна стена.

Поддръжка на информационната сигурност в изследваните лечебни заведения

Резултатите от анкетата показват, че 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. Това състояние е очаквано, като се има предвид, че почти половината респонденти работят в организации с над 250 души персонал.

Фигура 4. Характеристики на ИС на изследваните лечебни заведения

Фигура 4 представя състоянието на ИС на респондентите по отношение на определени, важни за защитата характеристики на системата. 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 написани правила. При останалите 40% от респондентите правата за достъп се предоставят по преценка на системния администратор.

По отношение на един от основните инструменти за намиране, отстраняване на потенциални проблеми – системата за докладване на грешки в ИС, 90% от респондентите са заявили, че поддържат възможности за докладване на грешки. Това може да спомогне за намаляването на щетите от вече съществуващ проблем като например успешен пробив, компрометиране и др.

Почти две трети (70%) от респондентите заявяват, че ИС в техните болнични заведения осигуряват отдалечен достъп на служители и пациенти. Възможност за осъществяване на достъпа е използване на виртуална частна мрежа (VPN). Това е компютърна мрежа, логически изградена чрез криптиране, използвайки инфраструктура на по-голяма мрежа, като в повечето случаи се използва Интернет. От тези отговори може да стигне до заключението, че се осигурява сериозно ниво контрол на достъп до ИС. И не само до достъпа, но и осъществяване на обратна връзка с ИТ отдел или поне на наличния администратор. Също така трябва да отбележим, че дори и наличието на сериозно ниво на защита на достъпа до ИС винаги съществуват рискове с предоставянето на външен достъп.

По отношение наличието на система за регистриране на нарушения, почти две трети (70%) от респондентите заявяват, че имат такава. Това е изключително важен елемент, който осигурява цялостността на данните и може да послужи за намаляване на щетите от евентуален успешен пробив.

Оценяване на информационната сигурност като мениджърски проблем и познаване на регламента за защита на личните данни на Европейския съюз (GDPR)

В изследваните лечебни заведения информационната сигурност все още не е приета от всички като основен мениджърски проблем и задача. Само половината от респондентите (50%) приемат информационната сигурност като задача с висок приоритет. Състояние, което според нас е следствие от два факта: естеството на работа и по-точно осигуряването на защита на личните данни на пациентите; и влизането в сила на регламент за GDPR, задължаващ всички държави–членки на Европейския съюз да следват неговите директиви.

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. Фактът, че към текущия момент около една пета от ИТ специалистите не познават в подробности GDPR, е притеснителен, тъй като те са основният двигател за неговото реализиране и спазване.

Много голяма част от анкетираните (90%) заявяват, че в техните лечебни заведения са разработени вътрешни правила за прилагане на регламента, в което откриваме известно противоречие с отговорите на предходния въпрос или поне притеснение относно качеството на тези правила. Относно наличието и спазването на собствени правила за работа със здравната информация на пациентите 90% от респондентите заявяват, че имат дефинирани такива. Като цяло може да се направи заключението, че създаването и следването на правила за защита са относително добре застъпени в лечебните заведения.

Политиките и процедурите за сигурност

На фиг. 5 е представена степента на прилагане на популярни 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 е-

mail, интранет и Интернет; управление на паролите. Малко повече от половината (60%) респонденти осигуряват отговор и управление на инцидентите, свързани със сигурността, по-малко от половината (40%) декларират наличие на политика и използване на стандарти за криптиране.

Фигура 5. Прилагани политики и процедури за сигурност

Инвестиране в информационната сигурност

На въпроса за наличието на бюджет, който е специално определен за осигуряване и поддържане на информационна сигурност, голяма част от респондентите (80%) декларират, че имат такъв. По отношение на относителния дял на тези разходи спрямо общия бюджет за ИТ, една трета (25%) от респондентите (с бюджет за сигурност) заявяват, че изразходват между 6% и 10 %., при останалите (75%) тези разходи са между 2% и 5 %.

Възможностите за противодействие

Фигура 6 представя степента на прилагане на определени техники за противодействие на атаките. Всички респонденти (100%) използват централизирано хранилище за данни и контрол на достъпа до дневниците за сигурността. Почти всички (90%) осъществяват наблюдение на сигурността и на нарушенията по отношение на наличните приложения и мрежови услуги. Много голяма част от респондентите (80%): използват инструменти за отчитане и анализиране на дневниците на защитната стена; извършват сканиране на услугите, предоставяни от сървъра на защитната стена; сканиране на e-mail съобщенията за вируси; контролират инсталирането на софтуер на потребителските компютри; записват в дневници на всички опити за достъп.

Фигура 6. Прилагани техники за противодействие на атаките

1.2. Проучване на публично достъпната инфраструктура на лечебните заведения

1.2.1. Методика

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.

Целта и последователността на прилагане на инструментите е, както следва:

- Първо използваме **ThreatInteligence** – платформа, за комплексен анализ на:
  - *Главната инфраструктура*: главния домейн, прилежащи под домейни, имейл сървър, уебсървър и др.;
  - *SSL сертификат и прилежащите му настройки*: валидност; валидации на името; поддържани протоколи; проверка за актуални уязвимости.
  - *Проверка за зловредни софтуерни продукти*;
  - *Проверка на репутацията на домейна*.

- Второ използваме **Whois протокола** за получаване на цялостна информация за домейна.
- **Лаборатория за анализ на SSL сертификати** за получаване на пълната информация за приложения и конфигуриран сертификат:
  - *използвана версия;*
  - *използван шифър;*
  - *използвани ключове за успешно „ръкостискане“.*

1.2.2. Резултати

В Таблица 1 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 1

Резултати от онлайн тестовете

Лечебно заведение	Threat Intelligence оценка	Whois протокол	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

Данните показват, че според оценката на ThreatInteligence, публично достъпната инфраструктура на 45% от изследваните лечебни заведения се характеризира с висока степен на защита. Останалите 55% са със средна степен на защита.

Оценката на Whois протокола констатира, че порталите за онлайн услуги на всички изследвани лечебни заведения са действителни и принадлежат на съответните лечебни заведения.

Според тестванията с инструмента на Лаборатория за анализ на SSL сертификати, *55%* от порталите за онлайн услуги на изследваните лечебни заведения са с *висока степен на защита*, 30% са със средна степен на защита, а 15% са със слаба степен на защита.

