

ХМЕЛЬНИЦЬКИЙ УНІВЕРСИТЕТ УПРАВЛІННЯ ТА ПРАВА
ІМЕНІ ЛЕОНІДА ЮЗЬКОВА

ФАКУЛЬТЕТ УПРАВЛІННЯ ТА ЕКОНОМІКИ

Кафедра: менеджменту, економіки, статистики та цифрових технологій

МАГІСТЕРСЬКА РОБОТА

на здобуття освітнього ступеня магістра

на тему:

«Внутрішній контроль за обробкою та реєстрацією медико-діагностичної інформації в закладах охорони здоров'я (на матеріалах КП «Львівське територіальне медичне об'єднання «Клінічна лікарня планового лікування, реабілітації та паліативної допомоги)»

Виконала: студентка магістратури за спеціальністю 073 Менеджмент зі спеціалізацією Організація і управління охороною здоров'я за заочною формою

Лемішко Я.О.

(прізвище та ініціали)

Керівник: доктор економічних наук, професор, професор кафедри

Іжевський П.Г.

(науковий ступінь, вчене звання, прізвище та ініціали)

Рецензент:

(науковий ступінь, вчене звання, прізвище та ініціали)

Анотація

Лемішко Я.О. Внутрішній контроль за обробкою та реєстрацією медико-діагностичної інформації в закладах охорони здоров'я (на матеріалах КП «Львівське територіальне медичне об'єднання «Клінічна лікарня планового лікування, реабілітації та паліативної допомоги»)– Кваліфікаційна наукова праця на правах рукопису. Магістерська робота на здобуття освітнього ступеня магістра за спеціальністю 073 Менеджмент. Хмельницький університет управління та права імені Леоніда Юзькова, Хмельницький, 2023. 68 с.

Магістерська робота присвячена узагальненню теоретичних засад та удосконаленню практичних аспектів внутрішнього контролю за обробкою та реєстрацією медико-діагностичної інформації в КП «Львівське територіальне медичне об'єднання «Клінічна лікарня планового лікування, реабілітації та паліативної допомоги». Визначено, що внутрішній контроль за збереженням медико-діагностичної інформації представляє собою процес отримання об'єктивних оцінок, якісних і кількісних, щодо поточного рівня захисту такої інформації організації відповідно до визначених критеріїв та вимог законодавства. Охарактеризовано нормативно-правові аспекти захисту медико-діагностичної інформації в Україні.

Сформовано комплекс заходів із забезпечення внутрішнього контролю за обробкою та реєстрацією медико-діагностичної інформації в закладі охорони здоров'я. Розглянуто перспективні напрями розвитку системи підтримки прийняття лікарських рішень у медичній інформаційній системі закладу охорони здоров'я на основі медико-діагностичної інформації, що дозволяє істотно покращити якість медичної допомоги та скоротити кількість лікарських помилок. Обґрунтовано, що розробка нових функцій системи СППР та впровадження нових технологій вимагає вдосконалення процесів роботи з медичною інформацією, отже внутрішній контроль має забезпечити гнучкість та легкість впровадження нововведень, ефективний внутрішній аудит та оптимізацію робочих процесів.

Summary

Lemishko Ya.O.

Internal control over the processing and registration of medical and diagnostic information in healthcare institutions (based on the materials of the KP "Lviv Territorial Medical Association "Clinical Hospital of Planned Treatment, Rehabilitation and Palliative Care) - Qualified scientific paper on the basis of copy. Master's degree program for obtaining an open master's degree in the specialty 073 Management. Khmelnytskyi Leonid Yuzkov University of Management and Law, Khmelnytskyi, 2023. 68 p.

The master's thesis is devoted to the generalization of theoretical principles and improvement of practical aspects of internal control over the processing and registration of medical diagnostic information in the KP "Lviv Territorial Medical Association "Clinical Hospital of Planned Treatment, Rehabilitation and Palliative Care". It was determined that internal control over the preservation of medical diagnostic information is a process of obtaining objective assessments, qualitative and quantitative, regarding the current level of protection of such information of the organization in accordance with the defined criteria and requirements of the law. The normative and legal aspects of the protection of medical and diagnostic information in Ukraine are characterized.

