ХМЕЛЬНИЦЬКИЙ УНІВЕРСИТЕТ УПРАВЛІННЯ ТА ПРАВА ІМЕНІ ЛЕОНІДА ЮЗЬКОВА

ФАКУЛЬТЕТ УПРАВЛІННЯ ТА ЕКОНОМІКИ

Кафедра: менеджменту, фінансів, банківської справи та страхування

МАГІСТЕРСЬКА РОБОТА
на здобуття освітнього ступеня магістра
на тему:

«Управління інформаційною безпекою закладу охорони здоров'я (на матеріалах комунального підприємства «Хмельницька міська дитяча лікарня»)»

Виконав: студент магістратури за спеціальністю 073 Менеджмент
Бойко І.М
(прізвище та ініціали)

Керівник: к.е.н., доцент,
Захаркевич Н.П.
(науковий ступінь, вчене звання, прізвище та ініціали)

Рецензент: _____
(науковий ступінь, вчене звання, прізвище та ініціали)

Хмельницький – 2020 рік

Анотація

Бойко І.М. Управління інформаційною безпекою закладу охорони здоров'я (на матеріалах комунального підприємства «Хмельницька міська дитяча лікарня»)– Кваліфікаційнанауковапраця на правахрукопису. Магістерськаробота на здобуттяосвітньогоступенямагістра за спеціальністю 073 Менеджмент. – Хмельницький університетуправління та праваіменіЛеонідаЮзькова, Хмельницький, 2020. – 75 с.

Мета роботи полягає в поглибленні теоретичних і практичних аспектів управління інформаційною безпекою закладу охорони здоров'я.Встановлено, що процес забезпечення інформаційної безпеки закладу охорони здоров'я можна представити як взаємодію трьох підсистем: підсистема інформаційного забезпечення процесу управління; підсистема захисту інформаційного середовища; підсистема діагностики рівня інформаційної безпеки.

Обґрунтовано необхідність впровадження системи менеджменту інформаційної безпеки, що базується на вимогах стандарту ISO/IEC 27001. Представлена модель системи менеджменту інформаційної безпеки закладу охорони здоров'я, описані основні етапи її впровадження у КП «Хмельницька міська дитяча лікарня». Наголошено на необхідності регламентування управління інформаційною безпекою через систему локальних нормативних актів, представлено основні складові такої системи, зокрема Концепцію інформаційної безпеки, паспорт загрози інформаційної безпеки закладу охорони здоров'я.

Сформовано комплекс заходів забезпечення інформаційної безпеки КП «Хмельницька міська дитяча лікарня», який передбачає зниження інформаційних загроз, що пов'язані із людським фактором. До таких заходів віднесено: організація тренінгів для персоналу служби інформаційної безпеки, зокрема на знання вимог стандарту ISO/IEC 27001; впровадження системи корпоративних носіїв інформації (флешки); організація навчання персоналу підприємства з питань інформаційних безпеки (зокрема тих, хто

працює з медичними інформаційними системами), підготовка інформаційних матеріалів (інструкцій, пам’яток) тощо. Для кожного заходу визначено необхідні процедури для реалізації, очікуваний результат, а також обґрунтовано витрати на впровадження.

Ключові слова:інформаційна безпека, загрози, ризики, система менеджменту інформаційної безпеки.

Annotation

Boyko I.M. Managementofinformationsecurityofthehealthcareinstitution (onthematerialsofthecommunalenterprise "KhmelnytskyCityChildren'sHospital") - Qualifyingscientificworkontherightsofthemanuscript. Master'sworkforobtainingtheeducationaldegreeofmasterinthespecialty 073 Management. - KhmelnytskyUniversityofManagementandLawnamedafterLeonidYuzkov, Khmelnytsky, 2020. - 75 p.

Theaimoftheworkistodeepenthetheoreticalandpracticalaspectsofinformationsecuritymanagementof a healthcareinstitution. Thenecessityofimplementationoftheinformationsecuritymanagementsystembasedonthe requirementsofthe ISO / IEC 27001 standardissubstantiated. Theneedtoregulatethemanagementofinformationsecuritythrough a systemoflocalregulationsisemphasized, themaincomponentsofsuch a systemarepresented, inparticulartheConceptofinformationsecurity, passportofinformationsecuritythreatof a healthcareinstitution. A setofmeasurestoensureinformationsecurityofKhmelnytskyCityChildren'sHospitalhasbeenformed, whichprovidesforthereductionofinformationthreatsrelatedtothehumanfactor. Suchmeasuresinclude: organizationoftrainingsforinformationsecuritypersonnel, inparticularonknowledgeoftherequirementsofthe ISO / IEC 27001 standard;

introductionof a systemofcorporatemedia (flashdrives); organizationoftrainingofthecompany'spersonneloninformationsecurityissues (includingthosewhoworkwithmedicalinformationsystems), preparationofinformationmaterials (instructions, memos), etc.

Keywords:informationsecurity, threats, risks, informationsecuritymanagementsystem.

ЗМІСТ

ВСТУП

Актуальність теми.Одним з найважливіших напрямів, що дозволяють закладу охорони здоров’я реалізувати свою діяльність на сучасному рівні, є впровадження інформаційних систем. Тема інформатизації є надзвичайно актуальною в галузі охорони здоров'я, що підтверджується широкомасштабними заходами, реалізованими в рамках програми модернізації охорони здоров'я в Україні. Інформатизація закладів охорони здоров’я не є самоціллю, а дозволяє деталізувати і систематизувати величезний обсяг інформації, що надходить до керівництва організації. Разом з тим інформаційні системи і мережі закладу охорони здоров’я є об’єктом численних загроз для безпеки. Джерелами загроз можуть бути хакерські атаки, шахрайські програми, різного роду впливи, що викликають відмови в роботі інформаційних систем. Незалежно від того, в якому вигляді інформація зберігається, яким чином використовується, необхідно реалізовувати адекватні заходи захисту. Кожен керівник закладу охорони здоров’я повинен об'єктивно оцінювати поточний стан інформаційних систем, бачити і розуміти потреби в інформаційному забезпеченні та існуючі інформаційні проблеми. У цьому контексті тема створення дієвої системи управління інформаційною безпекою медичної організації залишається однією з найбільш актуальних у сфері інформатизації та побудови системи управління

Серед провідних вітчизняних та зарубіжних дослідників проблематики варто виділити таких: Гавловський В.Д. [10], Дзьобань О.П. [13], Дудатьєв А.В. [15], Альошин Г.В., Герасимов С.В., Засядько А.А. [28], Кіреєнко О. [31], Когут Н.Д. [32], Курило А.П. [34], Ліпкан В.А. [39], Манин С.А., Двадненко М.В. [40], Маркіна І.А. [41], Перун Т.С. [52], Рой Я.В. [54], Самохвалов Ю.Я. [59], Северина С.В. [60], Стрельцов А.А. [65], Чунарьова А. [75]ШахаловІ.Ю. [77]. Більшість науковихпрацьприсвячуєтьсядослідженню інформаційної безпеки

комерційних структур, забезпеченнюінформаційноїбезпеки інформаційних систем, оцінюванню інформаційних ризиків тощо. В той же час розробці практичних аспектів управління інформаційною безпекою закладу охорони здоров'я приділено недостатньо уваги.

Мета й завдання дослідження. Мета роботи полягає в поглибленні теоретичних і практичних аспектів управління інформаційною безпекою закладу охорони здоров'я.Визначена мету зумовила необхідність виконання таких завдань:

– розкрити поняття та значення інформаційної безпеки в сучасних умовах господарювання;

– розглянути методи забезпечення інформаційної безпеки підприємства;

– проаналізувати організаційне забезпечення управління інформаційною безпекою закладу охорони здоров'я;

– оцінити рівень інформаційної безпеки медичної установи;

– визначити напрями підвищення ефективності управління інформаційною безпекою Комунального підприємства «Хмельницька міська дитяча лікарня».

Об'єктом дослідження є система управління інформаційною безпекою як підсистема загальної системи управління організації**. Предметом дослідження** є теоретичні та практичні аспекти управління інформаційною безпекоюКП «Хмельницька міська дитяча лікарня»**.**

Методи дослідження. Теоретичну й методологічну основу роботи становлять наукові праці провідних вітчизняних і зарубіжних вчених з питань пошуку та реалізації шляхів удосконалення управління інформаційною безпекою організацій.

У процесі вирішення поставлених завдань використано такі методи наукового дослідження: теоретичного узагальнення, системного аналізу, синтезу (для дослідження теоретичних основ управління інформаційною

безпекою); групування і класифікації (для дослідження методів протидіїінформаційним загрозам на діяльність організацій); аналітичний метод та експертне опитування – для оцінювання рівня інформаційної безпеки КП «Хмельницька міська дитяча лікарня»; системний метод – для обґрунтування перспективних напрямів розвитку системи управління інформаційною безпекою та оцінки ефективності їх реалізації; абстрактно-логічний - для теоретичних узагальнень і висновків за результатами дослідження.

Інформаційну базу дослідження склали Конституція України, закони України: «Про основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки», «Про інформацію», «Про Концепцію Національної програми інформатизації», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про захист персональних даних», конвенції, угоди, які регулюють інформаційну безпеку, як суспільні відносини в інформаційному середовищі, законодавство зарубіжних країни, локальні акти Комунального підприємства «Хмельницька міська дитяча лікарня». Емпіричну базу дослідженнястановлять статистичні матеріали, що характеризують стан інформаційної безпеки в Комунальному підприємстві «Хмельницька міська дитяча лікарня», довідкові видання, наукові публікації з досліджуваної проблематики.

Практичне значення одержаних результатів полягає в узагальненні теоретичних основ управління інформаційною безпекою закладу охорони здоров’я, опрацюванні конкретних пропозицій щодо удосконалення управління інформаційною безпекою.

РОЗДІЛ 1
ТЕОРЕТИЧНІ ЗАСАДИ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ ЗАКЛАДУ ОХОРОНИ ЗДОРОВ'Я

1.1. Сутність управління інформаційною безпекою закладу охорони здоров'я

Розвиток сучасного суспільства багато в чому ґрунтується на використанні інформаційних ресурсів. Інформація перестала бути тільки одним з факторів виробництва, а управління інформацією не є більш прерогативою тільки корпоративних структур. Інформація виступає також особливого роду громадським активом, причому його особливістю слід вважати формування одночасних позицій представників суспільства як споживачів інформації і як учасників її створення. Розвитку ролі інформації в суспільстві сприяє не лише створення нових засобів зв'язку і алгоритмів обробки інформації, втілених в програмні продукти. Основною рушійною силою зростання значущості інформації для суспільства слід вважати зміну ставлення до інформації. Сьогодні інформація стає продуктом, одночасно визначає умови суспільного розвитку. Тому безумовну значимість набуває послідовна реалізація концепції інформаційної безпеки.

Інформаційну безпеку раніше досліджували лише як складову економічної безпеки, або як окрему категорію, пов'язану з захистом технічних засобів обробки, зберігання, переробки та представлення інформації. Серед робіт вчених, які займалися вивченням інформаційної безпеки особливу увагу заслуговують дослідження Домарева В.В. [14], Расторгуєва С.П. [53], Феоктистова Г.Г. [71], Стрельцова О.О. [65], Петренко С., Алексенцев А.І. [12] та інших (табл. 1.1).

Сучасне трактування поняття «інформаційна безпека» досить неоднозначне. Це свідчить про те, що не існує єдиного підходу до її

визначення, так як сутність даноїкатегорії залежить від безлічі обставин, якими характеризується соціально-економічнасистема. У табл. 1.1 приведена інтерпретація поняття «інформаційна безпека»

Таблиця1.1. Інтерпретація поняття "інформаційна безпека"

№з/п	Автор / джерело	Трактування поняття
1	2	3
1	Горбатюк О. [17]	стан захищеності інформаційних ресурсів людини, суспільства і держави, яке забезпечує реалізацію і прогресивний розвиток життєво важливих для них інтересів
		рівень захищеності інформаційного середовища суспільства, який забезпечує його формування, використання і розвиток в інтересах громадян, організацій, держави і нейтралізації негативних наслідків інформатизації суспільства.
2	Стрельцов А.А. [68]	неможливість нанесення шкоди властивостям об'єкта безпеки, що може бути спричинена інформацією і інформаційною інфраструктурою.
3	Великий економічний словник [8]	забезпечення захисту інформації від випадкового або навмисного доступу осіб, які не мають на це право
		інтегральна властивість інформації, що характеризується конфіденційністю, цілісністю і доступністю
		захищеність пристроїв, процесів, програм, середовища і даних, що забезпечує цілісність інформації, яка обробляється, зберігатися і видається цими засобами
		властивість середовища забезпечувати захист інформації
4	Садердінов А.А. [58]	захищеність інформації, якою володіє суб’єкт (продукує, передає або отримує) від несанкціонованого доступу, руйнування, модифікації, розкриття і затримок при вступі. Інформаційна безпека включає в себе заходи по захисту процесів створення даних, їх введення, обробки і виведення
5	Вікіпедія[25]	стан збереження інформаційних ресурсів держави і захищеності законних прав особистості і суспільства в інформаційній сфері
		відсутність неприпустимого ризику, пов'язаного з витоком інформації технічними каналами, несанкціонованими і ненавмисними діями на дані і (або) на інші ресурси автоматизованої інформаційної системи, що використовуються в автоматизованій системі
6	Домарєв В.В. [14]	захищеність інформації і підтримуючої інфраструктури від випадкових або навмисних впливів природного або штучного характеру, що можуть призвести до нанесення шкоди власникам або користувачам інформації і підтримуючої інфраструктури
7	Алексенцев А.І. [12]	властивість середовища передавати, накопичувати, обробляти та зберігати інформацію, що характеризує її ступінь захищеності від дестабілізуючого впливу зовнішнього середовища і внутрішніх загроз, тобто її конфіденційність, цілісність і стійкість до руйнуючих впливів і перешкод
8	Министерств оборони США [85]	захист інформації та інформаційних систем від несанкціонованого доступу або модифікації інформації, яка зберігається, обробляється, або передається, а також від відмови в обслуговуванні авторизованих

		користувачів

Продовження табл. 1.1

1	2	3
9	КОЛЕС 27000:2009 [86]	збереження конфіденційності, цілісності та доступності інформації
10	ГОСТ РИСО/МЭК 27002-2012 [26]	захист конфіденційності, цілісності та доступності інформації; крім того, сюди можуть бути віднесені й інші властивості, наприклад автентичність, підзвітність, неспростовності і надійність

Примітка. Систематизовано автором.

Аналіз змісту визначень, наведених в табл. 1.1 дає можливість виділити різні аспекти, які дозволяють тлумачити «інформаційну безпеку» в залежності від контексту застосування даного поняття [13, с.61; 77; 60]:

- це ступінь захищеності інформаційного середовища, який забезпечує його формування, використання і розвиток в інтересах громадян, організацій, держави і нейтралізації негативних наслідків інформатизації суспільства;

- це стан захищеності інформаційних ресурсів людини, суспільства і держави, яке забезпечує реалізацію і прогресивний розвиток життєво важливих для них інтересів; це стан збереження інформаційних ресурсів держави і захищеності законних прав особистості і суспільства в інформаційній сфері; це стан захищеності національних інтересів в інформаційній сфері, що визначаються сукупністю збалансованих інтересів особистості, суспільства і держави;

- це властивістьінформації, що характеризуються конфіденційністю, цілісністю і доступністю; це властивість середовища забезпечувати захист інформації; це властивість середовища передавати, накопичувати, обробляти, зберігати інформацію, що характеризує її ступінь захищеності від дестабілізуючого впливу зовнішнього середовища і внутрішніх загроз, тобто її конфіденційність, цілісність і стійкість до руйнуючих, що імітує і викривляє впливів і перешкод;

- це захищеність пристроїв, процесів, програм, середовища і даних, що забезпечує цілісність інформації, яка обробляється, зберігатися і продукується цими засобами; це захист інформації, яку має суб’єкт (виробляє, передає або отримує) від несанкціонованого доступу, руйнування,

модифікації, розкриття і затримок при вступі. Інформаційна безпека включає в себе заходи по захисту процесів створення даних, їх введення, обробки і виведення; це захищеність інформації і підтримуючої інфраструктури від випадкових або навмисних впливів природного або штучного характеру, що можуть призвести нанесення шкоди власникам або користувачам інформації і підтримуючої інфраструктури; це захищеність інформації від випадкового або навмисного доступу осіб, які не мають на це право; це захищеність інформації та інформаційних систем від несанкціонованого доступу або модифікації інформації, яка зберігається, обробляється, або передається, а також від відмови в обслуговуванні авторизованих користувачів; це захищеність конфіденційності, цілісності, доступності, автентичності, підзвітності, неспростовності і надійності інформації;

- це відсутність неприпустимого ризику, пов'язаного з витоком інформації технічними каналами, несанкціонованими і ненавмисними діями на дані і (або) на інші ресурси автоматизованої інформаційної системи, що використовуються в автоматизованій системі;

- це неможливістьнанесення шкоди властивостям об'єкта безпеки обумовлених інформацією та інформаційною інфраструктурою;

- це збереженняконфіденційності, цілісності та доступності інформації.