Извършеното проучване на публично достъпната инфраструктура на лечебните заведения констатира един сериозен проблем. Това е фактът, че дори и с потвърждението на Whois протокол, около 85% използват външен хостинг, т.е. нямат собствена уеббазирана сървърна инфраструктура. Това поражда съмнения относно ефективния контрол върху медицинската информация на пациентите, когато тя се предава през уеб.

1.3. Изводи от извършеното проучване на състоянието на информационната сигурност

1. Основните проблеми, с които се сблъсква медицинският персонал в качеството му на основен потребител на ИС на лечебните заведения, са от 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). Това негативно към момента състояние се компенсира до известна степен с наличието на собствени правила за защита на информацията за здравето на пациентите в голяма част от българските лечебни заведения. Като необходими действия за повишаване сигурността на информацията в лечебните заведения в България медиците виждат основно в усъвършенстване на софтуерната защитата и на мрежовата защита.

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, те 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 със здравната информация на пациентите.

6. Политиките и процедурите 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 на 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. 55 % от системите на изследваните лечебни заведения имат препратки към други сайтове, скриптове за отваряне на допълнителни техни вътрешни страници, отворени портове (като за SQL сървър) и опция за браузване на файловата система. Потенциален риск за сигурността е и обстоятелството, че някои от конфигурираните сертификати са оставени с наличието на TLS 1.0 и TLS 1.1 сертификати, които също могат да бъдат риск за сигурността (въпреки че ще бъдат свалени от употреба през 2020 г.).

9. Използването на външен хостинг от 85% от лечените заведения крие рискове за ефективния контрол върху медицинската информация за здравното състояние на техните пациенти.

2. Подход за информационната сигурност, базиран на модел

2.1. Необходимост от модел

Един от подходите за защита на ИС е прилагане на модел, който гарантира сигурност и надеждност. Според Lee (Lee, 1999), „*Информационният модел* е представяне на концепции, взаимоотношения, правила и операции за уточняване на семантиката на данните за избрана област“. Според автора прилагането на модел гарантира подходяща структура на информационните изисквания в контекста на избраната област. Заради предимствата, които осигурява моделът за информационна сигурност, този подход е ефективно решение и се препоръчва от изследователи и експерти по информационна сигурност.

Според Fernandez и Mujica (Fernandez & Mujica, 2011) най-добрият начин за осигуряване на единна концепция за сигурност е чрез използване на абстракция на модели, обезпечаващи както сигурност, така и надеждност. Използвайки шаблони, авторите описват архитектурата на взаимоотношенията в различните типове мрежи. На практика, моделите са капсулирани решения, с които могат да се решават повтарящи се системни проблеми. Те дефинират речник, който накратко описва изискванията и решенията. Предимствата от използването на шаблони за описание на архитектурата са в няколко аспекта: по-лесно разбиране; осигуряват насоки за проектиране и анализ; по-висока степен на сигурност на структура при увеличаване на атаките, като едновременно се увеличава общата им надеждност.

За прилагане на този подход Fernandez и Mujica разработват методология, базирана на принципите за сигурност, които се прилагат на всяка фаза от жизнения цикъл на софтуерния продукт. Освен това всяка фаза се тества за съответствие с тези принципите. Методологията съдържа пет фази на развитие: фаза за анализ на областта; фаза на изискванията; фаза на анализ; фаза на проектиране; фаза на развитие.

В своите разработки Димитров (Димитров, 2018, стр. 15-16) поставя знак за равенство между термините модел за сигурност на информационни и комуникационни технологии (ИКТ) и система за сигурност на системата от ИКТ. Според автора моделите за сигурност на ИКТ могат да се изградят на различни основи: стратегия за сигурност; цел на бизнеса и др. Димитров предлага модел за киберсигурност, „базиран на управление на промяната в аспекта и разширяването на ИТ вселената с нови технологични парадигми, които непрекъснато увеличават и променят повърхността за заплахи“. В тази постановка авторът отчита навлизането на новите технологии като C2 (Command and Control), BYOD и IoT, които съществено променят информационната инфраструктура и организацията на софтуера. Второто изисква преход от „дефинирани параметри, статични правила и монолитни стекове

към динамична софтуерна инфраструктура, основана на виртуализация и контейнеризация“.

В изследване на Ahlfeldt и др. (Åhlfeldt, Spagnoletti, & Sindre, 2007) е възприета идеята за ИС, съставена от технически формални и неформални (ТФН) части, които взаимодействат помежду си и чрез които се осигурява цялостен подход към гарантиране на сигурността на ИС. *Техническото ниво* на сигурност има за цел запазване на конфиденциалността, целостта и отчетността, изисквайки прилагане на защитни решения като криптиране на данни и комуникации, контролиране на достъпа, сигурно кодиране на програмния код, механизми за автентификация и оторизация, сигурност на бази от данни, системи за откриване на проникванията, защитни стени и др. На това ниво може да се опишат методи за избор на технологични решения, подходящи за различните софтуерни приложения. *Формалното ниво* включва комплект от политики, контроли и стандарти за осигуряване на интерфейса между технологичните подсистеми (техническото ниво) и поведенческата подсистема. В най-голяма степен мениджмънтът на ИС е насочен към това ниво. Началните стъпки за постигане на сигурност в това ниво са подготовката на контролни списъци и анализ и оценка на риска. *Неформалното ниво на сигурност* разглежда поведенчески въпроси като морални ценности, отношения, убеждения и норми, които имат важно значение за участието на индивидуалния служител в практиките за сигурност на бизнес организацията.

Експерти от ISACA[2] предлагат бизнес модел за информационна сигурност (The Business Model for Information Security, n.d.), който да подпомогне мениджърите по информационна сигурност да вземат точните решения. Експертите от ISACA смятат, че международно приетите стандарти и рамки традиционно разглеждат предприятието като система, акцентирайки на аспекти като култура и възникване, докато бизнес моделът за информационна сигурност е цялостен подход за нейното управление. Според тях бизнес моделът за информационна сигурност следва да включва четири елемента (организационна схема и стратегия; хора; процеси; технологии) и шест взаимовръзки (култура; архитектура; управление; възникване; предоставяне и поддръжка; човешкия фактор), които се интерпретират в три измерения и се представят като пирамида.