A set of measures to ensure internal control over the processing and registration of medical and diagnostic information in the healthcare institution has been formed. Prospective directions for the development of the medical decision-making support system in the medical information system of the healthcare institution based on medical diagnostic information, which allow to significantly improve the quality of medical care and reduce the number of medical errors, are considered. It is substantiated that the development of new functions of the SPPR system and the introduction of new technologies require improvement of the processes of working with medical information, therefore,

internal control should ensure flexibility and ease of introduction of innovations, effective internal audit and optimization of work processes.

ЗМІСТ

ВСТУП	6
РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ ВНУТРІШНЬОГО КОНТРОЛЮ ЗА ОБРОБКОЮ ТА РЕЄСТРАЦІЄЮ МЕДИКО-ДІАГНОСТИЧНОЇ ІНФОРМАЦІЇ В ЗАКЛАДАХ ОХОРОНИ ЗДОРОВ'Я	10
1.1. Поняття та значення внутрішнього контролю за медико-діагностичною інформацією в закладі охорони здоров'я	10
1.2. Нормативно-правові аспекти захисту медико-діагностичної інформації в Україні	15
РОЗДІЛ 2. СУЧАСНИЙ СТАН ОРГАНІЗАЦІЇ СИСТЕМИ ВНУТРІШНЬОГО КОНТРОЛЮ ЗА ОБРОБКОЮ ТА РЕЄСТРАЦІЄЮ МЕДИКО-ДІАГНОСТИЧНОЇ ІНФОРМАЦІЇ КП «ЛЬВІВСЬКЕ ТЕРИТОРІАЛЬНЕ МЕДИЧНЕ ОБ'ЄДНАННЯ «КЛІНІЧНА ЛІКАРНЯ ПЛАНОВОГО ЛІКУВАННЯ, РЕАБІЛІТАЦІЇ ТА ПАЛІАТИВНОЇ ДОПОМОГИ»	20
2.1. Практичні аспекти організації внутрішнього контролю за обробкою та реєстрацією медико-діагностичної інформації в закладі охорони здоров'я	20
2.2. Заходи забезпечення інформаційної безпеки в процесі обробки та реєстрації медико-діагностичної інформації в закладах охорони здоров'я	29
РОЗДІЛ 3. НАПРЯМИ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ВНУТРІШНЬОГО КОНТРОЛЮ ЗА ОБРОБКОЮ ТА РЕЄСТРАЦІЄЮ МЕДИКО-ДІАГНОСТИЧНОЇ ІНФОРМАЦІЇ В ЗАКЛАДІ ОХОРОНИ ЗДОРОВ'Я	40
3.1. Організаційні заходи удосконалення внутрішнього контролю за обробкою та реєстрацією медико-діагностичної інформації в закладі охорони здоров'я	40
3.2. Напрями підтримки прийняття лікарських рішень у медичних інформаційних систем на основі медико-діагностичної інформації	47
ВИСНОВКИ	60
СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ	63
ДОДАТКИ	71

ВСТУП

Актуальність дослідження. В час швидкого розвитку технологій та зростання обсягу медичної інформації, організація внутрішнього контролю за обробкою та реєстрацією цих даних стає критично важливою для забезпечення ефективності та безпеки системи охорони здоров'я. Наявність належного контролю допомагає попереджати помилки та недоліки в обробці медичних даних, що може вплинути на правильність діагнозів та лікування пацієнтів. Збільшення кількості цифрових платформ та електронних медичних записів також ставить питання про безпеку та конфіденційність пацієнтських даних в центр уваги. Несанкціонований доступ до цих даних може призвести до серйозних порушень конфіденційності та потенційно негативних наслідків для пацієнтів. Окрім цього, зростання кількості медичних інформаційних обмінів і міжнародних пацієнтських баз даних вимагає відповідності міжнародним стандартам і законодавчим вимогам. Недотримання цих вимог може призвести до обмежень у співпраці та обміну даними, що має важливе значення для міжнародного співробітництва у сфері медицини. Зазначене обумовило вибір теми дослідження, його мету та завдання.

Серед провідних вітчизняних та зарубіжних дослідників проблематики варто виділити таких: Бем М. В. [4], Копняк К.В. [20], Куперштейн Л.М. [23], Ліпкан В.А. [28], Кнігавко В. Г. [30], Мусієнко А. В. [33], Панасюк А.В. [38], Сопілко І. М. [44], Ясінська Я.О. [23]. Більшість наукових праць присвячується дослідженню інформаційної безпеки організації, правовим основам захисту персональних даних. В той же час розробці практичних аспектів управління внутрішнім контролем за збереженням медичної інформації в закладі охорони здоров'я приділено недостатньо уваги.