Наведемо власну інтерпретацію «інформаційної безпеки» в рамках об'єкта дослідження: інформаційна безпека закладу охорони здоров’я - це такий стан інформаційного середовища, яке дозволяє зберегти властивості інформації і інформаційних потоків, забезпечує цілісність, виключає ризики і запобігає витоку інформації з медичної установи.

Аналіз наукової літератури засвідчує, що питання управління інформаційною безпекою недостатньо досліджені. В.А. Ліпкан, Ю.Є. Максименко, В.М. Желіховський розглядають систему управління інформаційною безпекою як систему інформаційно-аналітичних, теоретико-методологічних, адміністративно-правових, організаційно-управлінських, спеціальних та інших заходів, спрямованих на забезпечення стійкого

розвитку об’єктів інформаційної безпеки, а також інфраструктури її забезпечення [39, с. 158]. Як бачимо, автори у громіздкому визначенні поєднують суб’єктивний та нормативний підходи, не вказавши елементів системи.

Інший підхід демонструє А.А. Стрельцов і до системи управління інформаційною безпекою включає такі елементи: суб’єкти інформаційних процесів, інформація, призначена для використання суб’єктами інформаційного суспільства, інформаційна інфраструктура, суспільні відносини, які складаються у зв’язку зі створенням, зберіганням, передачею та розповсюдженням інформації [67, с. 15-21]. Але вчений, на наш погляд, розглядає механізм забезпечення інформаційної безпеки, а не її систему управління. Очевидним є те, що система забезпечення інформаційної безпеки є сукупністю окремих елементів, якими, зазвичай, є об’єкт, суб’єкти та види. У той же час окремими її складовими є основні характеристики, рівні інформаційної безпеки та перелік загроз.

Таким чином, система управління інформаційною безпекою – це внутрішня структура, систематизована сукупність, єдність, взаємозв’язок і диференціація окремих її елементів (об’єкт, суб’єкти, основні характеристики, рівні інформаційної безпеки та перелік загроз) [15, с.47].

Однією з основних умов ефективного функціонування системи управління інформаційною безпекою закладу охорони здоров’я є залучення керівництва в процес управління інформаційною безпекою. Всі співробітники повинні розуміти, що, по-перше, вся діяльність по забезпеченню інформаційною безпекою ініційована керівництвом і обов'язкова для виконання, по-друге, керівництво особисто контролює функціонування системи управління інформаційною безпекою, по-третє, саме керівництво виконує ті ж правила по забезпеченню інформаційною безпекою, що і всі співробітники медичного закладу.

Отже, управління інформаційною безпекою закладу охорони здоров’я – це циклічний процес, що включає усвідомлення ступеня необхідності захисту

інформації та постановку завдань; збір та аналіз даних про стан інформаційної безпеки в організації; оцінку інформаційних ризиків; планування заходів по обробці ризиків; реалізацію та впровадження відповідних механізмів контролю, розподіл ролей і відповідальності, навчання і мотивацію персоналу, оперативну роботу по здійсненню захисних заходів; моніторинг функціонування механізмів контролю, оцінку їх ефективності та відповідні коригувальні дії. Завдання забезпечення інформаційної безпеки необхідно вирішувати системно. Це означає, що засоби захисту інформації повинні застосовуватися одночасно і під централізованим управлінням. При цьому компоненти системи повинні «знати» про існування один одного, взаємодіяти і забезпечувати захист від зовнішніх і від внутрішніх загроз.

1.2. Методи забезпечення інформаційної безпеки закладу охорони здоров'я

У сучасному суспільстві інформація є дуже цінним ресурсом в будь-якій діяльності людини. Тому кожна організація зацікавлена в своїй інформаційній безпеці. Інформаційною безпекою називають заходи щодо захисту інформації від несанкціонованого доступу, руйнування, модифікації, розкриття і затримок у доступі. Метою інформаційної безпеки є захист цінності системи, збереження і гарантування точності і цілісності інформації, а також мінімізація її руйнування, якщо інформація буде модифікована або зруйнована. Інформаційна безпека вимагає врахування всіх подій, в ході яких інформація створюється, модифікується, поширюється або, коли до неї забезпечується доступ. Забезпечення інформаційної безпеки організації здійснюються на практиці з використанням різних механізмів захисту, для створення яких застосовують такі засоби [14; 40]:

- фізичні;

- апаратні;
- програмні;
- апаратно-програмні (технічні);
- криптографічні;
- адміністративні (організаційні);
- законодавчі (правові);
- морально-етичні.

Розглянемо їх більш детально. Так, фізичні засоби захисту - це різного роду механічні, електронно-механічні пристрої, спеціально призначені для утворення фізичних перешкод на можливих шляхах проникнення і доступу можливих порушників до компонентів автоматичної системи, а також технічні засоби візуального спостереження, зв'язку та охоронної сигналізації. Фізична безпека пов'язана з введенням заходів захисту, які захищають від стихійних лих, наприклад, таких як пожежа, повінь, ураган, землетрус.

Апаратні засоби захисту – церізні електронні, електромеханічні пристрої, прямо вбудовані в блоки автоматизованої інформаційної системи або оформлені у вигляді автономних пристроїв і поєднуються з цими блоками.Їх завдання: внутрішній захист структурних елементів засобів і систем обчислювальної техніки, наприклад, процесорів, терміналів, периферійного обладнання. Реалізується це за допомогою методу управління доступом (ідентифікація, аутентифікація і перевірка повноважень суб'єктів системи, реєстрація, реагування) [6].

Програмні засоби захисту використовуються для виконання логічних і інтелектуальних функцій захисту. Вони включаються або до складу програмного забезпечення автоматизованої інформаційної системи, або до складу засобів, комплексів і систем апаратури контролю. Програмні засоби захисту є найбільш поширеним видом захисту, оскільки вони універсальні, прості у використанні, є можливістю зміни і розвитку. Дана обставина робить їх і найуразливішими елементами захисту інформаційної системи організації. В даний час створена велика кількість операційних систем, систем

управління базами даних, мережевих пакетів і пакетів прикладних програм, що включають різноманітні засоби захисту інформації [55].

Для розв'язання задачі оцінки ризиків інформаційної безпеки в даний час найбільш часто використовуються наступні програмні комплекси: CRAMM, FRAP, RiskWatch, Microsoft SecurityAssessmentTool (MSAT), ГРИФ, CORAS і ряд інших. Всі відомі методики можна розділити на:

- методики, що використовують оцінку ризику на якісному рівні (наприклад, за шкалою «високий», «середній», «низький»), до таких методик, зокрема, відноситься FRAP;
- кількісні методики (ризик оцінюється через числове значення, наприклад, розмір очікуваних річних втрат), до цього класу належить методика RiskWatch;
- методики, що використовують змішані оцінки (такий підхід використовується в CRAMM, методиці MSAT) [61; 29].

До прийняття рішення про впровадження тієї чи іншої методики управління інформаційною безпекою слід переконатися, що вона досить повно враховує потреби закладу охорони здоров’я, його масштаби, а також відповідає кращим світовим практикам і має досить докладний опис процесів і необхідних дій.

У таблиці 1.2 представлений порівняльний аналіз найбільш популярних в даний час методик (CRAMM, ГРИФ, RiskWatch, CORAS, MSAT).

Таблиця 1.2. Порівняння програмного інструментарію для управління ризиками інформаційної безпеки

Критеріїпорівняння	GRAMM	ГРИФ	RiskWatch	CORAS	MSAT
1	2	3	4	5	6
Ризики					
Використання категорій ризиків	+	+	+	+	+
Використання поняття максимально допустимого ризику	+	+	+	+	+
Підготовка плану заходів щодо зниження ризиків	+	+	+	-	+
Управління					
Інформування керівника	+	+	+	+	+
План робіт по зниженню ризиків	-	+	+	-	+
Включає проведення тренінгів, семінарів, зборів	-	+	+	-	+

Оцінка бізнес-ризиків / операційних ризиків / IT-ризиків	-	+	+	+	-
Оцінка ризиків на організаційному рівні	+	+	-	+	+
Оцінка ризиків на технічному рівні	+	+	+	+	+

Продовження табл. 1.2

1	2	3	4	5	6
Пропонованіспособизниженняризиків					
Обхід (виключення) ризику	-	+	+	-	-
Зниження ризику	+	+	+	+	+
Прийняття ризику	-	+	-	+	+
Процеси					
Використанняелементівризику					
Матеріальні активи	+	+	+	+	+
Нематеріальні активи	+	+	+	+	+
Загрози	+	+	+	+	+
Цінність активів	+	+	+	+	+
Уразливість	+	+	+	+	+
Заходи безпеки	+	+	+	-	+
Потенційний збиток	+	+	+	+	+
Імовірність реалізації загроз	+	+	+	+	+
Типи ризиків, якіаналізуються					
Бізнес-ризики	-	+	+	+	-
Ризики, пов'язані з порушенням законодавчих актів	-	+	-	-	+
Ризики, пов'язані з використанням технологій	-	+	-	+	+
Комерційні ризики	+	+	+	+	+
Ризики, пов'язані з залученням третіх осіб	+	+	+	+	+
Ризики, пов'язані з залученням персоналу	+	+	-	+	+
Повторні оцінки ризиків	-	+	+	-	+
Визначення правил прийняття ризиків	-	+	-	-	+
Способивизначеннявеличиниризику					
Якісна оцінка	+	+	+	+	+
Кількісна оцінка	-	+	+	-	-
Способиуправління					
Якісне ранжування ризиків	+	+	+	+	+
Кількісне ранжирування ризиків	-	+	+	-	-
Використання незалежної оцінки	-	+	-	+	+
Розрахунок повернення інвестицій	-	+	-	-	-
Розрахунок оптимального балансу міжрізними типами заходівбезпеки, такими як:					
Заходи запобігання	-	+	+	-	+
Заходи виявлення	-	+	+	-	+
Заходи щодо виправлення	-	+	+	-	+
Заходи по відновленню	-	+	+	-	+
Інтеграція способів управління	-	+	-	-	-
Опис призначення способів управління	-	+	+	+	+
Процедура прийняття остаточних ризиків	+	+	-	-	+
Управління залишковими ризиками	-	+	-	-	+
Моніторингризиків					
Застосування моніторингу ефективності заходів ІБ	-	+	+	-	-
Проведення заходів щодо зниження ризиків	-	+	+	-	+
Використання процесу реагування на інциденти в області ІБ	-	+	-	-	+
Структуроване документування результатів оцінок ризиків	-	+	+	-	+

Примітка. Систематизовано на основі джерела [5; 36]

У тих випадках, коли потрібно виконати тільки разову оцінку рівня ризиків в організації середнього розміру, доцільно рекомендувати використання методики CORAS. Для управління ризиками на базі

періодичних оцінок на технічному рівні найкраще підходить CRAMM. Методики Microsoft SecurityAssessmentTool і RiskWatch кращі для використання у великих організаціях, де планується впровадження управління ризиками ІБ на базі регулярних оцінок, на рівні не нижче організаційного і потрібна розробка обґрунтованого плану заходів щодо їх зниження [75, с.49].

Апаратно-програмні засоби захисту являють собою різні електронні пристрої і спеціальні програми, що входять до складу автоматичної системи організації і виконують самостійно або в комплексі з іншими засобами, функції захисту (ідентифікацію та аутентифікацію користувачів, розмежування доступу до ресурсів, реєстрацію подій, криптографічне закриття інформації) [78].

Криптографічний метод захисту інформації заснований на принципі її шифрування. Криптографічний метод може бути здійснений як програмними, так і апаратними засобами. Засіб криптографічного захисту інформації здійснює криптографічне перебудову інформації для забезпечення її безпеки. Криптографічний захист або криптографічне перетворення інформації, шифрування є одним з важливих способів захисту інформації [35].

Адміністративний спосіб захисту є методом організаційного характеру, який регламентує процеси функціонування системи обробки даних, застосування її ресурсів, діяльність обслуговуючого персоналу, а також порядок взаємодії користувачів з системою так, щоб максимальноускладнити чи унеможливити реалізації загроз безпеці або мінімізувати розмір втрат у разі їх здійснення. Головна мета адміністративних заходів сформувати політику в галузі забезпечення безпеки інформації та забезпечити її виконання, шляхом визначення необхідних ресурсів і контролю їхнього стану [1].

До правових заходів захисту відносяться закони, укази та нормативні акти, які регламентують правила поводження з інформацією, що

закріплюють права і обов'язки учасників інформаційних відносин у процесі її обробки і використання, а також встановлюють відповідальність за порушення цих правил, перешкоджаючи тим самим неправомірному використанню інформації і є стримуючим фактором для потенційних порушників. Правові засоби захисту носять в основному попереджувальний, профілактичний характер і вимагають постійної роз'яснювальної роботи з користувачами і обслуговуючим персоналом системи [38, с.57].

До морально-етичних засобів відносяться норми поведінки та правила поведінки з інформацією,які традиційно склалися або складаються в міру поширення електронно-обчислювальних машин в суспільстві, країні [52]. Ці норми здебільшого не є обов'язковими, як законодавчо затверджені нормативні акти. Однак, їх недотримання веде зазвичай до падіння авторитету, престижу людини, групи осіб або організації. Морально-етичні норми бувають як неписані, наприклад, загальновизнані норми, так і писані, тобто оформлені в певний статут правил. Морально-етичні засоби захисту є профілактичними і вимагають постійної роботи зі створення здорового морального клімату в колективах підрозділів.

Отже, на даному етапі загальносвітового розвитку, роль інформаційного середовища дуже велика. Інформація є системоутворюючим фактором у всіх етапах життя суспільства, вона все більш активно впливає на стан політичної, економічної, оборонної, особистої, майнової та інших складових безпеки. Тому незважаючи на те, що побудова ефективної системи інформаційної безпеки є складним і безперервним процесом, цьомунеобхідно приділяти значну увагу, а саме, оперувати даними методами які забезпечать інформаційну безпеку.

РОЗДІЛ 2
СУЧАСНИЙ СТАН УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ КОМУНАЛЬНОГО ПІДПРИЄМСТВА «ХМЕЛЬНИЦЬКИЙ МІСЬКА ДИТЯЧА ЛІКАРНЯ»

2.1. Аналіз організаційного забезпечення управління інформаційною безпекою закладу охорони здоров'я

Комунальне підприємство «Хмельницька міська дитяча лікарня» Хмельницької міської ради (далі – КП «Хмельницька міська дитяча лікарня») є закладом охорони здоров'я - комунальним унітарним некомерційним підприємством, що надає амбулаторно-поліклінічну та стаціонарну медичну допомогу дитячому населенню в порядку та на умовах, встановлених законодавством України та Статутом, а також вживає заходів із профілактики захворювань дитячого населення та підтримання громадського здоров'я.

КП «Хмельницька міська дитяча лікарня» створене за рішенням Хмельницької міської ради шляхом перетворення Хмельницької міської дитячої лікарні в комунальне підприємство «Хмельницька міська дитяча лікарня» Хмельницької міської ради. КП «Хмельницька міська дитяча лікарня» є правонаступником усього майна, всіх прав та обов'язків Хмельницької міської дитячої лікарні [62].

КП «Хмельницька міська дитяча лікарня» створене з метою реалізації державної політики в сфері охорони здоров'я, інтеграції та ефективного використання ресурсів для досягнення найкращих кінцевих результатів в наданні доступної амбулаторно-поліклінічної, спеціалізованої (вторинної), високоспеціалізованої (третинної) стаціонарної медичної допомоги дитячому населенню міста Хмельницького, але не обмежуючись вказаним населеним пунктом, а також вжиття заходів з профілактики захворювань дитячого населення та підтримки громадського здоров'я.

Відповідно до поставленої мети предметом діяльності КП «Хмельницька міська дитяча лікарня» є:

– здійснення оперативного управління, організаційно-методичного керівництва роботи структурних підрозділів підприємства;

– консультативно-діагностичні послуги;

– стаціонарне лікування хворих;

– експертиза і контроль якості медичної допомоги;

– реабілітація хворих;

– надання невідкладної медичної допомоги хворим на інфекційні захворювання;

– своєчасне та кваліфіковане надання медичної допомоги дитячому населенню віком від 0 місяця до 17 років 11 місяців 29 днів, у стаціонарних та амбулаторних відділеннях підприємства;

– взаємодія з іншими закладами охорони здоров'я з метою забезпечення наступництва у наданні медичної допомоги на різних рівнях та ефективного використання ресурсів системи медичного обслуговування [62].