Моделът на ISACA има следните предимства за бизнес организацията (The Business Model for Information Security, n.d.):

- увеличаване на репутацията и марката;
- повишаване на осведомеността за културата за сигурност;
- осигуряване на ефективна комуникация за риска за информационната сигурност в бизнес организацията;
- осигуряване на ROI;

[2] ISACA е независима нестопанска световна асоциация, ангажирана с разработването, приемането и използването на общоприети, водещи знания и практики за информационни системи.

- намаляване на преекспонирането на информационната сигурност.

Обобщавайки представените по-горе становища, може да направим заключението, че подходът за постигане на информационна сигурност, базиран на модел, осигурява нейното цялостно и комплексно управление. Моделът за информационна сигурност трябва да очертава всички насоки, политиката и стратегията, хардуерните и софтуерните системи, обучението и културата на персонала. Този подход е приложен по-долу за дефиниране на концептуален модел за информационна сигурност в МБАЛ.

2.2. Ключови компоненти на информационната сигурност

По отношение на ключовите компоненти на рамката за информационна сигурност в бизнес организацията има различни становища. Преобладаващата част от авторите се базират на посочените изисквания в CIA триадата, добавяйки към тях още изисквания. Други изследователи акцентират на моделиране на заплахите, на базата на които се идентифицират изискванията към информационната сигурност.

Базовите изисквания за информационна сигурност са формулирани от Whitman и Mattord (Whitman & Mattord, 2013, p. 4) и в тях се включват широки области от управление на информационната сигурност, сигурност на компютрите и данните и мрежова сигурност. Според авторите в основата на информационната сигурност е концепцията за политика, която да осигурява осведоменост, обучение, образование и технологии, които са жизнено важни за предпазване на ИС от заплахи.

Триадата CIA (Confidentiality, Integrity, Availability) формулира основните стандарти за защита на информацията: защита на конфиденциалността, цялостността и наличността. Моделът за сигурност CNSS представя една по-детайлна перспектива на сигурността, добавяйки допълнителни характеристики на информацията и разглеждайки информационната сигурност в три измерения: съхраняване, обработка и предаване; наличност, цялостност и достъпност; политика, обучение и технологии. Слабите страни на CNSS модела са две: в него не са включени подробни насоки и политики за прилагане на контроли; резултатите са незадоволителни, когато моделът се използва ограничено само от една перспектива. Пълният списък с понятия, осигуряващи информационната сигурност, предложен от Whitman и Mattord (Whitman & Mattord, 2013, pp. 5-8), е: конфиденциалност (confidentiality), цялостност (integrity), наличност (availability), поверителност (privacy), идентификация (identification), автентификация (authentication), авторизация (authorization), отчетност на субекта (accountability).

Предложение за рамка за информационна сигурност прави Parker (Bosworth, Kabay, & Whyne, 2014), според когото класическата триада CIA не е достатъчна да опише какво се включва в информационната сигурност и е нужна нова рамка, която да бъде пълна, точна и последователна. Тази

нова рамка има за цел да посочи всички аспекти на сигурността на основно ниво, като представя в друга форма моделите на заплахи, активи и уязвимости, включвайки подробни дескриптори за всяка тема от модела.

Предложеният от Parker модел включва шест основни части:

1. Елементи за сигурност, запазващи информацията: наличност; полезност; цялостност; автентификация; конфиденциалност; притежание.

2. Източници, водещи до загуба на елементите за сигурност на информацията: хора, злоупотребяващи с информация; случайни събития; естествени природни бедствия.

3. Действия, причиняващи загуба: унищожаване; вмешателства при използването; използване на неверни данни; модифициране или замяна; грешно представяне или отхвърляне; неправилна употреба или провал при използване; местоположение; разкриване; наблюдение; копиране; вземане; излагане на опасност.

4. Функции за защита на информацията от представените по-горе действия: проверка; отхвърляне; възпиране; откриване; превенция; предотвратяване; смекчаване; прехвърляне; разследване; санкции и награди; възстановяване.

5. Методи за избор на предпазни мерки: прилежно използване; спазване на наредбите и стандартите; отговаряне на специални нужди.

6. Цели, които трябва да се постигнат чрез информационната сигурност: избягване на небрежност; отговаряне на изискванията на законите и разпоредбите; сигурно извършване на е-търговия; етично поведение; защита на поверителността; минимализиране на въздействието на сигурността върху производителността; дисциплинирано отношение и защитаване на обществото.

Други автори обосновават тезата, че преди формулиране на изисквания към информационната сигурност трябва да се извърши моделиране на заплахите. Според Myagmar и др. (Myagmar, Lee, & Yurcik, 2005) идентифицирането на заплахите помага за разработване на реални и смислени изисквания за сигурност, което намалява възможността на атакуващите да злоупотребяват със системата. За тази цел те предлагат процес за моделиране на заплахите, състоящ се от три стъпки: характеризиране на системата; идентифициране на активите и точките за достъп; и идентифициране на заплахите.

Използването на методи за моделиране на заплахите се предлага от автори като Shevchenko (Shevchenko, et al., 2018). Чрез методите за моделиране на заплахите се създава абстракция на системата, профили на потенциални нападатели (включително техните цели и методи) и съставяне на списък с потенциални заплахи. Изследователите предлагат 12 метода, които могат да се използват за моделиране на заплахите: STRIDE, PASTA, LINDUN, CVSS, дърво на атаките, Persona non Grata, карти за сигурност, hTMM, количествен TMM, Trike, VAST моделиране, OCTAVE. Според посочените автори няма метод, който да бъде препоръчан като универсално

решение, затова изборът трябва да се основава на целите на проекта и неговата специфика.

Предложените от CIA триадата стандарти очертават само базовите изисквания за информационна сигурност. В течение на времето те са допълнени от други модели и рамки, предложени от автори, работещи в тази област. Извършването на моделирането на заплахите, на база на което да се формулират изискванията за информационна сигурност, дава възможности на системните архитекти да постигнат специфичните цели и да отговорят на изисквания на текущия проект.

3. Концепция за модел за информационна сигурност на МБАЛ

В този параграф се предлага 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). Независимо от това, при отчитане на специфичните особености, предлаганата концепция е приложима и за други видове лечебни заведения. Поради ограничения обем на настоящата студия в концепцията за 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 предлагаме концепция за **абстрактен логически модел** на организация на информационната инфраструктура и осъществяване на защитени комуникации. Като концептуална основа на нашия модел е предложението на Hunt и др. (United States of America Patent No. US 6,907,395 B1, 2005), както и съвременни технологични решения за сигурност на ИС на лечебните заведения.