Мета і завдання дослідження. Метою дослідження є узагальнення теоретичних засад та удосконалення практичних аспектів внутрішнього контролю за обробкою та реєстрацією медико-діагностичної інформації в

закладі охорони здоров'я.

Визначена мету зумовила необхідність виконання таких завдань:

- визначити сутність та значення внутрішнього контролю за медико-діагностичною інформацією в закладі охорони здоров'я;
- охарактеризувати нормативно-правові аспекти захисту медико-діагностичної інформації в Україні;
- визначити особливості організації внутрішнього контролю за обробкою та реєстрацією медико-діагностичної інформації в закладі охорони здоров'я КП «Львівське територіальне медичне об'єднання «Клінічна лікарня планового лікування, реабілітації та паліативної допомоги»;
- дослідити практичні аспекти забезпечення інформаційної безпеки в процесі обробки та реєстрації медико-діагностичної інформації в закладах охорони здоров'я;
- запропонувати організаційні заходи удосконалення внутрішнього контролю за обробкою та реєстрацією медико-діагностичної інформації в закладі охорони здоров'я;
- визначити напрями підтримки прийняття лікарських рішень у медичних інформаційних систем на основі медико-діагностичної інформації.

Об'єктом дослідження є процеси внутрішнього контролю за обробкою та реєстрацією медико-діагностичної інформації в закладах охорони здоров'я.

Предметом дослідження є теоретичні та практичні аспекти організації внутрішнього контролю за обробкою та реєстрацією медико-діагностичної інформації в КП «Львівське територіальне медичне об'єднання «Клінічна лікарня планового лікування, реабілітації та паліативної допомоги».

Методи дослідження. Теоретичну й методологічну основу роботи становлять наукові праці провідних вітчизняних і зарубіжних вчених з питань пошуку та реалізації шляхів удосконалення внутрішнього контролю за використанням інформації в організації.

У процесі вирішення поставлених завдань використано такі загальні та спеціальні методи наукового дослідження: Теоретичне узагальнення, системний аналіз та синтез були застосовані для розгляду теоретичних аспектів внутрішнього контролю за збереженням медичної інформації. Аналітичний метод та експертне опитування використовувалися для оцінювання рівня захищеності медичної інформації у КП «Львівське територіальне медичне об'єднання «Клінічна лікарня планового лікування, реабілітації та паліативної допомоги». Системний метод використовувався для обґрунтування перспектив розвитку внутрішнього контролю та оцінки ефективності їх реалізації. Абстрактно-логічний метод використовувався для формулювання теоретичних узагальнень та висновків, отриманих у результаті 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 країн, локальні акти внутрішнього контролю за збереженням медичної інформації. Емпіричну базу дослідження становлять статистичні матеріали, що характеризують стан інформаційної безпеки та внутрішнього контролю за збереженням медичної інформації, довідкові видання, наукові публікації з досліджуваної проблематики.

Апробація результатів дослідження. Деякі положення та результати магістерської роботи були оприлюднені на Міжнародній науково-практичній конференції «Сучасні виклики та напрями вдосконалення в економічній та технічній наукових сферах» (5-6 грудня 2023 року, м. Запоріжжя)[26].

Практичне значення одержаних результатів полягає в узагальненні теоретичних основ внутрішнього контролю за обробкою та реєстрацією

медико-діагностичної інформації в закладах охорони здоров'я, опрацюванні конкретних пропозицій щодо удосконалення управління і цій сфері.

РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ ВНУТРІШНЬОГО КОНТРОЛЮ ЗА ОБРОБКОЮ ТА РЕЄСТРАЦІЄЮ МЕДИКО-ДІАГНОСТИЧНОЇ ІНФОРМАЦІЇ В ЗАКЛАДАХ ОХОРОНИ ЗДОРОВ'Я

1.1. Поняття та значення внутрішнього контролю за медико-діагностичною інформацією в закладі охорони здоров'я