Для здійснення господарської некомерційної діяльності КП «Хмельницька міська дитяча лікарня» залучає і використовує матеріально-технічні, фінансові, трудові та інші види ресурсів, використання яких не заборонено законодавством. КП «Хмельницька міська дитяча лікарня» має самостійний баланс, рахунки в установах банків, органах Державного казначейства України, круглу печатку із своїм найменуванням, штампи, а також бланки з власними реквізитами.

КП «Хмельницька міська дитяча лікарня» надає медичні послуги на підставі ліцензії на медичну практику. Забороняється розподіл отриманих доходів (прибутків) КП «Хмельницька міська дитяча лікарня» або їх частини між Засновником та працівниками (крім оплати їхньої праці, нарахування єдиного соціального внеску) та інших пов'язаних з ним осіб. Доходи (прибутки) КП «Хмельницька міська дитяча лікарня» використовуються

виключно для фінансування видатків на його утримання, реалізації мети, цілей та завдань і напрямків діяльності, визначених Статутом.

Управління КП «Хмельницька міська дитяча лікарня» здійснюється відповідно до Статуту на основі поєднання прав Засновника, Уповноваженого органу управління та керівника підприємства, щодо господарського використання комунального майна і участі в управлінні трудового колективу. Поточне керівництво КП «Хмельницька міська дитяча лікарня» здійснює керівник – Директор, який призначається на посаду відповідно до чинного законодавства України.Структура КП «Хмельницька міська дитяча лікарня» відображено на рис. 2.1.

Фінансовий план та план використання бюджетних коштів КП «Хмельницька міська дитяча лікарня» затверджуються Уповноваженим органом управління. КП «Хмельницька міська дитяча лікарня» має право здавати в оренду майно в порядку визначеному Засновником. Списання з балансу основних фондів підприємства можуть проводитися в порядку, визначеному Засновником за згодою Уповноваженого органу управління.

Сьогодні в складі лікарні працює стаціонар на 380 ліжок та поліклініка на 920 тис. відвідувань за рік. Щороку в ХМДЛ лікується понад 11 тис. дітей, проводиться понад 6 тис. оперативних втручань. Поліклініка обслуговує 47200 дітей від 0 до 18 років. Лікарський склад лікарні нараховує 219 лікарів, з них 4 кандидата медичних наук, 57 лікарів вищої, 87 – першої та 26 другої категорій.

Під наглядом поліклініки знаходиться біля 50 тисяч дітей. В поліклініці створено 7 педіатричних відділень дільничних педіатрів, які ведуть прийоми дітей на 5 філіях у всіх районах міста. Амбулаторний прийом проводять лікарі з 24 медичних спеціальностей. Лікарі 3 педіатричних відділень для дітей дошкільно-шкільного віку та підліткового відділення надають медичну допомогу та проводять велику профілактичну роботу у всіх навчальних закладах міста.

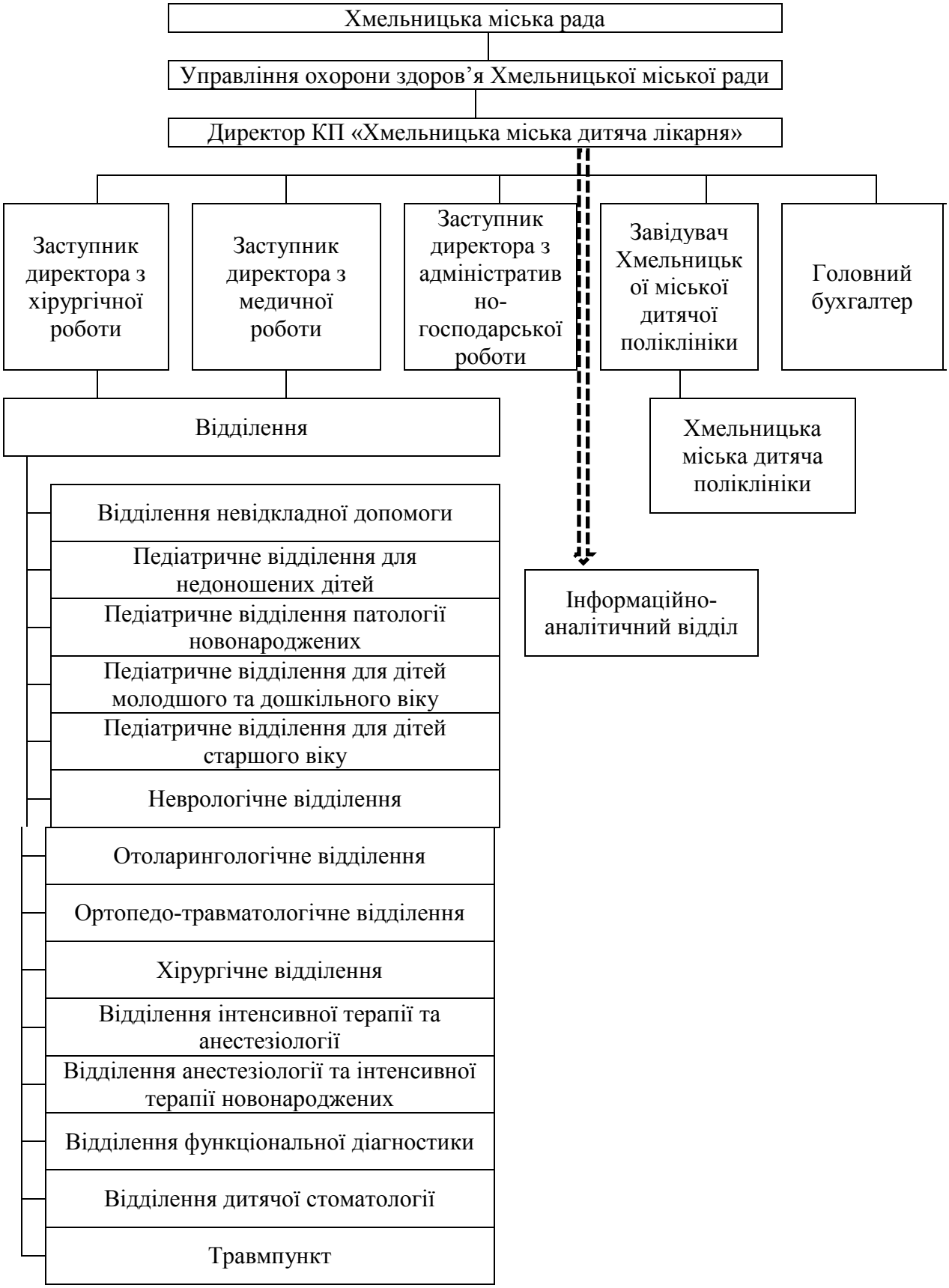

Рисунок 1.1 – Організаційна структура КП «Хмельницька міська дитяча лікарня»

Примітка. Складено автором на основі [62; 81].

Для лікування дітей в амбулаторних умовах працює денний стаціонар, функціонує відділення фізіотерапевтичного лікування, кабінети лікувальної фізкультури, масажу, рефлексотерапії. В кабінеті охорони зору та сурдологічному кабінеті діти мають можливість повного комплексу дослідження зорового та слухового аналізаторів. Відкрито вперше в області реабілітаційний центр “Турбота” для дітей з особливими потребами, в якому проводиться медико-соціальна реабілітація.

Спеціалізована стаціонарна медична допомога дітям у Хмельницькій міській дитячій лікарні надається у 10 відділеннях лікарні, в яких розташовано 380 ліжок. Крім того функціонують відділення анестезіології та інтенсивної терапії на 6 ліжок та відділення анестезіології та інтенсивної терапії для новонароджених на 9 ліжок. Хмельницька міська дитяча лікарня надає допомогу дітям не лише міста, але й всієї Хмельницької області. 8 відділень лікарні із 10 працюють як відділення обласного значення. Заклад надає допомогу хворим новонародженим дітям всього регіону [62].

Інформаційна безпека є комплексом заходів та засобів щодо забезпечення збереження інформації, що знаходиться в системі інформаційного забезпечення діяльності органу медичного закладу, переданої, оброблюваної, а також тієї, що зберігається та надається системою. Призначення системи інформаційної безпеки КП «Хмельницька міська дитяча лікарня» полягає в організації безпечних і надійних: заходів з доступу до інформації, способів передачі та зберігання інформації, методів обробки інформації, правил управління доступом до інформації, способів відновлення інформації, методів резервування інформації тощо.

Завдання системи інформаційної безпеки КП «Хмельницька міська дитяча лікарня» обумовлюються її призначенням і полягають у:

– забезпеченні безпечного, надійного зберігання і передачі інформації в електронному та друкованому вигляді, розташованої на різних носіях;

– організації надійного доступу до інформації;

– обмеження і контроль доступу до інформації, з якою працюють співробітники, зокрема забезпечення збереження персональних даних пацієнтів;

– створенні правил безпечної роботи з інформацією;

– проведенні заходів щодо резервування інформації;

– забезпеченні відновлення інформації в аварійних ситуаціях;

– підтримці інформаційної безпеки на заданому рівні.

В нинішній час для забезпечення належного стану інформаційної безпеки потрібна не просто розробка окремих механізмів захисту, а реалізація системного підходу, що включає комплекс взаємопов'язаних заходів (використання спеціальних технічних і програмних засобів, організаційних заходів, нормативно-правових актів і т.д.). Головною метою будь-якої системи забезпечення інформаційної безпеки є створення умов функціонування медичного закладу, запобігання загроз його безпеки, захист законних інтересів установи від протиправних посягань, недопущення розкрадання, розголошення, втрати, витоку, спотворення і знищення службової інформації, забезпечення в рамках діяльності всіх підрозділів організації.

Інформаційна безпека органу охорони здоров’я відображає захищеність інформаційного середовища та ефективність інформаційного забезпечення процесу управління в установі [7; 27; 57].

Процес забезпечення інформаційної безпеки закладу охорони здоров’я можна представити як взаємодію трьох підсистем:

підсистема інформаційного забезпечення процесу управління;

підсистема захисту інформаційного середовища;

підсистема діагностики рівня інформаційної безпеки.

Ключовими задачами підсистеми інформаційного забезпечення процесу управління закладу охорони здоров’я є: збирання необхідної інформації; обробка і систематизація інформації; оцінка й аналіз інформації;

прогнозування всіх аспектів діяльності; надання необхідної інформації особам, що приймають рішення.

Безперервне виконання всіх цих задач необхідне для ефективного функціонування зазначеної підсистеми. Захист інформаційного середовища установи включає захист від зловмисних дій, так і власних співробітників, а також захист від незловмисних внутрішніх негативних впливів.

Для забезпечення захисту інформаційного середовища КП «Хмельницька міська дитяча лікарня» необхідне систематичне виконання наступних етапів (рис. 2.2.):

Рисунок 2.2 - Схема функціонування системи інформаційної безпеки КП «Хмельницька міська дитяча лікарня»

Примітка. Складено автором.

- аналіз загроз інформаційній безпеці;
- планування та розробка заходів щодо забезпечення інформаційної безпеки;
- оперативна реалізація запланованих дій.

Функції щодо управління інформаційною безпекою КП «Хмельницька міська дитяча лікарня» розподілено між директором, його заступниками та

інформаційно-аналітичним відділом медичного закладу, керівниками лінійних та інших функціональних підрозділів. Проведемо аналіз фактично виконуваних функцій з управління інформаційною безпекою закладу охорони здоров'я шляхом аналізу потреби і фактично виконуваних функцій (таблиця 2.1)

Таблиця 2.1. Аналіз розподілу функціональних повноважень щодо управління інформаційною безпекою КП «Хмельницька міська дитяча лікарня»

№ з/п	Функції	Структурні підрозділи					Ступінь реалізації функцій (фактичне/ необхідне)
		Директор	Головний лікар	Інформаційно-аналітичний відділ	Лінійні керівники	Керівники інших функціональних підрозділів	
1.	Виявлення та аналіз ризиківінформаційної безпеки медичного закладу	+	-	+	-	-	2/4
2.	Планування та практична реалізація процесів, спрямованих на мінімізацію ризиків ІБ медичного закладу	-	-	-	-	-	0/2
3.	Контроль реалізації процесів, спрямованих на мінімізацію ризиків ІБ медичного закладу	-	-	-	-	-	0/3
4.	Внесення в процеси мінімізації інформаційних ризиків медичного закладу необхідних коригувань	-	-	-	-	-	0/1
5.	Забезпечення цілісності, конфіденційності та доступності критичних інформаційних ресурсів медичного закладу	-	-	+	+	+	3/3
6.	Аудит інформаційних ресурсів та послуг медичного закладу	-	-	-	-	-	0/1
7.	Захист права на інтелектуальну власність медичного закладу	+	+	+	-	-	2/5
	Разом	2/4	1/2	3/7	1/3	1/3	8/19

- необхідне виконання

«+/-» - фактичне виконання

Примітка. Складено автором на основі власних спостережень

Таким чином, проведений аналіз свідчить, що у КП «Хмельницька міська дитяча лікарня» виконується лише 8 із 19 необхідних функцій. Найбільший ступінь недовиконання спостерігається саме по інформаційно-аналітичному відділу лише 3 з 7 необхідних. Крім того, слід відзначити відсутність заходів з планування, контролю та перегляду ризикозахищеності медичного закладу. Тобто в медичний установі функціонує система забезпечення інформаційної безпеки, яка не орієнтована на превентивну діяльність, а є за своїм характером реактивною, тобто реагує на ті загрози, які вже фактично виникли.

Опишемо більш детально функціональні повноваження інформаційно-аналітичного відділу КП «Хмельницька міська дитяча лікарня». Так у розділі 5 Стандарти акредитації закладів охорони здоров’я, затверджених наказом Міністерства охорони здоров’я України «Про вдосконалення акредитації закладів охорони здоров’я» від 14.03.2011 № 142 визначена вимога щодо наявності у закладі інформаційно-аналітичного відділу. Інформаційно-аналітичний відділ КП «Хмельницька міська дитяча лікарня» здійснює реалізацію державної політики в службі медичної статистики та інформатизації галузі охорони здоров'я. Відділ очолює завідувач, який призначається та звільняється з посади директором КП «Хмельницька міська дитяча лікарня» за погодженням з начальником інформаційно-аналітичного центру медичної статистики Управління охорони здоров'я Хмельницької міської ради.Відділ підпорядкований директору, в організаційно-методичному плані інформаційно-аналітичному центру медичної статистики Управління охорони здоров'я Хмельницької міської ради.

Мета діяльності відділу

- реалізація державної політики з питань медичної статистики.
- інформаційно-аналітичне забезпечення управління охороною здоров'я.

- впровадження інноваційних технологій в систему охорони здоров'я.

Завданнями відділу інформаційно-аналітичного забезпечення у сфері забезпечення інформаційної безпеки є:

- формування єдиної системи ведення, збору, обробки, зберігання та передачі медико-статистичної інформації в закладі охорони здоров'я.

- збір медико-статистичної та адміністративної інформації від підрозділів лікарні, обробка та аналіз інформації, щодо стану здоров'я населення, обсягів та якості надання медичної допомоги, ресурсів охорони здоров'я та їх використання.

- підтримка інформаційного банку даних щодо стану здоров'я населення, ресурсного забезпечення та діяльності закладу охорони здоров'я.

- надання консультативної та організаційно-методичної допомоги закладу охорони здоров'я та запровадження автоматизованого статистичного обліку.

Функції відділу інформаційно-аналітичного забезпечення у сфері забезпечення інформаційної безпеки:

1. Забезпечує впровадження уніфікованої системи збору, обробки та надання медико-статистичної та адміністративної інформації.

2. Здійснює впровадження сучасних інформаційних технологій (сертифікованих програмних продуктів, комп'ютерної техніки, засобів зв'язку) для автоматизації системи управління, обліку, збору, обробки та аналізу статистичної інформації.

3. Здійснює заходи щодо оптимізації діяльності інформаційно-аналітичної служби, надає методичну допомогу з питань організації статистичного обліку і звітності.

4. Здійснює контроль за впровадженням і використанням у закладі охорони здоров'я форм державної та галузевої статистичної звітності у т. ч. форм суворої статистичної звітності.

5. Проводить у закладі охорони здоров'я та його структурних підрозділах перевірку стану медико-статистичного обліку, достовірності звітних даних.

6. Формує банк даних щодо стану здоров'я населення, діяльності та ресурсного забезпечення закладу охорони здоров'я.

7. Проводить підготовчі заходи щодо акредитації КП «Хмельницька міська дитяча лікарня».

8. Бере участь у виконанні окремих завдань, за планом КП «Хмельницька міська дитяча лікарня» та територіального інформаційно-аналітичного центру медичної статистики.

Одним із завдань інформаційно-аналітичного відділу КП «Хмельницька міська дитяча лікарня», є дотримання єдиної системи ведення, збирання, оброблення, зберігання та передавання медико-статистичної інформації у закладах охорони здоров’я, централізоване збирання медико-статистичної та адміністративної інформації від підрозділів, оброблення та аналіз інформації щодо стану здоров’я населення, обсягів та якості надання медичної допомоги, ресурсів закладу охорони здоров’я та їх використання, участь у формуванні єдиного медичного інформаційного простору.