Първата стъпка в концепцията за модела е да се **очертае обхватът на информационната инфраструктура**: вътрешни и външни ресурси. Логическата структура трябва да се базира на стандартите за сигурност (Teare, 1999) за изграждане на мрежа и свързаните с това политики за регулиране на достъпа:

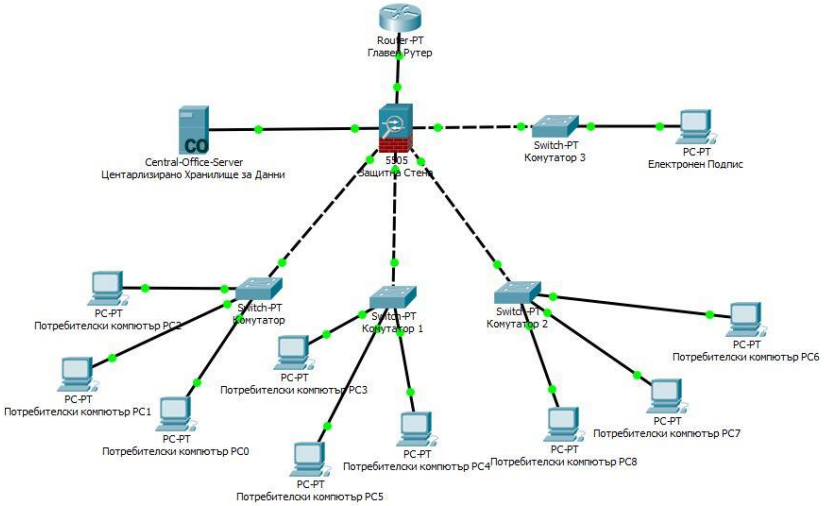
В предложения модел за информационна сигурност акцентираме на:

- Използване на хардуерни защитни стени;
- Сегментиране на наличните мрежи;
- Използването на централизирано хранилище за данни;
- Формулиране на специфични за организацията списъци на потребителите за контрол на достъпа;
- Дефиниране и използване на потребителски роли.

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, са контролиране на получаваните по мрежата информационни пакети за съответствие на предварително дефинираните правила. На практика те регулират режима на пропускане. 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.



Фигура 7. Логическа архитектура на модел за информационна сигурност в МБАЛ[3]

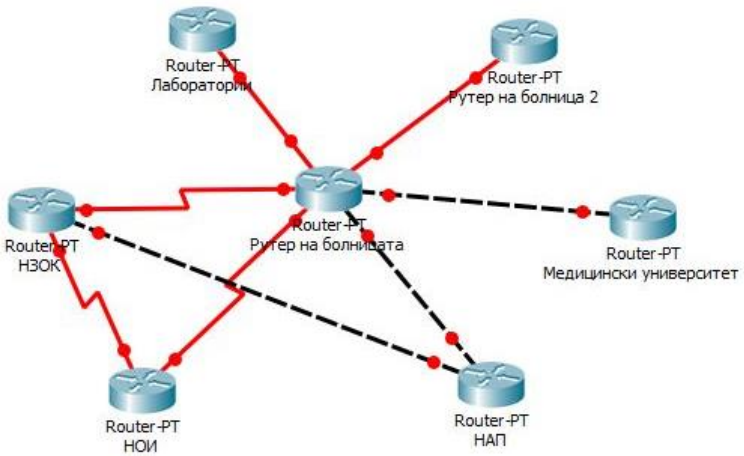
Към основните функции на външното ниво се отнася осъществяването на комуникация с други организации като: болници; лаборатории; медицински университети; НЗОК; НОИ; НАП.

Концепцията за сигурна връзка чрез Интернет се базира на връзката между отделни маршрутизатори. Те от своя страна осигуряват връзката

[3] Изобразяването е извършено с помощта на Сиско Пакет Трейсър.

между различните организации, които ги използват и поддържат. В повечето случаи това са доставчици на интернет услуги. Те формират гръбнака за осъществяване на защитена комуникацията между отделни организации и структурни звена от областта на здравеопазването. По този начин може да бъде изградена единна ИС, която ще предоставя достъп на пациента до информация за неговото здравословно състояние, както е описано в Националната здравна стратегия (2014 – 2020 г.). Като най-интензивна и сложна комуникация може да посочим осъществяването на връзка между ИС на едно лечебно заведение с тази на друго или на друга организация. В тези случаи връзката най-често се осъществява чрез използване на:

- Електронен портал за достъп;
- Контролиране на достъпа чрез потребителски роли;
- Електронен подпис;
- Използването на стандарти за шифриране, като:
  - Симетрично шифриране, което използва следните алгоритми:
    - Data Encryption Standard;
    - Triple Data Encryption Standard;
    - International Encryption Algorithm;
    - Advanced Encryption Standard.
  - Асиметрично шифриране, което използва:
    - RSA;
    - DSA;
- Използване на SSL сертификат.



Фигура 8. Комуникационни връзките между болница с други организации и структурни звена

За осъществяването на сигурна комуникация между ИС-и на организациите е необходимо да се използва **SSL сертификат**, чрез който се извършва криптиране на комуникациите. Автори като (Zhang & Liu, 2010),

(Benaloh, Chase, Horvitz, & Lauter, 2009), (Farzandipour, Sadoughi, Ahmadi, & Karimi, 2010) също обръщат внимание на значението на такъв сертификат като базова стъпка за осигуряване на защита.

Друг важен елемент от инфраструктурата за информационна сигурност е **електронният подпис**, използван за потвърждаване на самоличността на този, който изпраща съобщението. Той се прилага при изпращането на отчетите за медицинските дейности на лечебното заведение.

Други начини за достъп могат да бъдат предоставянето на **потребителски роли** и определяне на **правата за достъп** на регистрираните потребители. От съществено значение е въпросът, кой трябва да определи тези роли. Изследователи, работещи в областта (Kahn & Sheshadri, 2008), предлагат, тези роли да се определят от съответните институции, болници или специални комисии, докато други (Daglish & Archer, 2009) предлагат, пациентите да имат участие при определянето на достъпа. Според нас е добре да се подходи комбинирано, като първо се направи обратна връзка с пациентите, за изграждането на нужния интерфейс с цел по-добро обслужване, след което съответните институции, лечебни заведения или специални комисии да дефинират правилата.