Організація внутрішнього контролю за обробкою та реєстрацією медико-діагностичної інформації стає надзвичайно актуальною у сучасному світі охорони здоров'я. Зі зростанням обсягу медичних даних і використанням сучасних інформаційних технологій, важливо забезпечувати надійну обробку та збереження цієї інформації. Це стосується не лише якості діагностики та лікування, але й безпеки пацієнтів і їхньої конфіденційності. У зв'язку із зростанням загроз кібербезпеці, дотримання відповідних стандартів та законодавчих вимог стає надзвичайно важливим аспектом в управлінні медичною інформацією. Недотримання цих вимог може призвести до суттєвих проблем, включаючи витіки конфіденційної інформації та порушення прав пацієнтів. Організація внутрішнього контролю також допомагає вдосконалити якість надання медичних послуг і оптимізувати процеси в охороні здоров'я. Вона дозволяє виявляти і усувати можливі помилки та неефективності в обробці медичної інформації. Крім того, враховуючи швидкий розвиток сучасних технологій і збільшення обсягу медичних даних, організація внутрішнього контролю стає необхідною для забезпечення якості, безпеки і конфіденційності медичної інформації, що є ключовими аспектами сучасної системи охорони здоров'я. Термін «медико-діагностична інформація» вказує на інформацію, яка стосується результатів медичних досліджень, діагностики та тестувань, що проводяться для визначення стану здоров'я пацієнта, встановлення діагнозів і вибору методів лікування [30, с.34]. Ця інформація включає в себе результати лабораторних аналізів, зображення з медичних обстежень, структуровані клінічні дані,

анамнези пацієнтів та інші медичні записи.

Медико-діагностична інформація є важливою для прийняття медичних рішень, планування лікування та спостереження за пацієнтами. Вона може бути представлена у різних форматах, включаючи текстові описи, числові дані, зображення (наприклад, рентгенограми, МРТ, УЗД), електрокардіограми та інші облікові записи. Зберігання та обробка медико-діагностичної інформації вимагає великої уваги до конфіденційності, цілісності та безпеки даних, оскільки ця інформація містить особисті медичні дані пацієнтів і має велике значення для їхнього здоров'я і лікування [31]. Внутрішній контроль є важливим аспектом у сфері медико-діагностичної інформації. Це система, яка дозволяє відстежувати та контролювати процес обробки та реєстрації медичних даних в медичних закладах. Завдання організації системи внутрішнього контролю за обробкою та реєстрацією медико-діагностичної інформації у закладі охорони здоров'я відображено на рис. 1.1.



Рисунок 1.1. Систематизація завдань організації системи внутрішнього контролю на підприємстві за обробкою та реєстрацією медико-діагностичної

інформації у закладі охорони здоров'я

Примітка. Систематизовано автором.

Внутрішній контроль за обробкою та реєстрацією медико-діагностичної інформації є важливим елементом забезпечення якості медичної допомоги. Він спрямований на виявлення та усунення недоліків у роботі з медичною інформацією, запобігання її втраті або несанкціонованому доступу.

Внутрішній контроль за обробкою та реєстрацією медико-діагностичної інформації здійснюється уповноваженими особами медичної організації. Вони мають право [33, с.18]:

отримувати доступ до медичної інформації;

проводити перевірку правильності її обробки та реєстрації;

вимагати від працівників медичної організації усунення виявлених недоліків.

Об'єктами внутрішнього контролю є [41, с18]:

наявність та стан нормативно-правової бази, що регулює обробку та реєстрацію медико-діагностичної інформації;

порядок організації та здійснення обробки та реєстрації медико-діагностичної інформації;

наявність та стан технічних засобів, що використовуються для обробки та реєстрації медико-діагностичної інформації;

рівень кваліфікації працівників, які здійснюють обробку та реєстрацію медико-діагностичної інформації.

При проведенні перевірки внутрішнього контролю перевіряються такі питання [46]:

чи здійснюється обробка та реєстрація медико-діагностичної інформації відповідно до вимог нормативно-правової бази;

чи забезпечено конфіденційність медичної інформації;

чи вживаються заходи щодо запобігання втраті або несанкціонованому доступу до медичної інформації;

чи забезпечується достовірність та повнота медичної інформації.

За результатами перевірки внутрішнього контролю складається акт, у якому зазначаються виявлені недоліки та рекомендації щодо їх усунення. Акт підписується уповноваженою особою, яка проводила перевірку, та керівником медичної організації. У разі виявлення значних недоліків у роботі з медичною інформацією керівник медичної організації зобов'язаний вжити заходів щодо їх усунення. Внутрішній контроль за обробкою та реєстрацією медико-діагностичної інформації є важливим інструментом забезпечення якості медичної допомоги та захисту прав пацієнтів.