Крім того в діяльності інформаційно-аналітичного відділу КП «Хмельницька міська дитяча лікарня»передбачено такі регламентувальні документи: перелік нормативно-правових актів щодо обліку та звітності у закладах охорони здоров’я; графік надання звітної інформації підрозділами та службами до інформаційно-аналітичного відділу. У цьому графіку визначають відповідальних за збирання та звіряння інформації з первинною документацією осіб, а також строки подання інформації, осіб, яким надається інформація, споживачів та особу, що аналізує інформацію; схему взаємодії інформаційно-аналітичного відділу з трирівневим джерелом інформації; схему інформаційного медичного статистичного забезпечення закладу; схему руху директивної інформації.

Слід зауважити, що використання сучасних сертифікованих програмних продуктів типу «Поліклініка» та «Стаціонар» у КП «Хмельницька міська дитяча лікарня» значно зменшує кількість помилок при веденні первинної медичної документації, підвищує достовірність отриманої інформації та економить робочий час працівників.

У КП «Хмельницька міська дитяча лікарня» затверджений перелік документів, що містять конфіденційну інформацію (таблиця 2.2). Його наявність має принциповий характер, тому що неможливо вимагати від працівників нерозголошення абстрактної конфіденційної інформації, як іноді вказують у зобов'язальних документах: «зберігати ноу-хау, ділові секрети, службові відомості». Захищається тільки документована інформація, а тому, необхідно якомога конкретніше описати всі групи й види конфіденційної документації.

Таблиця 2.2. Перелік категорій відомостей, що складають конфіденційну інформацію КП «Хмельницька міська дитяча лікарня»

Відомості конфіденційної інформації	Особливості режиму конфіденційної інформації
1	2
1. Персональні данні:	
1.1. Персональні дані: національність, освіта, сімейний стан, релігійні переконання, стан здоров'я, дата і місце народження, адреси місць проживання, номери телефонів, анкетні та автобіографічні дані.	Строк дії – безстроково. Для документа - до передавання його до державної архівної установи.
2. Відомості про пацієнтів.	
2.1. Відомості, що розкривають дані про пацієнтів (аналізи, діагноз, стан перебігу хвороби)	Строк дії – безстроково. Для документа - до передавання його до державної архівної установи.
3 Економіка і фінанси.	Строк дії – безстроково. Для документа - до передавання його до державної архівної установи.
3.1. Відомості, що розкривають наявність коштів на рахунках медичного закладу	
3.2. Відомості, що розкривають розмір і структуру фонду оплати праці	
4. Безпека.	
4.1. Відомості про особу яка сповістила про	Строк дії – безстроково.

скоєння корупційного правопорушення або дії в умовах конфлікту інтересів.	Для документа - до передавання його до державної архівної установи. Гриф "Конфіденційно".

Продовження табл. 2.2

1	2
4.2. Відомості про скоєння корупційного правопорушення або дії в умовах конфлікту інтересів.	Строк дії – до завершення службового розслідування. Гриф "Конфіденційно".
4.3. Індивідуальні паролі доступу співробітників до корпоративної комп'ютерної мережі та баз даних Товариства.	Строк дії - 1 рік.
4.4. Відомості про методику, перелік, назву, розташування і характеристики технічних засобів, у тому числі програмно-апаратних, які застосовані для захисту інформації.	Строк дії – безстроково. Для документа - до передавання його до державної архівної установи. Гриф "Конфіденційно".
4.5. Інформація, що надійшла на телефон довіри.	Строк дії - до прийняття щодо неї рішення відповідальною особою.

Примітка. Складено автором за даними КП «Хмельницька міська дитяча лікарня».

Облік документів та видань з грифом «Конфіденційно» ведеться у журналах за формою 52 окремо від обліку іншої неконфіденційної документації. За основу для встановлення контролю над доступом до інформації медичної установи береться класифікація інформації за рівнем конфіденційності, залежно від змісту й можливих наслідків у разі втрати інформації або зловживань.

За категоріями конфіденційності основні види інформації розподіляються так. Найнижчий гриф конфіденційності «ДСК» ставиться на телефонні довідники, де є окремі дані про кадровий склад. Цей гриф також ставиться на журнали реєстрації, документи, що регламентують діяльність, службове листування (заяви, розпорядження, накази, доповідні й т. д.).

До категорії документів із грифом «Конфіденційно» належать ті, де міститься інформація про розгорнуті відомості про персонал медичного закладу; про поточну фінансову діяльність; дані про пацієнтів, які не надаються третім особам; дані щодо заробітної плати персоналу.

Гриф «суворо конфіденційно» присвоюється документам, що містять дані про особисту інформацію пацієнта (діагноз, аналізи, лікування тощо). Якщо цінність інформації з яких-небудь причин знижується, знижується й гриф документа. Окремої уваги заслуговує питання про терміни дії грифів конфіденційності. Строк таємності визначається автором документа, виконавцем, особою, що підписує або затверджує документ за узгодженням керівником служби інформаційної безпеки. Строк може вказуватися у вигляді періоду грифа, з дати закінчення грифа, настання певної події, на яку зорієнтований документ, або напису «безстроково». У деяких випадках рішення, щодо зняття грифа залишається за начальником служби інформаційної безпеки.

Допуск співробітникам КП «Хмельницька міська дитяча лікарня» до конфіденційної інформації та баз даних, що є власністю медичного закладу, надається директором на підставі мотивованої службової записки начальника інформаційно-аналітичного відділу.

Робота будь-якого закладу неможлива без наявності доступу до інтернету. Інженер-програміст, відповідальний за роботу з комп’ютерною технікою, періодично складає аналітичну довідку, у якій відображає: наявність договору з оператором електронного зв’язку про підключення закладу до інтернету; наявність поштової скриньки, персонального веб-ресурсу (сайту закладу); показники розвитку інформатизації закладу — кількість персональних комп’ютерів у закладі та кількість персональних комп’ютерів, під’єднаних до мережі інтернет. Крім того, у цій довідці вказують обсяг провадження інформаційно-телекомунікаційних технологій — участь персоналу закладу у телеконференціях, селекторних нарадах у форматі відеоконференцій, можливість проведення попереднього запису на

прийом до лікарів через мережу інтернет, наявність тематичного підрозділу для проведення лікарями закладу онлайн-консультування на власному вебресурсі тощо. У довідці вказують і наявність автоматизованих робочих місць лікаря та інші дані — у яких підрозділах закладу вони наявні, скільки лікарів мають змогу використовувати у роботі персональні комп'ютери, у тому числі під'єднані до мережі інтернет, із програмами для електронного ведення документації тощо. Реєстри, бази і банки даних, які ведуть у закладі теж вказують у довідці.

Отже, управління інформаційною безпекою медичного закладу здійснюється інформаційно-аналітичним відділом КП «Хмельницька міська дитяча лікарня», діяльність якого тісно пов'язана з іншими підрозділами. Від організації роботи інформаційно-аналітичного відділу, підбору фахівців, їхніх особистих якостей залежить якість лікувально-діагностичного процесу та наявність достовірної перевіреної інформації у адміністратора закладу.

2.2. Оцінювання рівня інформаційної безпеки медичного закладу

Діагностику рівня інформаційної безпеки КП «Хмельницька міська дитяча лікарня» пропонується проводити за трьома ключовими напрямками: оцінка програмно-технічної захищеності інформації; оцінка інформаційної надійності персоналу; оцінка інформації, що надається особам, що приймають рішення [87].

Для оцінки інформаційної надійності персоналу закладу охорони здоров'я пропонуємо розраховувати коефіцієнт правової захищеності інформації, коефіцієнт досвіду роботи персоналу, що забезпечує інформаційну безпеку установи, коефіцієнт надійності персоналу, що забезпечує інформаційну безпеку та коефіцієнт підготовленості персоналу до розпізнавання погроз [83; 88; 89].

Оцінку інформації, що надається особам, що приймають рішення, пропонуємо проводити за допомогою трьох показників: коефіцієнт повноти інформації, коефіцієнт точності інформації та коефіцієнт суперечливості інформації, які варто доповнити коефіцієнтом своєчасності надання інформації та коефіцієнтом надійності інформації.

Варто зазначити, що для отримання інформації, необхідної для розрахунку наведених показників, обов'язковою умовою є наявність системи моніторингу діяльності закладу охорони здоров'я [34, с.76].

Кількісний аналіз та моделювання є тими інструментальними засобами, які дають змогу оцінити, виокремити, нехай і наближено, суттєві ризики з несуттєвих (надуманих).Однак у більшості випадків одного лише якісного аналізу недостатньо для ідентифікації та виокремлення суттєвих чинників ризику й нехтування несуттєвими (надуманими). З цією метою необхідно здійснювати кількісний аналіз небезпеки. А це потребує здобуття відповідної інформації.

Методи експертних оцінки включають комплекс логічних і математико-статистичних методів і процедур, пов'язаних з діяльністю експерта по переробці необхідної для аналізу і прийняття рішень інформації. Центральною «фігурою» експертної процедури є сам експерт – цефахівець, який використовує свої здібності (знання, вміння, досвід, інтуїцію і т.п.) для знаходження найбільш ефективного рішення. Експерти, що залучаються для оцінки небезпеки, в тому числі і інформаційної, повинні: мати доступ до всієї наявної в розпорядженні розробника інформації; володіти достатнім рівнем креативності мислення та необхідними знаннями у відповідній предметній області; бути вільним від особистих переваг щодо проекту (не лобіювати його).

Можна виділити наступні основні методи експертних оцінок, що застосовуються для аналізу небезпеки: опитувальники; SWOT-аналіз; роза і спіраль ризиків; оцінка ризику стадії проекту; метод Дельфі.

Інформація може існувати в самих різних формах. Її можна друкувати або писати на папері, зберігати на електронних носіях, пересилати за традиційною або електронною поштою, показувати у фільмах або передавати в усній розмові. Яку б форму не приймала інформація і які б кошти не використовувалися для її передачі та зберігання, необхідно завжди забезпечувати відповідний рівень її захисту.

Інформаційна безпека досягається шляхом впровадження сукупності необхідних засобів захисту, до числа яких можуть входити політики, рекомендації, інструкції,організаційні структури і програмні функції. Ці засоби необхідно реалізувати для того, щоб гарантувати виконання вимог до безпеки в конкретній організації.

Система показників оцінки рівня інформаційної безпеки КП «Хмельницька міська дитяча лікарня» за кожним з запропонованих напрямків з розрахунковими формулами та граничні значеннями наведена в табл. 2.1.

Таблиця 2.1. Система показників оцінки рівня інформаційної безпеки КП «Хмельницька міська дитяча лікарня»

№ з/п	Назва показника	Алгоритм розрахунку	Граничне значення
1	2	3	4
1.	Оцінка програмно-технічної захищеності інформації		
1.1	Коефіцієнт технічного захисту інформації *Кт.з.*	*Кт.з. = ІАн.В.* де *ІАн.в.* – кількість не відвернутих інформаційних атак.	0
1.2	Коефіцієнт програмної захищеності інформації *Кп.з.*	*Кп.з. = Чб.ф./ Чб.ф.* де *Чб.ф.* – час безперебійного функціонування інформаційної системі, год. *Чн.ф.* – нормативний час функціонування інформаційної системи, год.	1
1.3	Коефіцієнт фінансового захисту інформації *Кф.з.*	*Кф.з. = Вз.ін. / Впр.ін.* де *Вз.ін.* – витрати на захист інформаційних ресурсів, грн.; *Впр.ін.* – витрати на придбання інформаційних ресурсів,грн.	0,15, зростання
1.4	Коефіцієнт фінансування інформаційної служби *Кфін.*	*Кфін. = Кфін./Вз* де *Вфін.* – витрати на фінансування інформаційної служби установи, грн.; *Вз*– загальні витрати установи.	0,5-0,15, зростання
2.	Оцінка інформаційної надійності персоналу		
2.1	Коефіцієнт правової захищеності	*Кпр.з.= І/Іюр.з* де *І*– обсяг інформації, розголошення якої може спричинити негативні наслідки для установи, %	1, зменшення

	інформації *Кпр.з.*	*Іюр.з.* – загальний обсяг юридично захищеної інформації, %	
2.2	Коефіцієнт досвіду роботи персоналу, що забезпечує інформаційну безпеку Кд.р.	*Кд.р. = ЧП1/ ЧПз* *де ЧП1*– чисельність працівників, які мають доступ до інформації для службового використання, що працюють в установі більше одного року, ос.; *ЧПз* – загальна чисельність працівників, що мають доступ до інформації для службового використання, ос.	1, зростання
2.3	Коефіцієнт надійності персоналу, що забезпечує інформаційну безпеку Кн.п.	*Кн.п. = (ЧПз.зв- ЧПвип)/ ЧПз.зв* *де ЧПвип* – чисельність працівників, звільнених за причиною витоку інформації, осіб; *ЧПз.зв.* – загальна чисельність звільнених працівників, осіб	1, зростання

Продовження табл. 2.1

1	2	3	4
2.4	Коефіцієнт підготовленості персоналу до розпізнавання погроз *Кпп*	*Кпп = (ЧПз- ЧПп)/ ЧПз* де *ЧПп* – чисельність працівників, ненавмисні дії яких призвели до витоку інформації завдяки низькому рівню підготовки персоналу до розпізнавання загроз безпеки, осіб; *ЧПз* – загальна чисельність працівників, що мають доступ до інформації для службового використання, осіб.	1, зростання
3.	Оцінка інформації, що надається особам, що приймають рішення (ОПР)		
3.1	Коефіцієнт повноти інформації *Кп.ін.*	*Кп.ін.= Ін/Інеоб.* де *Ін* – обсяг інформації, що є в розпорядженні ОПР, %; *Інеоб.*– обсяг інформації, необхідної для ухвалення обґрунтованого рішення, %	1, зменшення
3.2	Коефіцієнт точності інформації *Кт.ін.*	*Кт.ін.= Ір/ Ін* де *Ір* – обсяг релевантної інформації, % *Ін* – загальний обсяг наявної в розпорядженні ОПР інформації, %	1, зростання
3.3	Коефіцієнт суперечливості інформації *Кс.ін.*	*Кс.ін.= Іухв/Із* де *Іухв* – кількість незалежних свідчень на користь ухвалення рішення, %; *Із* – загальна кількість незалежних свідчень у сумарному обсязі релевантної інформації, %.	1, зростання
3.4	Коефіцієнт своєчасності надання інформації *Кс.н.ін.*	*Кс.н.ін.= Іс.н.*/Інеоб. де *Іс.н.*– обсяг своєчасно наданої ОПР інформації, %; *Інеоб.*– обсяг інформації, необхідної для ухвалення обґрунтованого рішення, %	1, зростання
3.5	Коефіцієнт надійності інформації *Кн.ін.*	Кн.ін.=*Ін.д./ Ін.д.* де *Ін.д.*– обсяг інформації, наданої ОПР з надійних джерел, %; *Із.н.*– загальний обсяг наданої ОПР інформації, %	1, зростання

Примітка. Складено автором

Проведемо фактичну оцінку рівня інформаційної безпеки КП «Хмельницька міська дитяча лікарня» на онові розрахунку коефіцієнтів, визначених в табл. 2.1 (табл. 2.2)

Таким чином, наведені в табл. 2.2 дані свідчать, що переважна більшість показників не відповідають граничному значенню. Зокрема, має місце «відставання» від норми всіх показників групи оцінки програмно-технічної захищеності інформації та оцінки інформації, що надається особам, що приймають рішення.

Таблиця 2.2. Система показників оцінки рівня інформаційної безпеки КП «Хмельницька міська дитяча лікарня»

№ з/п	Назва показника	Фактичне значення показника	Граничне значення
1	2	3	4
1.	Оцінка програмно-технічної захищеності інформації		
1.1	Коефіцієнт технічного захисту інформації *Кт.з.*	3	0
1.2	Коефіцієнт програмної захищеності інформації *Кп.з.*	0,87	1
1.3	Коефіцієнт фінансового захисту інформації *Кф.з.*	0,28	0,15, зростання
1.4	Коефіцієнт фінансування інформаційної служби *Кфін.*	0,12	0,15-0,5, зростання
2.	Оцінка інформаційної надійності персоналу		
2.1	Коефіцієнт правової захищеності інформації *Кпр.з.*	0,87	1, зменшення
2.2	Коефіцієнт досвіду роботи персоналу, що забезпечує інформаційну безпеку *Кд.р.*	0,95	1, зростання
2.3	Коефіцієнт надійності персоналу, що забезпечує інформаційну безпеку *Кн.п.*	1	1, зростання
2.4	Коефіцієнт підготовленості персоналу до розпізнавання погроз *Кпп*	1	1, зростання
3.	Оцінка інформації, що надається особам, що приймають рішення (ОПР)		
3.1	Коефіцієнт повноти інформації *Кп.ін.*	0,83	1, зменшення
3.2	Коефіцієнт точності інформації *Кт.ін.*	0,26	1, зростання

3.3	Коефіцієнт суперечливості інформації *Кс.ін.*	0,32	1, зростання
3.4	Коефіцієнт своєчасності надання інформації *Кс.н.ін.*	0,85	1, зростання
3.5	Коефіцієнт надійності інформації *Кн.ін.*	0,74	1, зростання

Примітка. Розраховано автором

Однак, показники надійності персоналу практично всі (окрім коефіцієнту досвіду персоналу) знаходяться в межах нормативних значень, що засвідчує достатній рівень кадрового потенціалу КП «Хмельницька міська дитяча лікарня» у сфері захисту інформації.