Понастоящем тези начини за сигурна комуникация се използват за осъществяване на обмен на информация между лечебните заведения и НЗОК. И по-точно така се изпраща информация, свързана със здравното състояние на пациента:

- SSL сертификат осигурява защитена връзка за комуникация;
- Електронен портал за осъществяване на достъп;
- Електронен подпис, осигуряващ верификация на подателя на информацията;
- Предоставянето на ПИН код за достъп.

Според нас, посоченият по-горе начин на комуникация може да се използва за осъществяване на връзки с външни системи от два вида:

- Осъществяване на връзки с висок приоритет на информационна сигурност – с НЗОК, медицински университети, други болници, лаборатории;
- Осъществяване на връзки с по-нисък приоритет на информационна сигурност – с НАП и НОИ.

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. Този слой има най-важно значение за функциониране на ИС. Основен компонент в него е централизираното хранилище за данни, в което се съхраняват бази от данни (БД) и откъдето се контролира достъпът до всички подмрежи и свързани устройства.

Централизираното хранилище за данни е основен компонент на вътрешното ниво. То може да бъде съставено от различни физически БД, които могат да са хетерогенни и да се различават по типа, структурата, модел на данните и модел на складиране на данните. БД 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 БД.

Достъпът до сървъра за БД от различните отделения на МБАЛ се осъществява чрез:

1. Първо от главния комутатор, който осигурява главната връзка;
2. От предоставените компютърни конфигурации с нужните настройки и от софтуерните инструменти за обработка, приемане и предаване на информация;
3. За осигуряване на защитени комуникации може да се приложат запазени адреси за компютърните конфигурации и адреси на мрежите, които могат да комуникират помежду си.

Препоръчително е, всички БД да са централизирани, разположени на сървъра в централизираното хранилище за данни. Остарелите софтуерни системи с локални БД, които се използват само за информация за минали периоди, трябва да бъдат проучени с цел възможност за интегриране с нова БД в централизираното хранилище. Това ще осигури необходимото ниво на защита.

Като допълнителна мярка за повишаване на сигурността считаме, че е необходимо **обособяване на потребителски роли** за достъп до наличните компютърни конфигурации в отделенията и до ресурсите на централизираното хранилище за данни. Това се налага да бъде приложено във всяко отделение.

При осигуряване на защитата на личните данни трябва да отчетем и изискванията на GDPR, като специфичните неща за лечебните заведения са насочени към:

- Потребителските роли – даването на права на потребителите, които ще работят със системата и проследяване за евентуално неправомерно използване на тези права;
- Защита на данните вътре в системата – криптиране на данните.

Това може да се извърши с конфигурирането на протокол по мрежата SNMP (Simple Network Management Protocol). Той представлява стандартизиран интернет протокол, който колекционира и организира информацията за състоянието на всички устройства, включени към мрежата.

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. От архитектурна гледна точка това е допълнително подниво, свързано с ограничаването на физическия достъп чрез заключване на помещенията с посочените компютри, устрой-

ства и апарати. Регулирането на достъпа до отделенията може да се извършва с карти за достъп. Тази регулация може да бъде добавена като логическа подсистема към ИС на лечебното заведение.

За спазване на изискванията на GDPR е необходимо криптиране на личните данни, складирани в централното хранилище. Това ще осигури допълнително ниво на защита на чувствителната информация. То може да бъде извършено с различни методи в зависимост от използваните видове БД. В практиката се прилагат три начина за криптиране на БД: метод на интерфейс за програмиране на приложения (API); метод, използващ добавен модул за криптиране; прозрачен метод за криптиране на данни.

В повечето случаи вместо да се криптира цяла БД, е по-подходящо да се приложат различни нива на криптиране. Правилото в тези случаи е, че по-големият обхват на криптиране намалява производителността. Нивата на криптиране са на ниво: клетка; колона; таблици; файлове.

Криптирането може да бъде извършено на базата на два принципа:

- Симетрично – информацията се криптира, когато се записва в БД, и се декриптира, когато се изчита от там;
- Асиметрично – използват се публични и частни ключове, като публичните позволяват лесно криптиране, но се изисква частният ключ, за да може да бъде прочетена тази информация.

В заключение следва да се отбележи, че предложената концепция за модел има за цел да осигури оптимално ниво на защита на информацията в лечебните заведения, като се базира на:

- добри практики;
- следва препоръките, насочени към техническото изпълнение, предоставени от GDPR;
- базира се на принципа на нива на защита, като се стреми да намали щетите от евентуален пробив;
- остава отворен 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.

4. Новите ИТ – предизвикателства и възможности за информационната сигурност

4.1. Big data и Big data analytics

Big data analytics (BDA) се налага като ефективен инструмент в много сфери на съвременната обработка на информация, включително в

сферата на информационната защита. Осигурявайки инструменти за събиране и анализиране на големи количества от дигитална информация, генерирана от различни източници или регистрирана от различни устройства, BDA помага за откриване и дефиниране на модели и тенденции на непозволено поведение, търсене на методи за проследяване на киберпрестъпници, предсказване и стопиране на потенциални кибератаки.

Възможностите на Big data и BDA да подпомогнат информационната сигурност са свързани с множество проблеми и предизвикателства.

Анализът на Big data е значително по-сложен от прилагания в традиционните БД. Big data са с големи обеми, неагрегирани, в различни формати и тяхната обработка трудно може да се извърши в паметта само на един компютър. Обработката на Big data включва механични процеси и алгоритми. Използваните методи за анализ на Big data са два основни вида – реагиращ и прогнозиращ (CHAOVALITWONGSE, W., HUANG, S., 2015).

Реагиращият анализ има за цел да направи статистика за текущите и историческите данни и да осигури информация за това, което се е случило и защо се е случило. Той включва методи като статистическо моделиране, генериране на отчети за тенденциите, визуализация, асоциация и корелационен анализ.

Прогнозиращият анализ се фокусира върху използването на известни данни (данни за обучение), които включват входни свойства на данните (атрибути) и стойности на отговора (целеви модели) за изграждане на предсказуем модел (решение), за да се направят прогнози за невидими данни (тестови данни). Той използва методи като векторни машини, линейна регресия/класификация, нелинейна регресия (обобщаващ линеен модел), дърво на решенията, теорията на Bayes, невронни мрежи и др.