На основі вищенаведеного, можемо запропонувати наступне визначення: внутрішній контроль за обробкою та реєстрацією медико-діагностичної інформації - це система процедур, політик та практик, спрямованих на забезпечення правильності, цілісності, конфіденційності та доступності медичних даних та інформації про пацієнтів. Ця система призначена для мінімізації помилок в обробці даних, захисту від несанкціонованого доступу та забезпечення відповідності вимогам законодавства та стандартів у галузі охорони здоров'я.

Методи та інструменти внутрішнього контролю за обробкою та реєстрацією медико-діагностичної інформації (МДІ) спрямовані на виявлення та усунення недоліків у роботі з МДІ, запобігання її втраті або несанкціонованому доступу. До методів внутрішнього контролю за обробкою та реєстрацією МДІ відносяться [23]:

документальний контроль - перевірка наявності та стану нормативно-правової бази, що регулює обробку та реєстрацію МДІ, а також документів, що регламентують порядок її здійснення;

аналітичний контроль - аналіз даних про обробку та реєстрацію МДІ, виявлення тенденцій, закономірностей та відхилень;

інспектування - проведення перевірок дотримання вимог нормативно-правової бази, порядку організації та здійснення обробки та реєстрації МДІ, а також стану технічних засобів та рівня кваліфікації працівників, які здійснюють ці процеси;

тестування - перевірка правильності роботи програмного забезпечення, що використовується для обробки та реєстрації МДІ;

опитування - збір інформації від працівників медичної організації про їхні знання та навички щодо обробки та реєстрації МДІ, а також про виявлені ними недоліки.

До інструментів внутрішнього контролю за обробкою та реєстрацією МДІ відносяться [2, с.14]:

чек-ліст - перелік питань, які необхідно перевірити під час проведення внутрішнього контролю;

інструкція - документ, що регламентує порядок проведення внутрішнього контролю;

акт перевірки - документ, що складається за результатами проведення внутрішнього контролю.

Вибір методів та інструментів внутрішнього контролю за обробкою та реєстрацією МДІ залежить від конкретних умов медичної організації.

Одним із ефективних методів внутрішнього контролю за обробкою та реєстрацією МДІ є проведення регулярних аудитів. Аудити проводяться незалежними фахівцями, які мають досвід роботи у сфері охорони здоров'я. Вони оцінюють відповідність роботи медичної організації вимогам нормативно-правової бази, ефективності заходів щодо запобігання втраті або несанкціонованому доступу до МДІ.

Важливим елементом внутрішнього контролю за обробкою та реєстрацією МДІ є навчання працівників медичної організації. Працівники повинні бути ознайомлені з вимогами нормативно-правової бази, порядку організації та здійснення обробки та реєстрації МДІ, а також з правилами захисту конфіденційності медичної інформації [11].

Внутрішній контроль за обробкою та реєстрацією МДІ є важливим інструментом забезпечення якості медичної допомоги та захисту прав пацієнтів. Важливою метою внутрішнього контролю є забезпечення високого рівня захищеності медичної інформації та збереження її цілісності для

надання надійної та етичної медичної практики.

1.2. Нормативно-правові аспекти захисту медико-діагностичної інформації в Україні

Інформаційні технології (ІТ) та засоби комунікації, що розвиваються стрімкими темпами, створюють сприятливі передумови прискорення процесів інформатизації у вітчизняній охороні здоров'я. Завдяки впровадженню у повсякденну практику охорони здоров'я дедалі більшої кількості електронних сервісів та послуг, вже сьогодні є підстава називати її електронною охороною здоров'я (e-health) [54]. З усього різноманіття існуючих визначень, на думку авторів, найбільш коректно електронну охорону здоров'я визначити як сукупність інформаційно-комунікаційних технологій (ІКТ), спрямованих на вдосконалення потоку інформації медичного змісту з метою підтримки надання медичних послуг та управління системою охорони здоров'я.