З метою подальшого оцінювання рівня інформаційної безпеки установи проведемо порівняння фактично розрахованих показників із їх бальними оцінками представленими в табл. 2.3.

Таблиця 2.3. Інтервальні оцінки рівня інформаційної безпеки

№ з/п	Назва показника	Бали		
		1	2	3
1	2	3	4	5
1.	Оцінка програмно-технічної захищеності інформації			
1.1	Коефіцієнт технічного захисту інформації *Кт.з.*	3 і більше	1-2	0
1.2	Коефіцієнт програмної захищеності інформації *Кп.з.*	0,49 і менше	0,5-0,9	1
1.3	Коефіцієнт фінансового захисту інформації *Кф.з.*	0-0,5	0,6-0,14	0,15, і більше
1.4	Коефіцієнт фінансування інформаційної служби *Кфін.*	0,14 і менше	0,15-0,5	0,5 і більше
2.	Оцінка інформаційної надійності персоналу			
2.1	Коефіцієнт правової захищеності інформації *Кпр.з.*	0,9-1	0,4-0,89	0,39 і менше
2.2	Коефіцієнт досвіду роботи персоналу, що забезпечує інформаційну безпеку *Кд.р.*	0,49 і менше	0,5-0,89	0,9-1
2.3	Коефіцієнт надійності персоналу, що забезпечує інформаційну безпеку *Кн.п.*	0,49 і менше	0,5-0,89	0,9-1
2.4	Коефіцієнт підготовленості персоналу до розпізнавання погроз *Кпп*	0,49 і менше	0,5-0,89	0,9-1
3.	Оцінка інформації, що надається особам, що приймають рішення (ОПР)			
3.1	Коефіцієнт повноти інформації *Кп.ін.*	0,39 і менше	0,4-0,89	0,9-1
3.2	Коефіцієнт точності інформації *Кт.ін.*	0,49 і менше	0,5-0,89	0,9-1
3.3	Коефіцієнт суперечливості інформації *Кс.ін.*	0,39 і менше	0,4-0,89	0,9-1
3.4	Коефіцієнт своєчасності надання інформації	0,39 і	0,4-0,79	0,8-1

	Кс.н.ін.	менше		
3.5	Коефіцієнт надійності інформації *Кн.ін.*	0,49 і менше	0,5-0,89	0,9-1

Примітка. Складено автором

Наступним кроком оцінювання рівня інформаційної безпеки КП «Хмельницька міська дитяча лікарня» є визначення групових та індивідуальних коефіцієнтів вагомості, на основі яких проведемо розрахунок. Встановлення вагових коефіцієнтів ми проводили із використанням методу головних компонент. Результати відобразимо в табл. 2.4

Таблиця 2.4. Вагові коефіцієнти показників оцінки рівня інформаційної безпеки

№ з/п	Назва показника	Вагові коефіцієнти
1	2	3
1.	Оцінка програмно-технічної захищеності інформації	0,3892
1.1	Коефіцієнт технічного захисту інформації *Кт.з.*	0,2852
1.2	Коефіцієнт програмної захищеності інформації *Кп.з.*	0,2879
1.3	Коефіцієнт фінансового захисту інформації *Кф.з.*	0,2478
1.4	Коефіцієнт фінансування інформаційної служби *Кфін.*	0,1791
2.	Оцінка інформаційної надійності персоналу	0,3147
2.1	Коефіцієнт правової захищеності інформації *Кпр.з.*	0,1472
2.2	Коефіцієнт досвіду роботи персоналу, що забезпечує інформаційну безпеку *Кд.р.*	0,2157
2.3	Коефіцієнт надійності персоналу, що забезпечує інформаційну безпеку *Кн.п.*	0,3245
2.4	Коефіцієнт підготовленості персоналу до розпізнавання погроз *Кпп*	0,3126
3.	Оцінка інформації, що надається особам, що приймають рішення (ОПР)	0,2961
3.1	Коефіцієнт повноти інформації *Кп.ін.*	0,1468
3.2	Коефіцієнт точності інформації *Кт.ін.*	0,2165
3.3	Коефіцієнт суперечливості інформації *Кс.ін.*	0,1174
3.4	Коефіцієнт своєчасності надання інформації *Кс.н.ін.*	0,2685
3.5	Коефіцієнт надійності інформації *Кн.ін.*	0,2508

Примітка. Розраховано автором

Тепер розрахуємо рівень інформаційної безпеки шляхом переведення фактичних значень коефіцієнтів у бали та формування суми добутків вагових значень та бальних оцінок (2.5). Таким чином, проведена оцінка засвідчила посередній рівень інформаційної безпеки 63% від максимального рівня, що

зумовлює необхідність обґрунтування напрямів удосконалення інформаційної безпеки закладу охорони здоров'я.

Так, КП «Хмельницька міська дитяча лікарня» повинна визначити свої вимоги до безпеки. При оцінці вимог використовуються три основні показники.

Таблиця 2.5. Оцінка рівня інформаційної безпеки КП «Хмельницька міська дитяча лікарня»

№ з/п	Назва показника	Вагові коефіцієнти	Бальні оцінки	Загальна оцінка із врахуванням
1	2	3	4	5
1.	Оцінка програмно-технічної захищеності інформації	0,3892	1,2879	0,5013
1.1	Коефіцієнт технічного захисту інформації *Кт.з.*	0,2852	1	0,2852
1.2	Коефіцієнт програмної захищеності інформації *Кп.з.*	0,2879	2	0,5758
1.3	Коефіцієнт фінансового захисту інформації *Кф.з.*	0,2478	1	0,2478
1.4	Коефіцієнт фінансування інформаційної служби *Кфін.*	0,1791	1	0,1791
2.	Оцінка інформаційної надійності персоналу	0,3147	2,8528	0,8978
2.1	Коефіцієнт правової захищеності інформації *Кпр.з.*	0,1472	2	0,2944
2.2	Коефіцієнт досвіду роботи персоналу, що забезпечує інформаційну безпеку *Кд.р.*	0,2157	3	0,6471
2.3	Коефіцієнт надійності персоналу, що забезпечує інформаційну безпеку *Кн.п.*	0,3245	3	0,9735
2.4	Коефіцієнт підготовленості персоналу до розпізнавання погроз *Кпп*	0,3126	3	0,9378
3.	Оцінка інформації, що надається особам, що приймають рішення (ОПР)	0,2961	1,6661	0,4933
3.1	Коефіцієнт повноти інформації *Кп.ін.*	0,1468	2	0,2936
3.2	Коефіцієнт точності інформації *Кт.ін.*	0,2165	1	0,2165
3.3	Коефіцієнт суперечливості інформації *Кс.ін.*	0,1174	1	0,1174
3.4	Коефіцієнт своєчасності надання інформації *Кс.н.ін.*	0,2685	2	0,5370

3.5	Коефіцієнт надійності інформації *Кн.ін.*	0,2508	2	0,5016
Загальний рівень інформаційної безпеки				1,8924

Примітка. Складено автором

Першим показником служить оцінка небезпек, з якими стикається організація. Шляхом оцінки небезпек визначаються загрози для інформації, її вразливість та ймовірність виникнення загроз, а також можливий збиток. Другий показник - це законодавчі, нормативні та договірні вимоги, які повинна дотримуватися організація, її партнери, підрядники та постачальники послуг.Третій показник - це певний набір принципів, цілей і вимог до обробки інформації, розроблених організацією для підтримки своєї діяльності.

Визначення вимог до безпеки проводиться шляхом методичної оцінки ризиків. Витрати на підтримку безпеки необхідно збалансувати з шкодою для установи,який може виникнути при порушенні безпеки. Методи оцінки небезпек можуть застосовуватися до всієї організації або лише до її частин, а також до окремих інформаційних систем, системних компонентів і сервісів, в залежності від того, що виявиться найбільш практичним, реалістичним і корисним.

Важливими методами аналізу стану забезпечення інформаційної безпеки є методи опису і класифікації. Для здійснення ефективного захисту системи управління інформаційною безпекою слід, по-перше, описати, а лише потім класифікувати різні види загроз та небезпек, ризиків та викликів і відповідно сформулювати систему заходів по здійсненню управління ними.

У якості розповсюджених методів аналізу рівня забезпечення інформаційної безпеки використовуються методи дослідження причинних зв'язків. За допомогою даних методів виявляються причинні зв'язки між загрозами та небезпеками; здійснюється пошук причин, які стали джерелом і спричинили актуалізацію тих чи інших чинників небезпеки, а також розробляються заходи по їх нейтралізації. У числі даних методів причинних

зв'язків можна назвати наступні: метод схожості, метод розбіжності, метод сполучення схожості і розбіжності, метод супроводжувальних змін, метод залишків.

Для ефективного забезпечення інформаційної безпеки важливим є різноманітні моделі та методи оцінки загроз та небезпек. Їх варіативність занадто лабільна і залежить як від рівня розвитку тієї чи іншої цивілізації, так і від контексту оцінки, що проводиться, наявності всебічних даних по факторах загрози, алгоритму вирахування коефіцієнту імовірності настання та розміру негативних наслідків. Наявність конкретних даних з цього питання дозволяє достатньо точно визначити ступінь впливу інформаційної зброї, рівень загроз та небезпек.

Важливим методом забезпечення інформаційної безпеки є метод критичних сценаріїв. У зазначених сценаріях аналізуються ситуації, коли уявний противник паралізує систему державного управління і відповідно знижує здатність підтримувати державне управління в межах оптимальних параметрів.

Існують методи, які можна вважати основоположними, що дозволяють створити надійну основу для реалізації інформаційної безпеки. Ці методи або базуються на важливих законодавчих вимогах, або відносяться до загальновизнаних методів роботи в області управління інформаційною безпекою.

З законодавчої точки зору найважливішими для організації вважаються наступні заходи:захист даних і нерозголошення особистої інформації;захист організаційних записів;захист прав на інтелектуальну власність.

До загальновизнаних методів забезпечення інформаційної безпеки відносяться наступні: створення документа, що визначає політику інформаційної безпеки; розподіл відповідальності за інформаційну безпеку; навчання і підготовка в галузі інформаційної безпеки; створення звітів про інциденти. Ці методи можуть застосовуватися в більшості організацій і в більшості середовищ. Слід зауважити,що незважаючи на те, що всі описані

методи є важливими,значимість кожного методу слід визначати у світлі конкретних ризиків, з якими стикається організація.

Таким чином, використання пропонованого підходу до оцінювання стану і управління інформаційною безпекою КП «Хмельницька міська дитяча лікарня» дозволило не лише ідентифікувати рівень інформаційної захищеності установи, але й визначити напрями підвищення ефективності використання інформаційних ресурсів та збалансувати витрати на забезпечення інформаційної безпеки.

РОЗДІЛ 3
НАПРЯМИ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ УПРАВЛІННЯ ІНФОРМАЦІЙНОЮ БЕЗПЕКОЮ КОМУНАЛЬНОГО ПІДПРИЄМСТВА «ХМЕЛЬНИЦЬКИЙ МІСЬКА ДИТЯЧА ЛІКАРНЯ»

3.1. Розвиток політики інформаційної безпеки у закладі охорони здоров’я

Вітчизняні заклади охорони здоров’я активно інформатизуються, переходячи до комплексної автоматизації, інтеграції в єдиний інформаційний простір і впровадження технологій електронних реєстратур і електронних медичних карт. Особливої актуальності набувають інформаційні системи, пов'язані з телемедициною. Процес телемедичного консультування супроводжується передачею між учасниками заявок, виписок, медичних зображень, висновків, юридичних і фінансових документів. Інтелектуальною основою телемедичних комплексів є медичні інформаційні системи. Саме вони інтегрують і зберігають всі дані, дозволяють шукати і аналізувати потрібну лікарю інформацію.

Говорячи про інформатизацію закладів охорони здоров’я, треба розуміти нерозривність процесів створення та впровадження медичної інформаційної системи і реалізації комплексу заходів, спрямованих на захист інформації, що міститься в даній інформаційній системі, забезпечення її цілісності, доступності, конфіденційності. Однією з головних проблем при створенні медичних інформаційних систем є забезпечення інформаційної безпеки.

При цьому увага приділяється як даним про здоров'я пацієнтів та хід лікувально-діагностичного процесу, що містяться в медичних інформаційних систем, так і інформації, що становить сутність самої медичної інформаційної системи: кодам її модулів, організації зберігання і обробки даних, вмісту загальносистемних баз даних тощо.

Частина даних, що вводяться, оброблюються і збережених в процесі функціонування медичних інформаційних систем, є персональними даними або може становити лікарську таємницю.

Особливістю медичної інформації є її конфіденційність. База даних медичної інформаційної системи містить критично важливу інформацію, від якої часто може залежати життя людини. Тому ключовим фактором при створенні медичних інформаційних систем має стати забезпечення цілісності бази даних, а також можливість спостереження, моніторингу стану самої системи і її захищеності.

Інформаційна безпека досягається за допомогою застосування відповідного набору засобів управління, обраного за допомогою процесу управління ризиками і керованого з використанням системи менеджменту інформаційної безпеки, включаючи політику, процеси, процедури, організаційні структури, програмне та апаратне забезпечення, щоб захистити ідентифіковані інформаційні активи [17, с.28]. Ці засоби управління повинні бути визначені, реалізовані, перевірені, проаналізовані і при необхідності поліпшені, щоб гарантувати, що рівень безпеки відповідає діловим цілям організації. Засоби управління безпекою важливої інформації нерозривно зв'язуються з бізнес-процесами медичної організації [41, с.82].

Першим кроком на шляху до побудови системи повинні бути визначені загальні положення Політики інформаційної безпеки закладу охорони здоров’я, описані технічні, організаційні вимоги, визначено склад заходів захисту інформації та їх базові набори для відповідного класу захищеності інформаційної системи, що дозволяють вибудувати системи менеджменту інформаційної безпеки. В основі цього підходить лежить методологія, відома як «цикл PDCA» (Plan - Do - Check - Act) [86] (табл. 3.1).

Одним з ключових умов ефективного впровадження функціонування системи управління інформаційною безпекою є залучення менеджменту закладу охорони здоров’я в процес управління інформаційною безпекою. Всі працівники повинні розуміти, що, по-перше, вся діяльність з

забезпеченняінформаційної безпеки, ініційована керівництвом, є обов'язковою для виконання, по-друге, керівництво закладу особисто тримає на контролі функціонування системи менеджменту інформаційною безпекою, по-третє, керівництво також виконує правила щодо забезпечення інформаційною безпекою, як і всі працівники закладу.

Таблиця 3.1. Опис циклу PDCA (Plan-Do-Check-Act) для впровадження системи управління інформаційною безпекою

PDCA	Опис
Планування	Розроблення політики безпеки, визначення мети, процесів та процедур, пов’язаних з управлінням ризиками та підвищенням інформаційної безпеки для досягнення результатів відповідно до загальної політики та цілей організації
Виконання	Впровадження та використання політики безпеки, елементів керування, процесів та процедур, механізмів контролю
Перевірка	Оцінювання та вимірювання ефективності роботи відповідно до політики безпеки, цілей та практичного досвіду, а також підготовка звіту про результати для керівництва з метою подальшого аналізу й аудиту
Вплив (управління, коригування)	Застосування коригувальних та профілактичних заходів з метою досягнення постійного вдосконалення СУІБ на основі результатів аналізу; перегляд політики безпеки; підвищення поінформованості персоналу

Джерело: [86].

Провідною світової практикою у сфері управління інформаційною безпекою є стандарт ISO / IEC 27001 «Інформаційні технології - Методи забезпечення безпеки - Системи управління інформаційною безпекою - Вимоги» [44], розроблений Міжнародною організацією зі стандартизації (ISO) і Міжнародної електротехнічної комісією (IEC) на основі британського стандарту BS 7799 . Міжнародний стандарт ISO / IEC 27001 визначає вимоги до системи управління інформаційною безпекою та визначає її як «збереження конфіденційності, цілісності та доступності інформації», крім

того, можуть бути включені і інші властивості, включаючи достовірність, актуальність, авторство тощо [86, с.152].