Big Data технологиите, използвани в системите за защита, са способни да открият заплахите предварително. Например те могат да открият нетипично поведение в мрежата, да предскажат атака и да анализират източниците на атака.

Big Data създава условия за ефикасно и ефективно прилагане на някои техники за откриване на измами. В специализираната литература техниките за анализ на данни са разделени в две основни групи: *статистически* техники и техники, използващи *изкуствен интелект*.

Big Data Working Group дефинира четири аспекта на защитата в Big data, които са: защита на инфраструктурата; поверителност на данните; управление на данните; интегритет и реактивна защита (BIG DATA WORKING GROUP, 2013). Всяка от областите е свързана с множество проблеми. Например защита на инфраструктурата има следните проблеми:

- Наличие на еднослойна защита – компаниите трябва да включат многопластова отбрана в рамките на фирмената стратегия за отбрана, която е адресира както към вътрешни, така и външни заплахи за сигурността.

- Трансфериране на данни чрез множество устройства, което изисква допълнителни нива на сигурност и мониторинг, за да се гарантира, че данните не се прехващат по маршрута от едно устройство до друго.
- Бързо развитие на технологията за големи данни и на поддържащата я инфраструктура (като облачните услуги), която трябва да може да обработва данни от безкраен брой точки със скорост, сигурност и надеждност. Инфраструктурата трябва да включва мерки за сигурност, които да пазят информация на всеки етап от процеса.

На практика, освен че подсилва бизнес интелигентността, Big Data предоставя възможност да засили киберсигурността. Това увеличава съществуващите вече проблеми и предизвикателства, които изискват внимание и очакват решения.

Основните проблеми със сигурността на Big Data са свързани със:

- заплахи за сигурността на данните;
- рискове за поверителност;
- необходимост от потвърждаване на достоверността на данните;
- липсва технология за защита на поверителността на Big Data.

Посочените проблеми със сигурността на Big Data изискват справяне с много предизвикателства, по-важните от които се отнасят до:

a) Приемане на защитата за основен приоритет за Big Data платформите, което ще акцентира вниманието на мениджъри и разработчици в тази посока.
b) Въвеждане на реактивна и проактивна защита.
c) Физическата защита на устройствата и сървърите, които съдържат чувствителна информация, трябва да бъде управлявана с особено внимание и те да са изолирани от другите устройства.
d) Защитата на приложенията е толкова важна, колкото и защитата на устройствата. В тази връзка защита на Data mining solutions е от особено значение. Именно тези решения са в основата на Big Data платформите, допринасят за откриване на модели на поведение и тенденции на развитие и на тази база предлагат бизнес стратегии. Това значение на Data mining solutions изисква, те да са защитени не само срещу външни заплахи, но и от вътрешни индивиди, които злоупотребяват с привилегията си за достъп до чувствителна информация.
e) Високо ниво на контрола на достъпа, който да се осигурява с криптирана автентификация и да се определи кой какви данни може да вижда.
f) Използване на инструменти за защита в реално време. Тези инструменти генерират огромно количество информация. Тук проблем е да се игнорират неважните сигнали, така че служителите да се насочат към истинските нарушения.

g) Управление на складирането на данните. За Big Data архитектурата е типично, данните да се складират на множество нива в зависимост от тяхната важност за бизнеса и разходите за съхраняването им.
h) Осъществяване на детайлен одит, който може да помогне да бъде определено кога пропуснати засега атаки могат да се случат, какви са били последствията, какво да се промени в действащата система.
i) Използване на разпределени системи. С цел по-бърз анализ повечето Big Data платформи в действителност разпределят огромната работа по обработката на данните между много системи.

Наред с множеството възможности, които Big Data предоставя на потребителите (бизнес потребители и индивиди), тя води със себе си и множество заплахи за обществото, бизнеса и индивидите. Едновременно с това BDA се налага като ефективен инструмент в много сфери на съвременната обработка на информация, включително в сферата на информационната защита. Този доклад се занимава с проблемите и предизвикателствата на защита на Big Data в тези два аспекта.

4.2. Bring Your Own Device (BYOD)

С масовото използване на смартфоните и другите мобилни устройства и способността им с лекота да се справят със сложни и разнообразни задачи, заедно с тенденцията за засилваща се зависимост на хората от тези устройства, можем да отбележим, че мобилните технологии сериозно настъпват в сектора на здравеопазването. По данни на проучване, извършено от Spyglass Consulting Group (Malkary, 2018), 73% от изследваните медицински заведения са в процес на развиване на мобилни стратегии за отговаряне на нуждите на комуникацията и за увеличаване на сътрудничеството, а над 90% от здравните системи планират значителни инвестиции в сигурна мобилна технология в следващите 18 месеца.

Мобилните устройства предлагат огромни възможности за подобряване нивото на обслужване, производителността и редуциране на разходите в сектора на здравеопазването. Потенциалът им е отчетен още преди повече от две десетилетия, като още тогава са изведени редица техни ключови приложения (Hameed, 2003).

Наред с предимствата, които предоставят мобилните устройства, ги съпътстват немалко предизвикателства, свързани с безопасността на информацията (Varbanov, 2014). Основните рискове в тази насока включват:

- вредни програми;
- изтичане на данни поради нарушаване на контрола за достъп и на политиката за безопасност;
- нерегламентиран трафик от или към интернет;
- нарушаване на правилата за използване на устройствата.

Заедно с рисковете, съществуват и друг тип бариери, свързани с юридически правила и разпоредби. Вземайки предвид законодателството в

Европейския съюз и влезлия в сила GDPR (General Data Protection Regulation) (General Data Protection Regulation, n.d.), това са допълнителни мерки, въведени за защита на личните данни, което има сериозна тежест, особено за лечебните заведения, тъй като те боравят с изключително важна информация.