Використання автоматизованих інформаційних технологій у медичних установах є однією з найбільш актуальних тем у сфері охорони здоров'я останнім часом. Середньостатистичну лікарню або поліклініку великого міста щодня відвідують сотні пацієнтів. Лікарі, у свою чергу, щодня заповнюють сотні всіляких амбулаторних карт, медичних бланків та іншої документації, що негативно позначається як на швидкості прийому лікарем пацієнтів, так і на якості створення та заповнення всієї документації, оскільки ресурси будь-якого лікаря обмежені. Медичні інформаційні системи покликані вирішити цю проблему, і, принаймні, частково позбавити тих, хто лікує лікарів від паперової роботи. Це дозволить вивести якість прийому пацієнтів на новий рівень. Також відвідати лікаря зможе більша кількість пацієнтів за день, що безперечно позитивним чином позначиться на якості охорони здоров'я країни.

Згідно даних Міністерства охорони здоров'я України, електронні системи зберігання медичних даних виявляються більш захищеними

порівняно з паперовими медичними картками в медичних закладах. Один із прикладів такої системи в Україні - eHealth, яка впроваджує найсучасніші засоби захисту. Вона включає в себе можливість використання кваліфікованих електронних підписів (КЕР) користувачами, відокремлене зберігання медичних та особистих даних, а також використання алгоритмів для забезпечення цілісності даних [1]. Більше того, система також має офіційний атестат відповідності стандартам комплексної системи захисту інформації (КСЗІ) згідно з державними вимогами щодо захисту інформації [55].

В межах роботи закладів охорони здоров'я відбувається акумулювання величезної кількості персональних даних громадян, що регулюється Законом України «Про захист персональних даних» [39], Законом України «Про основні засади забезпечення кібербезпеки України» [40], Постановою Кабінету Міністрів України «Деякі питання електронної системи охорони здоров'я» від 25.04.2018 р. №411 [8].

Відповідно до Закону України «Про захист персональних даних», персональні дані – це відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована. Тобто до персональних даних належить вся інформація, що підлягає внесенню в декларацію про вибір лікаря первинної медичної допомоги, а саме: прізвище, ім'я, по батькові, дата народження, РНОКПП, дані документа, що посвідчує особу, адреса проживання, засоби зв'язку [39]. Українське законодавство також містить положення про відповідальність за порушення вимог роботи з персональними даними пацієнтів. Мова йде про адміністративну та кримінальну відповідальність. Наразі функції контролю за виконанням законодавства у сфері захисту персональних даних належать Уповноваженому Верховної Ради України з прав людини, в межах Секретаріату якого створений Департамент у сфері захисту персональних даних [4].

Вступ України до ЄС передбачає гармонізацію українського

законодавства з законодавством ЄС, у тому числі і в галузі захисту персональних даних. Гармонізація українського законодавства до європейських стандартів у сфері захисту персональних даних шляхом імплементації Регламенту Європейського Парламенту та Ради про захист фізичних осіб у зв'язку з обробкою персональних даних і про вільний рух таких даних 2016/679 (Загальний регламент про захист персональних даних) є одним із ключових завдань України відповідно п. 11 Плану заходів з виконання Угоди про асоціацію, затвердженого постановою Кабінету Міністрів України від 25.10.2017 р. №1106, яке досі залишається невиконаним.

Український медичний бізнес, який пропонує послуги (товари) резидентам ЄС або здійснює моніторинг поведінки суб'єктів даних, розташованих в ЄС, автоматично потрапляє до сфери дії Загального регламенту про захист даних №2016/679, або GDPR (далі – GDPR, Регламент) [43]. Багато іноземців надають перевагу, наприклад, українському медичному туризму, зокрема, через приємні ціни (ледь не вдвічі нижча вартість, ніж у європейських країнах) та високу якість надання медичних послуг. У медичному туризмі України лідирують такі галузі як стоматологія, офтальмологія, репродукція, неврологія, кардіологія, клітинна терапія, реабілітація [13].

GDPR встановлює жорсткі вимоги щодо захисту персональних даних, у тому числі даних про здоров'я. Зокрема, GDPR вимагає від володільців персональних даних, у тому числі медичних закладів, вживати всіх необхідних заходів для забезпечення їхньої конфіденційності, цілісності та доступності. Ці вимоги значно підвищують відповідальність медичних закладів за організацію внутрішнього контролю за обробкою та реєстрацією медико-діагностичної інформації [35].