У загальному вигляді модель системи менеджменту інформаційної безпеки закладу охорони здоров’я повинна бути представлена в зазначеному стандарті, проте розробку елементів системи необхідно розглядати з позиції застосування для конкретної медичної організації з урахуванням галузевої специфіки.Для успішної реалізації заходів щодо впровадження та сертифікації системи менеджменту інформаційної безпеки, в першу чергу, повинні бути визначені цілі проекту в медичній організації, наприклад [31, с.25]:

1) реалізація законодавчих вимогщодо захисту персональних даних, підвищення рівня безпеки всіх існуючих в організації інформаційних активів;

2) зниження і мінімізація кількості інцидентів, пов'язаних з інформаційною безпекою, їх ймовірності і наслідків;

3) інші цілі, пов'язані з мінімізацією ризиків інформаційної безпеки.

На початковій стадії проекту необов'язково ставити мету отримання сертифіката ISO/IEC 27000. Вимоги стандарту повинні бути прийняті керівництвом в якості інструменту для розуміння основних напрямів управлінських впливів в області вибору підходів, інструментів і процедур забезпечення захисту інформації. На основі опрацювання цього стандарту, успішної практики вітчизняних установ [32; 63; 18], нами розроблена модель системи менеджменту інформаційної безпеки, побудована на основі процесного підходу (рис.3.1).

Всі процеси в даній моделі розділені на класичні чотири групи: процеси управління, основні, що забезпечують процеси, а також процеси вимірювання, аналізу і поліпшення. Така логіка дозволяє легко вбудовувати процеси забезпечення інформаційної безпеки в інтегровану систему менеджменту, тобто гармонійно поєднується із системою менеджменту якості, що відповідає ISO 9001, і яка стратегічним напрямом для кожного закладу охорони здоров’я.

Рисунок 3.1. –Розробка системи менеджменту інформаційної безпеки (СМІБ) закладу охорони здоров'я

Примітка. Запропоновано автором.

Вихідним етапом в реалізації даної моделі повинна стати розробка політики закладу охорони здоров'я медичної організації у сфері інформаційної безпеки. Результати реалізації політики відображаються в аналізі даних (як правило, проводяться 1 раз в квартал) і аналізі СМІБ з боку керівництва один раз на рік. Необхідно реалізувати процес планування даної діяльності, ідентифікації ризиків, формування реєстру ризиків. Обов'язковою процесом є розробка методик оцінки ризиків відповідно до галузевої специфіки, управління ризиками. Найважливішим розділом діяльності

виділено внутрішній аудит, з проведення якого починається діагностика діючої системи менеджменту інформаційної безпеки [54]. Що стосується підходів до реалізації захисних заходів щодо забезпечення безпеки інформаційних систем, то необхідно є трьоетапна розробка таких заходів. Перша стадія - вироблення вимог - включає визначення складу засобів інформаційної системи, аналіз вразливих елементів ІС, оцінку загроз (виявлення проблем, які можуть виникнути при наявності вразливих місць), аналіз ризику (прогноз можливих наслідків, які можуть викликати ці проблеми). Друга стадія - визначення способів захисту - включає відповіді на наступні питання [70, с.82]:

які загрози повинні бути усунені і в якій мірі;

які ресурси системи повинні захищатись і в якій мірі?

за допомогою яких засобів повинен бути реалізований захист?

яка повинна бути повна вартість реалізації захисту і витрати на експлуатацію з урахуванням потенційних загроз?

Третя стадія - визначення функцій, процедур і засобів безпеки, що реалізуються у вигляді деяких механізмів захисту. Всі прийнятні підходи для забезпечення інформаційної безпеки повинні бути реалізовані з урахуванням принципів комплексності, безперервності захисту, розумної достатності, гнучкості системи захисту,відкритості алгоритмів і механізмів, простоти застосування засобів захисту [30, с.8].

Для підтримки системи в робочому стані необхідна розробка локальних нормативних актів (рис.3.2), приблизний перелік яких включає Концепцію інформаційної безпеки, Політику інформаційної безпеки, Положення про обробку і захист персональних даних (ПД) працівників, Положення про обробку і захист персональних даних пацієнтів», наказ «Про медичної інформаційної системі МІС », наказ«Про підготовку документів про обробку персональних даних», наказ«Про призначення відповідальних осіб за забезпечення захисту персональних даних», наказ«Про класифікацію інформаційних систем персональних даних», наказ«Про режим обробки і

захисту персональних даних », наказ«Про нерозголошення персональних даних» та інші. Встановлюється перелік структурних підрозділів і посад співробітників організації, допущених до роботи з персональними даними.

I рівень
Концепція інформаційної безпеки, Політика інформаційної безпеки
↓
II рівень
наказ «Про медичної інформаційної системі МІС », наказ «Про підготовку документів про обробку персональних даних», наказ «Про призначення відповідальних осіб за забезпечення захисту персональних даних», наказ «Про класифікацію інформаційних систем персональних даних», наказ «Про режим обробки і захисту персональних даних », наказ «Про нерозголошення персональних даних»
↓
III рівень
посадова інструкція адміністратора інформаційної безпеки; інструкція користувача інформаційної системи персональних даних; інструкція користувача інформаційної системи персональних даних при виникненні позаштатних ситуацій; інструкція адміністратора інформаційної безпеки персональних даних; інструкція адміністратора інформаційної системи персональних даних
↓
IV
регламенти інформаційного аудиту; модель загроз медичної інформаційної системи; реєстр інформаційних ризиків; план внутрішніх перевірок режиму захисту персональних даних в інформаційних системах; план заходів щодо забезпечення захисту персональних даних в інформаційних системах;

Рисунок 3.2. – Системалокальних нормативних актів, що регулює систему інформаційної безпеки закладу охорони здоров’я

Примітка. Складено автором.

Концепція інформаційної безпеки закладу охорони здоров’я визначає основні цілі та завдання, а також загальну стратегію побудови системи захисту персональних даних; визначає основні вимоги та базові підходи до їх реалізації, для досягнення необхідного рівня безпеки інформації. Структура такої концепціїКП «Хмельницька міська дитяча лікарня» для представлена у додатку А.

Для здійснення інформаційної безпеки (і її контролю) повинні бути класифіковані інформаційні системи персональних даних організації і розроблені локальні акти, які визначають наступне [42,с.15]:

перелік об'єктів захисту;

перелік класифікованих інформаційних систем персональних даних;

правила обробки персональних даних, які здійснюються без використання засобів автоматизації;

посадову інструкцію адміністратора інформаційної безпеки;

інструкцію користувача інформаційної системи персональних даних;

інструкцію користувача інформаційної системи персональних даних при виникненні позаштатних ситуацій;

інструкцію адміністратора інформаційної безпеки персональних даних;

інструкцію адміністратора інформаційної системи персональних даних;

порядок резервування та відновлення працездатності технічних засобів і програмного забезпечення баз даних ізасобів захисту інформації в інформаційних системах;

перелік технічних засобів захисту інформації, експлуатаційної та технічної документації до них, що застосовуються в організації;

план заходів щодо забезпечення захисту персональних даних в інформаційних системах;

план внутрішніх перевірок режиму захисту персональних даних в інформаційних системах.

Для кожної інформаційної системи персональних даних повинні бути розроблені моделі загроз. Повинні бути визначені склад заходів захисту інформації та їх базові набори для відповідного класу захищеності інформаційної системи, що визначають область дії СМІБ. Потрібні документування процесу реєстрації всіх інформаційних активів, визначення повного переліку загроз і ризиків ІБ, розрахунок ймовірності і можливих наслідків ризиків [59, с.20].

Розробка моделі загроз інформаційній безпеці закладу охорони здоров’я є необхідною умовою формування обґрунтованих вимог до забезпечення безпеки інформації медичних інформаційних систем і проектування системи управління інформаційною безпекою. Цей документ являє собою опис типових загроз, що містить опису в наступній структурі: анотація загрози; можливі джерела загрози; спосіб реалізації загрози; використовувані уразливості; види ресурсів, що потенційно знаходяться під загрозою; - характеристики безпеки ресурсів, що порушуються; можливі наслідки реалізації загрози. Приклад такого опису представлений у табл.3.1.

Таблиця 3.2 Паспорт загрози інформаційної безпеки КП «Хмельницька міська дитяча лікарня»

1. Анотація загрози	здійснення несанкціонованого ознайомлення, модифікації і блокування цільової інформації, що зберігається та оброблюваної в МІС.
2. Можливі джерела загрози:	1) користувачі МІС; 2) співробітники закладу, що мають санкціонований доступ в службових цілях до приміщень, в яких розміщуються ресурси МІС, але не мають права доступу до ресурсів; 3) обслуговуючий персонал закладу (охорона, працівники інженерно-технічних служб і т.д.) 4) особи, які мають можливість доступу до системи передачі даних; 5) користувачі, які є зовнішніми по відношенню до конкретної системи.
3. Способи реалізації загрози:	1) здійснення несанкціонованого доступу, використовуючи штатні засоби МІС; 2) використання безконтрольно залишених технічних засобів; 3) розкрадання порушниками і втрата уповноваженими особами технічних засобів МІС (в тому числі носіїв інформації); 4) несанкціонований перегляд засобів відображення інформації і роздрукованих документів.
4. Вразливості	- недоліки механізмів розмежуваннядоступу і організаційних заходів, пов'язані з можливістюздійснення несанкціонованого доступу до інформації, що захищається.
5. Вид ресурсів, що потенційно знаходяться під загрозою	цільова інформація
6. Характеристики безпеки ресурсів, що порушуються	конфіденційність, цілісність, доступність.
7. Можливі наслідки реалізації загрози	несанкціоноване ознайомлення з інформацією, що захищається; спотворення інформації; неподання цільової

	інформації споживачам в відведені часові рамки.

Примітка. Запропоновано автором.

Слід зазначити, що прийняття системи менеджменту інформаційної безпеки (СМІБ) закладу охорони здоров’я є стратегічним рішенням для, і необхідно, щоб це рішення нерозривно інтегрувалися, оцінювалося і оновлювалося відповідно до її потреб. На розробку і реалізацію системи менеджменту інформаційної безпеки закладу охорони здоров’я організації впливають потреби і цілі організації, вимоги безпеки, які використовуються бізнес-процеси, а також розмір і структура організації. Розробка і функціонування системи менеджменту інформаційної безпеки повинні відображати інтереси і вимоги інформаційної безпеки всіх зацікавлених осіб організації, включаючи пацієнтів, постачальників, ділових партнерів, страхові компанії, органи управління охороною здоров'я та інших осіб.

Основною проблемою при впровадженні системи інформаційної безпеки є людський фактор. Оскільки забезпечення інформаційної безпеки завжди пов'язано зі змінами логіки роботи і обмеженнями, необхідно в першу чергу переконатися в тому, що правила інформаційної безпеки не зроблять негативного впливу на працездатність закладу. Для того щоб уникнути цього, до впровадження наказів, інструкцій та положень доцільно створити комісію, що складається з представників ключових підрозділів організації. На засіданнях комісії фахівець з інформаційної безпеки буде доповідати про необхідність впровадження змін, подавати відповідні документи до обговорення та вносити виправлення згідно із зауваженнями членів комісії [37,с.70].

В закладі охорони здоров’я, де використовується дорога техніка, що стоїть на спеціальному обслуговуванні, одним з ключових питань є забезпечення взаємодії та розмежування повноважень зі сторонніми організаціями, що обслуговують цю техніку. Порядок взаємодії повинен бути затверджений документально і містити пункт про конфіденційність

інформації.Досить важливою і найбільш важкою частиною впровадження системи інформаційної безпеки є забезпечення контролю роботи системного адміністратора. Системний адміністратор в силу посадових обов'язків і при відповідному рівні кваліфікації має необмежені повноваження і можливості у інформаційній системі. Низький рівень заробітної плати, відсутність належної кваліфікації та відсутність контролю за діяльністю системного адміністратора створюють загрозу для роботи інформаційної системи закладу. Одним з найважливіших аспектів, про які часто забувають при впровадженні будь-якої системи контролю, в даному випадку системи інформаційної безпеки, є розробка системи штрафних санкцій за невиконання вимог. Без штрафних санкцій система працювати не буде.

Таким чином, сучасні практики з управління системи менеджменту інформаційної безпеки закладу охорони здоров’я базуються на міжнародному стандарті ISO/IEC 27000. Виконання вимог ISO/IEC 27000дозволяє медичної організації формалізувати і структурувати процеси управління інформаційною безпекою за наступними напрямами: розробка політики безпеки; організація інформаційної безпеки; організація управління внутрішніми активами і ресурсами, що складають основу ключових процесів діяльності; захист персоналу і зниження внутрішніх загроз; фізична безпека і безпека навколишнього середовища; управління засобами зв'язку та експлуатацією обладнання; управління і контроль доступу; розробка та обслуговування апаратно-програмних систем; відповідність вимогам стандарту і дотримання правових норм з безпеки [10,с.106].

Основні очікувані результати впровадження елементів системи інформаційної безпеки в закладі охорони здоров’я:

проводиться ідентифікація основних ризиків ІБ, в тому числі в рамках реалізації вимог Закону України «Про захист персональних даних»; ідентифіковані основні загрози, розроблений комплекс заходів по всіх напрямах захисту;

вірусні атаки відображаються стовідсотково, відсутні випадки несанкціонованого доступу, заблокована несанкціонована розсилка, відсутні випадки атак, втручання в роботу програм, несправності або поломки обладнання.

Основна вигода впровадження СМІБ - виявлення найбільш небезпечних загроз і економія коштів на створення ефективної системи забезпечення інформаційної безпеки [56, с.166]. Системаінформаційної безпеки повинна вийти на вищий рівень управління, дозволяючи всебічно оцінювати інформаційні ризики і завчасно їх мінімізувати.

3.2. Удосконалення організаційного забезпечення управління інформаційною безпекою закладу охорони здоров'я

Сформуємо комплекс заходів забезпечення інформаційної безпеки закладу охорони здоров'я, що дозволить створити чітку і злагоджену систему організації роботи з кадрами, здатну захистити інформацію та інформаційні системизакладу (табл.3.3). Управління інформаційною безпекою закладу охорони здоров'яповинна враховувати ступінь використання в господарській діяльності сучасних інформаційних систем: рівень залучення сервісів мережі Інтернет в управління закладом та здійснення медичної діяльності; якість і кількість залучених програмних засобів, які мають вихід у глобальний інформаційний простір і не передбачають виходу; кваліфікація персоналу, який здійснює управління інформаційним простором закладу; вартість утримання обслуговування інформаційних систем; перспективи зростання компанії з використанням внутрішніх інформаційних систем і сервісів мережі Інтернет [11, с.82].

Розглянемо окремі заходи більш детально.

1. Навчання керівного складу та співробітників, відповідальних за інформаційну безпеку, вимогам стандарту у контексті плану дій щодо

комплексної модернізації системи управління інформаційною безпекою (СУІБ) УДЦР за наступними програмами:

«ISO 27001. Внутрішній аудитор. Вступ, впровадження та внутрішній аудит системи управління інформаційною безпекою (СУІБ)» (1 фахівець)

«Стандарт ISO/IEC 27001:2013. Аудитор/Провідний аудитор систем менеджменту інформаційної безпеки» (1 фахівець).

Після успішної здачі екзамену кожен учасник отримує сертифікат від міжнародної компанії BureauVeritas про підтвердження кваліфікації внутрішнього аудитора.