От техническа гледна точка внедряването на мобилни технологии в сектора на здравеопазването налага справяне с множество предизвикателства, които най-общо включват (Mehta, 2019):

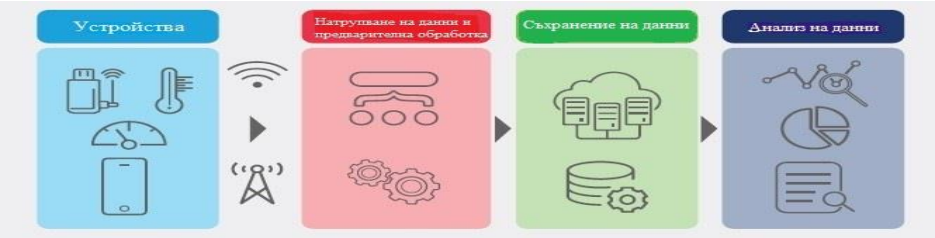
- сложност на системната интеграция;
- проблеми с оперативна съвместимост;
- рискове, свързани с данните;
- неизпълнение на ангажиментите към пациентите;
- незадоволителен потребителски опит;
- необходимост от персонализиране;
- ненадеждни решения.

4.3. The Internet of Things (IoT)

Устройствата с възможност за IoT (The Internet of Things) предоставят възможност за извършване на отдалечен мониторинг, разгръщайки потенциала за запазване здравето на пациентите и осигурявайки възможност на лекарите да повишат качеството на предоставяните грижи. По този начин се засилват ангажираността и удовлетвореността на пациентите, тъй като взаимодействията с лекарите стават по-лесни и ефективни, а дистанционното наблюдение на здравето на пациента помага за намаляване продължителността на болничния престой и предотвратява повторното приемане.

Разпространението на специфични за здравето IoT устройства отваря широки възможности, а огромното количество данни, генерирани от тези свързани устройства, притежават потенциала да трансформират здравеопазването.

IoT има четири компонентна архитектура, която по същество представлява стъпки в един процес (вж. фиг 9.), в който отделните компоненти са свързани по начин, по който данните се улавят или обработват от един компонент и предават стойност на следващия.



Фигура 9. Архитектура на системата за IoT (Karjagi, n.d.)

IoT устройствата в сектора на здравеопазване използват преносни мрежи, за да изпращат / получават данни, свързани със здравето на пациентите, което се счита за потенциална заплаха. Това налага изграждане на защитена и сигурна медицинска система, базирана на IoT, която да гарантира мащабируемост, оперативна съвместимост на устройствата, сигурност, мобилност и независимост от типа на мрежата (Alqantani, 2018).

По данни на изследване за 2018 г. предизвикателствата пред IoT в сектора на здравеопазване включват: автентификация, осигуряване на хранилище за данните, криптиране и образование и обучение (Kaplan, 2018):

В едно от актуалните за 2019 г. изследвания се посочват следните предизвикателства за IoT в здравеопазването (M., 2019):

- провал на повечето инициативи на IoT;
- прекалено много данни;
- киберсигурност;
- остаряла инфраструктура, която възпрепятства иновациите;
- проактивни нагласи, водещи до положителни резултати от IoT.

Заключение

Към настоящия момент малък дял от лечебните заведения в България отговарят на изискванията за високо и комплексно ниво на информационна сигурност. Масовата дигитализация, интеграцията на приложения и системи на лечебните заведения води до увеличаване на рисковете в сигурността.

Едновременно с това внедряването на нови технологии като IoT, BYOD, Big data и др. предоставя много възможности, но поражда и съществени рискове за сигурността на ИС.

Настоящото изследване предлага концепция за модел, който има за цел постигането на оптимално ниво на защита на информацията в лечебните заведения. Моделът се базира на: добри практики; следва препоръките, насочени към техническото изпълнение, изисквани от GDPR; отчита принципа на нивата на защита. В същото време концептуалният модел 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.

Използвани източници

Åhlfeldt, R., Spagnoletti, P., & Sindre, G. (2007). Improving the Information Security Model by using TFI. *New Approaches for Security, Privacy and*

Trust in Complex. Sandton. Retrieved from https://www.researchgate.net/publication/220722598_Improving_the_Information_Security_Model_by_using_TFI

Alqantani, F. (02 2018 r.). The Application of the Internet of Things in Healthcare. *International Journal of Computer Applications, 180*.

Benaloh, J., Chase, M., Horvitz, E., & Lauter, K. (2009). Patient controlled encryption: Ensuring privacy of electronic medical records. *ACM workshop on cloud computing security*, (стр. 103-14). Извлечено от http://erichorvitz.com/ccsw_2009_benaloh_chase_horvitz_lauter.pdf

Bosworth, S., Kabay, M., & Whyne, E. (Eds.). (2014). *Computer security handbook* (Sixth edition ed.). John Wiley & Sons.

Daglish, D., & Archer, N. (2009). Electronic personal health record systems: a brief reviewof privacy, security, and architectural issues. *Proc world congress privacy,security, trust and the management of e-business congress;*, (стр. 110-20).

Farzandipour, M., Sadoughi, F., Ahmadi, M., & Karimi, I. (2010). Security requirements andsolutions in electronic health records: lessons learned from a comparativestudy. *Journal of Medical Systems, Volume 34, Issue 4*, 629-642. Извлечено от https://link.springer.com/article/10.1007/s10916-009-9276-7?

Fernandez, E., & Mujica, S. (2011). Model-based development of security requirements. *Clei electronic journal, 14*(3). Retrieved from http://www.scielo.edu.uy/scielo.php?script=sci_arttext&pid=S0717-50002011000300003

General Data Protection Regulation. (н.д.). (Intersoft Consulting) Изтеглено на 15 07 2019 г. от gdpr-info.eu: https://gdpr-info.eu/

Hameed, K. (2003). The application of mobile computing and technology to health care services. *Telematics and Informatics 20 (2003) 99–106*.

Hunt, G., Hydrie, A., Welland, R., Tabbara, B., Levi, S., & Rehof, J. (2005). *United States of America Patent No. US 6,907,395 B1.* Retrieved from http://patft.uspto.gov/netacgi/nph-Parser?Sect1=PTO2&Sect2=HITOFF&u=%2Fnetahtml%2FPTO%2Fsearch-adv.htm&r=142&f=G&l=50&d=PTXT&s1=%22US+6,907,395+B1%22&p=3&OS=%22US+6,907,395+B1%22&RS=%22US+6,907,395+B1%22

Kahn, S., & Sheshadri, V. (2008). Medical record privacy and security in a digitalenvironment. *IT Professional, Volume 10, Issue 2*, 46-52. Извлечено от https://ieeexplore.ieee.org/document/4476253

Kaplan, Й. (25 04 2018 г.). *Application and Challenges of IoT in Healthcare*. (C. Pro, Продуцент) Изтеглено на 07 09 2019 г. от Career Pro: https://www.careerpro.com/2018/04/application-and-challenges-of-iot-in-healthcare/

Karjagi, R. (н.д.). *What can IOT do for healthcare*. (Wipro Limited) Изтеглено на 15 09 2019 г. от Wipro: https://www.wipro.com/en-IN/business-

process/what-can-iot-do-for-healthcare-/?fbclid=IwAR0YOuaAivUYdUQXTZ5twWwh-N3CTj-0SoYAE1uJbq2LJA1twmVU1pgo1f8

Lee, Y. (1999). *Information modeling: from design to implementation*. Retrieved from National Institute of Standards and Technology: https://tsapps.nist.gov/publication/get_pdf.cfm?pub_id=821265

M., B. (09 01 2019 r.). *The Biggest Challenges to Healthcare IoT in 2019*. (Dogtown Media) Изтеглено на 11 09 2019 r. от Dogtownmedia: https://www.dogtownmedia.com/the-biggest-challenges-to-healthcare-iot-in-2019/

Malkary, G. (2 04 2018 r.). Hospital IT smatrphone investmentsare driving clinical transformation. *Hospital IT smatrphone investmentsare driving clinical transformation*. MENLO PARK, CA. Изтеглено на 10 09 2019 r. от http://www.spyglass-consulting.com/press_releases/SpyglassPR_CLINICAL_COMM_2018.v1.0.pdf

Mehta, S. (2019). KEY CHALLENGES IN MOBILE HEALTHCARE IMPLEMENTATION. Edison, New Jersey, USA. Изтеглено на 21 06 2019 r. от https://health.techjini.com/blog/key-challenges-in-mobile-healthcare-implementation/?fbclid=IwAR1SuqUiwpVpkA3t25BtzeBXajs5IJW985JdneVLpptknPNsry4OeWVkJNg

Myagmar, S., Lee, A., & Yurcik, W. (2005). Threat Modeling as a Basis for Security Requirements. *IEEE Symposium on Requirements Engineering for Information Security.* Retrieved from https://www.researchgate.net/publication/228634178_Threat_Modeling_as_a_Basis_for_Security_Requirements

Shevchenko, N., Chick, T., O'Riordan, P., Scanlon, T., & Woody, C. (2018). *Threat Modeling: A Summary of Available Methods.* Извлечено от Software Engineering Institute: https://resources.sei.cmu.edu/library/asset-view.cfm?assetid=524448

Teare, D. (1999). *Designing Cisco Networks.* Cisco Press.

The Business Model for Information Security. (n.d.). Retrieved from ISACA.org: http://www.isaca.org/Knowledge-Center/BMIS/Documents/BMISBrochure.pdf

Varbanov, R. (2014). APPLICATIONS OF THE BYOD CONCEPTION – BENEFITS, RISKS AND APPROACHES. *Business management*(2).

Whitman, M., & Mattord, H. (2013). *Management of Information Security.* Cengage Learning.

Zhang, R., & Liu, L. (2010). Security models and requirements for healthcare application clouds. *Proc IEEE 3rd int cloud computing (CLOUD)* (стр. 268-75). IEEE. Извлечено от https://ieeexplore.ieee.org/document/5557983

Димитров, В. (2018). *Модел за сигурност на ИКТ.* София: Авангард Прима.

ИНСТИТУТ ЗА НАУЧНИ ИЗСЛЕДВАНИЯ
ПРИ СТОПАНСКА АКАДЕМИЯ
„Д. А. ЦЕНОВ" - СВИЩОВ

АЛМАНАХ
НАУЧНИ ИЗСЛЕДВАНИЯ

ИНСТИТУЦИИ, ПОЛИТИКИ И ПРЕДИЗВИКАТЕЛСТВА ПРЕД ДИГИТАЛНАТА ТРАНСФОРМАЦИЯ

том 28, 2020 г.

Академично издателство „ЦЕНОВ"
Свищов - 2020 г.

СТОПАНСКА АКАДЕМИЯ „Д. А. ЦЕНОВ”

АЛМАНАХ НАУЧНИ ИЗСЛЕДВАНИЯ

ТОМ 28

ИНСТИТУЦИИ, ПОЛИТИКИ И ПРЕДИЗВИКАТЕЛСТВА ПРЕД ДИГИТАЛНАТА ТРАНСФОРМАЦИЯ

Даден за печат на 27.02.2020 г., излязъл от печат на 30.03.2020 г.
Поръчка № 18460, тираж: 100 бр.

Издателство и печат: Академично издателство „Ценов”
Свищов, ул. Градево № 24

ISSN 1312-3815

СЪДЪРЖАНИЕ

Раздел I
Пазари, управление и иновации в икономиката на знанието

Маргарита Богданова, Христо Сирашки,
Евелина Парашкевова, Мариела Стоянова
Гъвкаво управление на проекти в организациите от публичния сектор 7

Ангелин Лалев, Александрина Александрова
Използване на дълбоки невронни мрежи за откриване на измами
с кредитни карти 39

Десислава Алексиева, Елена Йорданова
Интереси и поведение: управленски аспекти..... 63

Раздел II
Глобализация, конкурентоспособност и сътрудничество
за интелигентен растеж

Силвия Костова, Крум Крумов, Даниела Вткова-Милушева
Ролята на вътрешните и външните одитори за идентифициране
на измами в предприятията..... 95

Силвия Костова, Пресиян Василев, Ивана Димова Характеристика
на измамата и особености на извършителя на измами..... 126

Тихомир Върбанов Оценка на конвергенцията
в Европейския съюз по разходи за социална защита 157

Таня Тодорова Влияние на бюджетното салдо върху икономическия
растеж..... 183

Раздел III
Финансова стабилност, икономически политики, регулации и устойчиво развитие

Веселин Попов, Петя Емилова, Искрен Таиров, Владислав Василев
Информационната сигурност на лечебните заведения в България 211

Красимир Шишманов, Мария Ташкова, Михаела Маркова
Съвременни тенденции в създаването на приложения за електронна търговия 243

Атанаска Решеткова, Криста Нейкова
Влияние на дигитални маркетингови канали върху клиентската лоялност в банковия сектор 273

Диана Ималова, Галя Кузманова, Радосвета Кръстева
Обучението в докторска програма „Счетоводна отчетност, контрол и анализ на стопанската дейност (Счетоводство)" в СА „Д. А. Ценов" – проблеми и перспективи 306