Таблиця 3.3Організаційні заходи посилення інформаційної безпеки КП «Хмельницька міська дитяча лікарня»

Захід	Необхідні процедури	Результат	Витрати
1	2	3	4
1. Організація тренінгів для персоналу служби інформаційної безпеки	- складання планів навчання та графіків проходження працівниками; - пошук спеціалізованих курсів/організаторів та укладання відповідних угод; - навчання керівного складу та співробітників, відповідальних за інформаційну безпеку, вимогам стандарту ISO 27001	Підвищення кваліфікації персоналу служби інформаційної безпеки.	Оплата праці залучених працівників для проведення навчання.
2. Впровадження системи корпоративних носіїв інформації (флешки)	- встановлення програмного забезпечення на усі комп’ютери, що блокує використання сторонньої флешки; - закупівля корпоративних носіїв інформації (як мінімум 1 флешка на комп’ютеризований відділ; - проведення інструктажу персоналу щодо використання носіїв;	Неможливість використання такої флеш-картки на сторонніх комп’ютерах та використання «сторонніх» флешок в середині закладу	Витрати на програмне забезпечення та флеш-картки.
3. Організація навчання персоналу з питань інформаційних безпеки	- визначення переліку посад та структурних підрозділів, що підлягають обов’язковому проходженню навчання; - складання планів навчання та графіків проходження працівниками;	Формування моделі поведінки працівників у випадку настання реальної	Встановлення надбавки працівникам інформаційно-аналітичного відділу за кількість

	- визначення організаторів проведення (співробітників служби інформаційно-аналітичного відділу); - проведення занять; - перевірка знань;	загрози. Унеможлив-лення витоку інформації, у тому числі персональних даних працівників та пацієнтів	проведених занять або введення посади методиста з інформаційної безпеки

Продовж.табл.3.3

1	2	3	4
4. Підготовка інформаційних матеріалів	- виготовлення інформаційних папок (10 проспектів-листів А4) про типові ситуації протидії кібератакам та іншим загрозам (не менше 2 примірників на комп'ютеризований відділ); - підготовка підбірки відеороликів щодо типових ситуацій у сфері інформаційних злочинів у закладі охорони здоров'я	Формування моделі поведінки працівників у випадку настання реальної загрози. Унеможлив-леннявитоку інформації, у тому числі персональних даних працівників та пацієнтів	Витрати на папір, фарбу для принтера, папки для документів тощо.
5. Здійснення інформаційного аудиту інформаційних систем закладу охорони здоров'я	- виявляти інформаційні потреби підприємства, його структурних підрозділів; - вивчити стан і оцінити використання внутрішніх і зовнішніх інформаційних ресурсів і способи їх найбільш ефективного використання; - скласти карту інформаційних потоків і визначити вузькі місця в цих потоках;.	Визначення ризиків інформаційно безпеки, джерел їх виникнення, формування програми протидії	Оплата праці залучених працівників для проведення інформаційного аудиту або оплата навчання власного персоналу з питань здійснення інформаційного аудиту

Примітка. Складено автором.

Для організації навчання стандарту ISO 27001 з управління інформаційною безпекою КП «Хмельницька міська дитяча лікарня»повинна виділити певну суму як на оплату послуг компанії, що проводитиме навчання, так і на проїзд та проживання працівників у відповідне місце (у випадку здійснення навчання недистанційна). Нами визначено орієнтовану величину таких витрат для двох працівників, яким варто отримати навички у цій сфері (табл.3.4).

Таким чином, одноразові витрати становитиме 28 тис.грн. Слід зазначити, що щорічний аудит інформаційної безпеки з залученням сторонніх організацій буде коштуватиме 1500 тис.грн., що майже у 4 рази дорожче. Здійснивши навчання стандарту ISO 27001 працівники зможуть

самостійно проводити таку оцінку, організовувати та здійснювати внутрішні тренінги для користувачів інформаційних та телекомунікаційних мереж – працівників підприємства.

Таблиця 3.4Витрати на тренінги з навчання стандарту ISO 27001 з управління інформаційною безпекою

Витрати	Вартість на 1 працівника, грн./ $	Вартість на 2 працівників, тис.грн.
1. Навчання персоналу на курсах	275$	15400
2. Проживання в гуртожику/хостелі	750	350*2*4=6000
3. Проїзд	550	550*2=1100
4. Оплата відрядження	60	60*2=120
Всього	14010	28020

Примітка. Складено автором.

2. Поява флеш-носіїв інформації та їх широке використання, поруч зі зручністю та доступністю, стали додатковим шляхом розповсюдження шкідливого програмного забезпечення, «троянів» шпигунських агентів тощо. Наслідки такого зараження різні — починаючи від втрати інформації, її витоку і закінчуючи блокуванням роботи комп’ютера, інформаційної системи чи навіть втратою управління мережами спеціального зв’язку.

Рівень інформаційної та фізичної безпеки персональних накопичувачів інформації працівників і пацієнтів закладу охорони здоров’я повинна забезпечувати належний захист. Тому до таких накопичувачів висуваються підвищені вимоги до реалізації систем захисту інформації. Загроза витоку інформації, що зберігається на цифрових накопичувачах, в результаті передачі накопичувача за межі організації, нині добре відома багатьом фахівцям. Тому пропонуємо запровадити на підприємстві використання корпоративних USB-флеш накопичувачів, використання яких поза відповідної мережі неможлива.

У табл. 3.5 наведено основні характеристики USB-флеш накопичувачів, які пропонують розробники для експлуатації у корпоративних, державних та військових організаціях.

Таблиця 3.5Характеристики USB-флеш накопичувачів корпоративного класу різних виробників

Фірма-виробник	Основний тип автентифікації	Адміні-стрування	Система захисту	Вартість, дол. США
IronKey	КП*	+	-	59-299
Imation ВП	ВП*	+	+	129-683
SpyRus	КП	+	+	200-236
Lok-it	PIN-код	-	-	97-183
Lexar	КП	+	+	100-270
Gemalto	КП	+	+	121
Kanguru	КП	+	+	40-500
Verbatim	КП	+	-	118-460
CheckPoint	КП	+	+	160
McAfee	ВП/КП	+	+	169-417
Kingston	КП	-	-	80-212
SandiskEnteprise	КП	+	-	58-375
Integralmemory	КП	-	-	67-206
Elytra	КП	-	-	89-358

КП – введення паролю з клавіатури; ВП – сканування відбитка пальця.

Джерело: [33,с.62].

З наведених даних виділити основні показники, за якими флеш накопичувач може бути віднесений до системи з підвищеним ступенем захисту: в ньому реалізовані шифрування потоку даних між комп’ютером та накопичувачем за контролером накопичувача; система обмеженої кількості спроб введення паролю; разові паролі; вмикання на корпусі або при автентифікації режиму пам’яті тільки на читання або читання/запис файлів; система керування ключами на базі асиметричного шифрування та підтримка роботи в режимі багатофакторного автентифікатора.

Мінімальна вартість флеш накопичувачів приблизно складає 60 дол. США, з чого можна зробити висновок, що розробка таких виробів є

складною технічною задачею, вироби потребують високоякісних мікросхем та проходять сертифікацію.

Враховуючи, що на КП «Хмельницька міська дитяча лікарня»кількість комп'ютеризованих робочих місць становить 196 од., орієнтовна вартість реалізації пропозиції при мінімальній вартості флешки 60$ та курсі НБУ 28 грн./ $ становить:196*60*28=329280грн.

3. Організація навчання персоналу з питань інформаційних безпеки, для чого необхідним є здійснення таких заходів:

-визначення переліку посад та структурних підрозділів, що підлягають обов'язковому проходженню навчання;

- складання планів навчання та графіків проходження працівниками;

- визначення організаторів проведення (співробітників служби інформаційної безпеки);

- проведення занять;

- перевірка знань.

Результатом запровадження такого захисту є формування моделі поведінки працівників у випадку настання реальної загрози; унеможливлення витоку інформації, у тому числі персональних даних працівників та пацієнтів, зменшення кількості «успішних атак» на заклад; зменшення фінансових втрат на відновлення системи безпеки тощо.

Як вже говорилось, після проходження тренінгів працівниками служби інформаційної безпеки, вони зможуть здійснювати інструктажі/тренінги для відповідних працівників підприємства, робота яких пов'язана із роботою інформаційних та інформаційно-телекомунікаційних систем.

Розрахуємо кількість таких семінарів, виходячи із кількості користувачів ПЕОМ на підприємстві – 196 од. Оптимальним є склад групи для навчання в чисельності 10 осіб, тривалість навчання не менше 6 год. та 2 год. на перевірку знань, отже протягом року має бути організовано не менше ніж:

196/10*8=157 год.

Враховуючи, що тривалість робочого дня становить 8 год., для проведення таких занять працівник-тренер має витратити 20 днів (157/8) протягом року. Якщо таку діяльність буде здійснювати працівник без звільнення від основних функцій, йому пропонується виплачувати надбавку за інтенсивність у розмірі 50% до окладу, що становитиме:

12500/24*20=10416 грн., а витрати підприємства з урахуванням ЄСВ становитиме: 10416*1,22=12708 грн. (Середній оклад працівника інформаційно-аналітичного відділу КП «Хмельницька міська дитяча лікарня» становить 12500 грн./міс).

4. Підготовка інформаційних матеріалів. На бізнес-тренера з інформаційної безпеки буде покладено також розробка інформаційних матеріалів з питань протидії інформаційним загрозам. Це забезпечить формування моделі поведінки працівників у випадку настання реальної загрози; унеможливлення витоку інформації, у тому числі персональних даних працівників та пацієнтів тощо.

Як вже говорилось вище, для навчання працівників закладу охорони здоров'я, що використовують інформаційні технології, доцільним є виготовлення інформаційних папок про типові ситуації протидії кібератакам та іншим загрозам; підготовка/підбір відеороликів щодо типових ситуацій у сфері інформаційних злочинів, зокрема у закладах охорони здоров'я. Розрахуємо мінімальні витрати на здійснення заходів.

Тренером має бути підготовлено не менше 2 примірників папок на комп'ютеризований відділ з 10 проспектами-листам А4 про типові ситуації протидії кібератакам та іншим загрозам: це може бути пам'ятки або інші інструкції та алгоритми дій в тих чи інших ситуаціях.

У КП «Хмельницька міська дитяча лікарня»кількість комп'ютеризованих робочих місць становить 196 од., що розташовані у 65 кабінетах, відповідно визначимо вартість інформаційних матеріалів:

65*10*1*2=1300 грн. – вартість друку матеріалів;

480*2*5=650 грн. – вартість папок.

Загальна сума становить 1950 грн. на рік.

Визначимо загальну суму річних витрат на реалізацію запропонованих рішень (табл.3.6). Як бачимо, такі заходи не є витратомісткими, в той же час здатні знизити ризики інформаційних загроз та підвищити інформаційну безпеку закладу охорони здоров'я.

Таблиця 3.6Кошторис витрат на організаційні заходи посилення інформаційної безпеки КП «Хмельницька міська дитяча лікарня»

Захід	Витрати, грн./рік
1. Організація тренінгів для персоналу інформаційно-аналітичного відділу	28020
2. Впровадження системи корпоративних носіїв інформації (флешки)	329280
3. Організація навчання персоналу з питань інформаційних безпеки	12708
4. Підготовка інформаційних матеріалів	1950
Всього	=371958

Примітка. Складено автором.

Звичайно, щоб оцінити ефективність необхідно порівняти необхідні витрати з отриманою вигодою, що у нашому випадку може виступати як відвернення витрат на відновлення системи безпеки та ліквідацію наслідків впливу негативних факторів (відновлення діяльності пошкоджених комп'ютерів та відновленням втраченої інформації); втрачена вигода чи виплата компенсацій постраждалим через витік інформації тощо.

ВИСНОВКИ

Магістерська робота спрямована на поглиблення теоретичних основ та опрацювання практичних рекомендацій щодо управління інформаційною безпекою закладу охорони здоров’я. До основних результатів дослідження належать наступні:

1. На основі критичного аналізу літературних джерел встановлено, що інформаційна безпека орагнізації – це певний стан захисту інформаційних баз даних, інформаційних систем підприємства та їх інформаційної інфраструктури, при якому зводяться до мінімуму всі небажані наслідки використання інформаційних продуктів та інформаційних технологій, забезпечується їх збереження від несанкціонованого доступу та втручання. В змістовному плані, інформаційна безпека включає три складові: задоволення інформаційних потреб суб'єктів; забезпечення безпеки інформації; забезпечення захисту суб'єктів інформаційних відносин від негативного інформаційного впливу.

2. Відзначено, що управління інформаційною безпекою – це внутрішня структура, систематизована сукупність, єдність, взаємозв’язок і диференціація окремих її елементів (об’єкт, суб’єкти, основні характеристики, рівні інформаційної безпеки та перелік загроз). Технології захисту даних ґрунтуються на застосуванні сучасних методів, які запобігають витоку інформації та її втраті. Для запобігання втрати та витоку таємних даних використовуються засоби: фізичні; апаратні; програмні; апаратно-програмні; законодавчі; криптографічні та організаційні методи, які доцільно використовувати в комплексі.

3. Визначено завдання системи інформаційної безпеки КП «Хмельницька міська дитяча лікарня»: забезпеченні безпечного, надійного зберігання і передачі інформації в електронному та друкованому вигляді, розташованої на різних носіях; організації надійного доступу до інформації; обмеження і контроль доступу до інформації, з якою працюють

співробітники, зокрема забезпечення збереження персональних даних пацієнтів; створенні правил безпечної роботи з інформацією; проведенні заходів щодо резервування інформації; забезпеченні відновлення інформації в аварійних ситуаціях; підтримці інформаційної безпеки на заданому рівні.

Встановлено, що процес забезпечення інформаційної безпеки закладу охорони здоров'я можна представити як взаємодію трьох підсистем: підсистема інформаційного забезпечення процесу управління; підсистема захисту інформаційного середовища; підсистема діагностики рівня інформаційної безпеки. Ключовими задачами підсистеми інформаційного забезпечення процесу управління закладу охорони здоров'я є: збирання необхідної інформації; обробка і систематизація інформації; оцінка й аналіз інформації; прогнозування всіх аспектів діяльності; надання необхідної інформації особам, що приймають рішення.

4. Діагностику рівня інформаційної безпеки КП «Хмельницька міська дитяча лікарня» було запропоновано проводити за трьома ключовими напрямками: оцінка програмно-технічної захищеності інформації; оцінка інформаційної надійності персоналу; оцінка інформації, що надається особам, що приймають рішення. Для оцінки інформаційної надійності персоналу закладу охорони здоров'я розраховано: коефіцієнт правової захищеності інформації, коефіцієнт досвіду роботи персоналу, що забезпечує інформаційну безпеку установи, коефіцієнт надійності персоналу, що забезпечує інформаційну безпеку та коефіцієнт підготовленості персоналу до розпізнавання погроз. Оцінювання інформації, що надається особам, що приймають рішення, проведено за допомогою п'ятьох показників: коефіцієнт повноти інформації, коефіцієнт точності інформації та коефіцієнт суперечливості інформації, коефіцієнт своєчасності надання інформації та коефіцієнт надійності інформації. Проведена оцінка засвідчила посередній рівень інформаційної безпеки 63% від максимального рівня, що зумовлює необхідність обґрунтування напрямів удосконалення інформаційної безпеки КП «Хмельницька міська дитяча лікарня».

5. Обґрунтовано необхідність впровадження системи менеджменту інформаційної безпеки, що базується на вимогах стандарту ISO/IEC 27001. Представлена модель системи менеджменту інформаційної безпеки закладу охорони здоров'я, описані основні етапи її впровадження у КП «Хмельницька міська дитяча лікарня». Наголошено на необхідності регламентування управління інформаційною безпекою через систему локальних нормативних актів, представлено основні складові такої системи, зокрема Концепцію інформаційної безпеки, паспорт загрози інформаційної безпеки закладу охорони здоров'я. Основна вигода впровадження системи менеджменту інформаційної безпеки - убезпечення найбільш небезпечних загроз як в площині захисту ресурсів закладу, так і витоку інформації, у тому числі персональних даних працівників та пацієнтів.

6. Сформовано комплекс заходів забезпечення інформаційної безпеки КП «Хмельницька міська дитяча лікарня», який передбачає зниження інформаційних загроз, що пов'язані із людським фактором. До таких заходів віднесено: організація тренінгів для персоналу служби інформаційної безпеки, зокрема на знання вимог стандарту ISO/IEC 27001; впровадження системи корпоративних носіїв інформації (флешки); організація навчання персоналу підприємства з питань інформаційних безпеки (зокрема тих, хто працює з медичними інформаційними системами), підготовка інформаційних матеріалів (інструкцій, пам'яток) тощо. Для кожного заходу визначено необхідні процедури для реалізації, очікуваний результат, а також обґрунтовано витрати на впровадження.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Анисимов А. А. Менеджмент в сфереинформационнойбезопасности. URL: http://www.intuit.ru/department/itmngt/manofis/
2. Баланс (форма № 1 – додаток 1 до Порядку складання фінансової звітності розпорядниками та одержувачами бюджетних коштів) за 2019 р. КП «Хмельницька міська дитяча лікарня» Хмельницької міської ради. Хмельницький, 2019 р. 2 с.
3. Баланс (форма № 1 – додаток 1 до Порядку складання фінансової звітності розпорядниками та одержувачами бюджетних коштів) за 2018 р. КП «Хмельницька міська дитяча лікарня» Хмельницької міської ради. Хмельницький, 2018 р. 2 с.
4. Баланс (форма № 1 – додаток 1 до Порядку складання фінансової звітності розпорядниками та одержувачами бюджетних коштів) за 2017 р. КП «Хмельницька міська дитяча лікарня» Хмельницької міської ради. Хмельницький, 2017 р. 2 с.
5. Баранова Е.К. Методики и программноеобеспечение для оценкирисков в сфереинформационнойбезопасности. *Управление риском*. 2009. № 1(49). С. 15-26.
6. Баранова Е.К., Бабаш А.В.Информационнаябезопасность и защитаинформации. М.: ИНФРА-М_РИОР, 2014. 256 с.
7. Безбожний В.Л. Передумови забезпечення соціально-економічної безпеки великих промислових підприємств. *Управління проектами та розвиток виробництва: Зб.наук.пр. – Луганськ: вид-во СНУ ім. В. Даля*, 2013. №1(45). С. 10-15.
8. Большойэкономическийсловарь / под ред. А. Н. Азрилияна. М. : Институтновойэкономики, 2004. - 1376 с.
9. Бурячок В.Л. Інформаційний та кіберпростори: проблеми безпеки, методи та засоби боротьби. К. : ТОВ «СІК ГРУП УКРАЇНА», 2015. 449 с.

10. Гавловський В. Д. Захист інформації шляхом посилення ефективності протидії кібератакам. *Інформація і право*. 2019. № 3(30). С. 105-110.
11. Грищук Р. В. Технологічні аспекти інформаційного протиборства на сучасному етапі. *Захист інформації*. 2015. Т. 17, № 1. С. 80–86.
12. Джумалиева Е. Р. Информационнаякомпетентностькаксоставляющаяпрофессионализмабудущихспециалистов в областиинформационнойбезопасности и защитыинформации. *МНКО*. 2013. № 5. - С. 7-9.
13. Дзьобань О. П. Від "інформаційного суспільства" до "інформаційної безпеки": до проблеми концептуалізації сутності понять. *Інформація і право*. 2019. № 2(29). С. 60-73.
14. Домарев В. В. Безопасностьинформационныхтехнологий. Системныйподход. К. : ООО ТИД ДиаСофт, 2004. 992 с.
15. Дудатьєв А. В. Комплексна інформаційна безпека соціотехнічних систем: моделі впливу та захисту : монографія. Вінниця : ВНТУ, 2017. 128 с.
16. Економічна енциклопедія : в 3 т. Т. 1 // за ред. С. В. Мочерного. К. : Видавничий центр "Академія", 2000. 864 с.
17. Загальні принципи проведення тестування інформаційної безпеки підприємства / О. А. Курченко, М. В. Бржевський, А. Б. Гребенніков, В. І. Корсун // Сучасний захист інформації. 2018. № 4. С. 27-34.
18. Захаренко К. Основні суб'єкти та інститути інформаційної безпеки. *Науковий вісник. Серія «Філософія»*. Харків: ХНПУ. 2017. Вип.48 (частина І). С. 212–219.
19. Звіт про надходження та використання коштів загального фонду (форма № 2 д, № 2 м – додаток 2 до Порядку складання фінансової звітності розпорядниками та одержувачами бюджетних коштів) за 2017 р. КП «Хмельницька міська дитяча лікарня» Хмельницької міської ради. Хмельницький, 2017 р. 2 с.

20. Звіт про надходження та використання коштів загального фонду (форма № 2 д, № 2 м – додаток 2 до Порядку складання фінансової звітності розпорядниками та одержувачами бюджетних коштів) за 2018 р. КП«Хмельницька міська дитяча лікарня» Хмельницької міської ради. Хмельницький, 2018 р. 2 с.
21. Звіт про надходження та використання коштів загального фонду (форма № 2 д, № 2 м – додаток 2 до Порядку складання фінансової звітності розпорядниками та одержувачами бюджетних коштів) за 2019 р. КП «Хмельницька міська дитяча лікарня» Хмельницької міської ради. Хмельницький, 2019 р. 2 с.
22. Звіт про фінансові результати діяльності за 2017 р. КП «Хмельницька міська дитяча лікарня» Хмельницької міської ради. Хмельницький, 2017 р. 2 с.
23. Звіт про фінансові результати діяльності за 2018 р. КП «Хмельницька міська дитяча лікарня» Хмельницької міської ради. Хмельницький, 2018 р. 2 с.
24. Звіт про фінансові результати діяльності за 2019 р. КП «Хмельницька міська дитяча лікарня» Хмельницької міської ради. Хмельницький, 2019 р. 2 с.
25. Информационнаябезопасность. URL: https://ru.wikipedia.org/wiki/Информационная_безопасность.
26. Информационнаятехнология. Методы и средстваобеспечениябезопасности. Свод норм и правил менеджментаинформационнойбезопасности : ГОСТ Р ИСО/МЭК 27002-2012. 2012.
27. Інноваційні технології антикризового управління економічними системами : монографія / С.К. Рамазанов, Г.О. Надьон, Н.І. Кришталь, О.П. Степаненко, Л.А. Тимашова; під ред.. проф. С. К. Рамазанова. Луганськ-Київ: вид-во СНУ ім. В. Даля, 2009. – 584 с.

28. Інформаційна безпека та інформаційні технології : монографія / Альошин Г. В., Герасимов С. В., Засядько А. А. та ін. ; за заг. ред. В. С. Пономаренка. Харків : ТОВ "Діса Плюс", 2019. 322 с. :
29. Керівництво з управління ризиками для систем інформаційних технологій. Рекомендації Національного інституту Стандартів і технологій (GuideforConductingRiskAssessments. NationalInstituteofStandardsandTechnology). Gaithersburg: NationalInstituteofStandardsandTechnology, 200.332, 95 с.
30. Кібераудит: примха чи необхідність? / колектив експертів консалтингової компанії "СІДКОН". *Бизнес и безопасность*. 2019. № 4. С. 7-9.
31. Кіреєнко О. Рекомендації щодо розробки моделі порушника інформаційної безпеки із загальною та спеціалізованою інформацією. *Безпека інформації*. 2019. Т. 25, № 1. С. 24-29.
32. Когут Н. Д. Інформаційна безпека медичній сфері України. *Інформаційна безпека: сучасний стан, проблеми та перспективи: Матеріали І науково-практичної конференції*. 20 вересня 2019 р., м. Київ. / Упоряд. : В. М. Фурашев, С. Ю. Петряєв. Київ : Національний технічний університет України «Київський політехнічний інститут імені Ігоря Сікорського» Вид-во «Політехніка». 2019. С.56-59.
33. Корольов В.Ю. Захист інформації в корпоративних USB-флеш накопичувачах для хмарних обчислень. *Мат. машини і системи.* 2012. № 2. С. 60-69.
34. Курило А.П. Аудит информационнойбезопасности. М.: Издательскаягруппа «БДЦ-пресс», 2006. 420 с.
35. Левченко В.Н.Этапыанализарисков. URL: http://www.cfin.ru/finanalysis/risk/stag- es.shtml
36. Либідь І. В. Методи забезпечення інформаційної інформаційні http://www.rusnauka.com/35_OINBG_2010/Informatica/76346.doc.htm.

37. Лисецкий Ю. М. Комплексна інформаційна безпека корпоративних інформаційних систем. *Управляющиесистемы и машины*. 2019. № 1. С. 68-75.
38. Литвинов В.В. Моделювання та аналіз безпеки розподілених інформаційних систем: навч. пос. [для студ. спец. 121 «Інженерія програмного забезпечення»] / В.В. Литвинов, В.В. Казимир, І.В. Стеценко та ін. Чернігів: Чернігів. нац. технол. ун-т, 2016. 254 с.
39. Ліпкан В.А. Інформаційна безпека України в умовах євроінтеграції: навчальний посібник. К.: КНТ, 2006. 280 с.
40. Манин С.А., Двадненко М.В. Методы и средстваобеспеченияинформационнойбезопасности. *Материалы VIII Международнойстуденческойнаучнойконференции «Студенческийнаучный форум»* URL:http://scienceforum.ru/2016/article/2016019594">http://scienceforum.ru/2016/article/2016019594
41. Маркіна І. А. Основи формування системи менеджменту інформаційної безпеки підприємства. *Проблеми і перспективи розвитку підприємництва*. 2016. № 3(1). С. 80-88
42. Марущак А. Європейський досвід з питань боротьби з правопорушеннями в інформаційній сфері. *Безпека інформації*. 2019. Т. 25, № 1. С. 13-17
43. Медвідь Ф. Інформаційна безпека України: виклики та загрози. *Вісник МАУП.* 2015. № 3. С. 123-130.
44. Международный стандарт ISO/IEC 27000. 3-е изд. URL: http://pqm-online.com/assets/files/lib/std/iso-mek-27000-2014.pdf
45. Мирошниченко М. М. Особливості правового забезпечення інформаційної безпеки держави. *Науковий вісник публічного та приватного права.* 2016. Випуск 2. Том 3. С. 203-208.
46. Нашинець-Наумова А.Ю. Правове регулювання інформаційної безпеки корпорацій. *Правова інформатика.* 2014. №4/44. С. 95-99.

47. Олійник О. В. Принципи забезпечення інформаційної безпеки України. *Юридичний вісник.* №4 (41). 2019. С.72-78.
48. Олійник О.А. Захист інформації в умовах інформаційного суспільства. *Право України.* 2018. № 10. С. 100-103.
49. Олійник О.В. Методологічні засади забезпечення системи інформаційної безпеки та її складової – захисту інформаційних ресурсів. *Право і безпека.* 2019. № 1 (52). С. 103–109.
50. Олійник О.В. Нормативно-правове забезпечення інформаційної безпеки України. *Право і суспільство.* 2017. № 3. С. 132-137.
51. Олійченко І. М. Розвиток інформаційного забезпечення органів державного управління: теорія, методологія, практика : монографія. Ніжин : Аспект-Поліграф, 2010. 432 с.
52. Перун Т.С. Інформаційна безпека суб′єктів господарювання: нові загрози та перспективи розвитку. *Вчені записки ТНУ імені В.І. Вернадського. Серія: юридичні науки*. URL: /http://juris.vernadskyjournals.in.ua/ journals/2020/3_2020/26.pdf
53. Расторгуев С. П. Основыинформационнойбезопасности : учебноепособие. М. : Издательский центр "Академия", 2009. 192 с.
54. Рой Я.В. Аудит інформаційної безпеки –основа ефективного захисту підприємства. URL: http://csecurity.kubg.edu.ua/index.php/ journal/article/view/23/13
55. Ромака В. А. Менеджмент у сфері захисту інформації. Львів : ЗУКЦ, 2013. 462 с.
56. Романюков М. Г. Метод розрахунку оптимальності витрат на інформаційну та кібербезпеку. *Радіоелектроніка, інформатика, управління*. 2019. № 2. С. 167-176.
57. Россошанская О.В. Метод оценкиэкономическойбезопасностиинновационных проектно-ориентированыхпредприятий с позиции метрики

внутреннейсредыдеятельности. *Управління проектами та розвиток виробництва: Зб.наук.пр*. Луганськ: вид-во СНУ ім. В. Даля, 2013. №о 1(45). С. 33-44.

58. Садердинов А. А. Информационнаябезопасностьпредприятия : учебноепособие. М. : Дашков и К, 2005. 125 с.
59. Самохвалов Ю. Я. Оцінка інформаційної безпеки організації за критерієм впевненості. *Захист інформації*. 2019. Т. 21, № 1. С. 13-24.
60. Северина С. В. Інформаційна безпека та методи захисту інформації. Вісник Запорізького національного університету. *Економічні науки*. 2016. № 1. С. 155-161.
61. СредствооценкибезопасностиMicrosoftSecurityAssessmentTool (MSAT). http://technet.microsoft.com/ru-ru/security/cc185712.aspx
62. Статут КП «Хмельницька міська дитяча лікарня» Хмельницької міської ради, затверджений рішенням Хмельницької міської ради від 17.12.2019 р. Хмельницький, 2019, 14 с.
63. Степанов В. Ю. Інформаційнийпростірохорониздоров'я. URL : http://www.kbuapa.kharkov.ua/e-book/tpdu/2016-3/doc/2/01.pdf.
64. СтоєцькийО.В.Адміністративнавідповідальність за правопорушення у сфері інформаційної безпеки України: автореф. дис. на здобуття наукового ступеня кандидат юридичних наук: 12.00.07 «Адміністративне право і процес; фінансове право; інформаційне право». Запоріжжя, 2013. 19 с.
65. Стрельцов А. А. ОбеспечениеинформационнойбезопасностиРоссии. Теоретические и методологическиеосновы. М. : МЦНМО, 2002. 336 с.
66. Стрельцов А. А. Теоретические и методологическиеосновыправового обеспеченияинформационнойбезопасностиРоссии: автореф. дис. на соиск. науч. степени д-ра юрид. наук. М., 2004. 25 с.
67. Стрельцов А.А. Направлениесовершенствования правового обеспеченияинформационнойбезопасностиРоссийскойФедерации. *Информационноеобщество*. 1999. № 6. С. 15-21.

68. Стрельцов А.А. Содержаниепонятия «обеспечениеинформационнойбезопасности». *Информационноеобщество.* 2001. № 4. С.10-16.
69. СубінаТ.В.Адміністративно-правовезабезпечення інформаційної безпеки в органах державної податкової служби України: дис. ... канд. юрид. наук : 12.00.07. Ірпінь, 2010. 219 с.
70. УсР.Л. Аудит інформаційних технологій – новий вид аудиту організацій. *Формування ринкових відносин в Україні*. 2013. № 1. С. 81-86.
71. Феоктистов Г. Г. Информационнаябезопасностьобщества. *Социально-политический журнал.* 1996. № 5. С. 211-212.
72. ХартияЕвропейскогоСоюза об основных правах (2007/C303/01) // Европейский Союз: Основополагающиеакты в редакцииЛиссабонскогодоговора с комментариями; отв. ред. С. Ю. Кашкин. М.: ИНФРА-М, 2010. С. 554-570.
73. Цимбалюк В.С. Інформаційне право: концептуальні положення до кодифікації інформаційного законодавства. К.: Освіта України, 2011. 426 с.
74. Чмир Я. І Проблеми забезпечення інформаційної безпеки в системі публічного управління. *Аспекти публічного правління* Том 6 № 9 2018. С.16-22.
75. Чунарьова А. Система управління інформаційною безпекою на базі міжнародних стандартів серії ISO. *Правове, нормативне та метрологічне забезпечення системи захисту інформації в Україні : науково-технічний збірник*. 2012. Вип. 2(24). С. 48–52.
76. Шатун В. Т. Інформаційна безпека – невід'ємна складова національної безпеки України. *Наукові праці. Державне управління.* 2016. Т. 267. Вип. 255. С.174-180.
77. Шахалов И. Ю. Основыуправленияинформационнойбезопасностьюсовременнойорганиз

ации. URL: https://cyberleninka.ru/article/n/ osnovy-upravleniya-informatsionnoy-bezopasnostyu-sovremennoy-organizatsii

78. Шевченко С.Ю. Формування системи управління інформаційної безпеки підприємства. Економіка підприємства: теорія та практика: зб. мат. IV міжнар. наук.- практ. конф. 12 жовт. 2012р., К.: КНЕУ, 2012. 35 с.
79. Штатний розпис КП «Хмельницька міська дитяча лікарня» Хмельницької міської ради на 2017 р. Хмельницький, 2017 р. 4 с.
80. Штатний розпис КП «Хмельницька міська дитяча лікарня» Хмельницької міської ради на 2018 р. Хмельницький, 2018 р. 4 с.
81. Штатний розпис КП «Хмельницька міська дитяча лікарня» Хмельницької міської ради на 2019 р. Хмельницький, 2019 р. 4 с.
82. Ярочкин В. И. Информационнаябезопасность: учеб. для студ. вузов. М.: Академический Проект; Гаудеамус, 2019. – 544 с.
83. Deming W. Edward. Out of the Crisis: Quality, Productivity, and Competitive Position. – Cambridge (Mass.) Mass. Inst. of Technology, Center for Advanced Engineering Study: Cambridge University Press, 1982.
84. Information technology - Security techniques - Information security management Systems. - Overview and vocabulary : ISO/IEC 27000:2009.2009.
85. Information security // DOD. Dictionary of Military Terms. URL: http://www.dtic.mil/doctrine/dod dictionarv/data/i/10211 .html.
86. ISO/IEC 27001. Informationtechnology – Securitytechniques – Informationsecuritymanagementsystems – Requirements. Firstedition. 2005-10-15
87. ISO/TC 176/SC 2/N 544R2, ISO 9000 Introduction and Support Package: Guidance on the Concept and Use of the Process Approach for management systems, 13 May 2004
88. NIST Special Publication 800-61, Computer Security Incident Handling Guide. Recommendations of the National Institute of Standards and Technology, January 2004.

89. Technical Report ISO/IEC TR 18044, Information technology – Security techniques – Information security incident management.

Виконавстудентмагістратуриспеціальності
073 Менеджмент
заочної форминавчання _____ І.М. Бойко
«____» грудня 2020 р. Підпис Ініціали, прізвище

Науковийкерівник
доцент кафедри
к.е.н., доцент _____ Н.П. Захаркевич
«____»грудня 2020 р. Підпис Ініціали, прізвище

Роботадопущенадозахисту:
завідувачкафедри
д.е.н., професор _____ В.П. Синчак
«____» грудня 2020 р. Підпис Ініціали, прізвище

Додаток А

ПРОЕКТ

Концепція інформаційної безпеки КП «Хмельницька міська дитяча лікарня»

Зміст