GDPR передбачає можливість для контролюючих органів у сфері захисту персональних даних країн-членів ЄС накладати санкції екстериторіально, в тому числі на території України. Таким чином,

правозастосування GDPR є неминучим. Регламент передбачає фундаментальні зміни щодо збору, обробки, володіння та передачі даних про здоров'я. Тепер пацієнти повинні надати згоду на використання своїх даних про стан здоров'я та можуть її відкликати, коли це необхідно, або навіть видалити. Насправді це є новелою у світі, адже, наприклад, у США давно поширеною була практика медичних організацій зберігати дані пацієнтів на невизначений термін. Відповідно до GDPR, громадянин ЄС може попросити заклад охорони здоров'я видалити медичні записи про себе за певних обставин, а йому не можуть в цьому відмовити.

Існують три типи персональних даних, які особливо актуальні для галузі охорони здоров'я [39]:

дані, що стосуються здоров'я відповідно до GDPR – це будь-які дані, які стосуються фізичного чи психічного здоров'я людини, що включає також будь-яку інформацію, пов'язану з типом допомоги, яку отримав пацієнт;

генетичні дані – це будь-які дані (характеристики), які можуть виявити деталі фізіології або здоров'я пацієнта, а також будь-які результати лабораторних досліджень;

біометричні дані – це будь-які дані, пов'язані з певними фізичними або поведінковими характеристиками людини (наприклад, зображення обличчя, відбитки пальців, риси ходи тощо), які можна використати для ідентифікації конкретної особи.

Тобто ще раз варто підкреслити, що GDPR встановлює значно вищі стандарти стосовно інформованої згоди пацієнта, яка має містити тип персональних даних, які збиратимуться, пояснювати, як вони будуть використовуватися (пацієнта потрібно інформувати про можливі ризики збору даних «у зрозумілій та легкодоступній формі, чіткою та зрозумілою мовою»), а також включати поле для підтвердження або відмови пацієнта [32, с.47].

Згідно з GDPR, є дві особи, відповідальні за обробку персональних даних – контролер та процесор. Контролером називають особу (фізичну чи

юридичну) або орган державної влади, які визначають ціль та мету обробки персональних даних. Процесором є особа чи орган державної влади, що здійснює обробку персональних даних відповідно до мети та цілей, встановлених контролером. Наприклад, лікарня, яка збирає інформацію – це контролер, а власник програмного продукту, в якому зберігаються та обробляються дані, медпрацівники, які технічно вносять дані в електронну систему – це процесори (обробники) даних.

Саме контролер і процесор несуть солідарну відповідальність у випадку порушень GDPR та зобов'язані повідомляти контролюючі органи, а в окремих випадках і суб'єктів даних, про будь-які порушення (витік, викрадення, несанкціонований доступ тощо), пов'язані з персональними даними, протягом 72 годин після встановлення такого порушення. Необхідність дотримання українськими медичними установами положень

GDPR у найближчому майбутньому є неминучою. Тому вже сьогодні потрібно готуватися до більш жорстких та високих вимог щодо захисту такої чутливої категорії персональних даних як інформація про здоров'я, що обумовлює необхідність удосконалення організації внутрішнього контролю за обробкою та реєстрацією медико-діагностичної інформації в вітчизняних закладах охорони здоров'я.

РОЗДІЛ 2. СУЧАСНИЙ СТАН ОРГАНІЗАЦІЇ СИСТЕМИ ВНУТРІШНЬОГО КОНТРОЛЮ ЗА ОБРОБКОЮ ТА РЕЄСТРАЦІЄЮ МЕДИКО-ДІАГНОСТИЧНОЇ ІНФОРМАЦІЇ КП «ЛЬВІВСЬКЕ ТЕРИТОРІАЛЬНЕ МЕДИЧНЕ ОБ'ЄДНАННЯ «КЛІНІЧНА ЛІКАРНЯ ПЛАНОВОГО ЛІКУВАННЯ, РЕАБІЛІТАЦІЇ ТА ПАЛІАТИВНОЇ ДОПОМОГИ»

2.1. Практичні аспекти організації внутрішнього контролю за обробкою та реєстрацією медико-діагностичної інформації в закладі охорони здоров'я

КП «Львівське територіальне медичне об'єднання «Клінічна лікарня планового лікування, реабілітації та паліативної допомоги» Львівської міської ради (далі – КП «Львівське територіальне медичне об'єднання «Клінічна лікарня планового лікування, реабілітації та паліативної допомоги») є закладом охорони здоров'я - комунальним унітарним некомерційним підприємством, що надає первинну медичну допомогу та здійснює управління медичним обслуговуванням населенню міста Львова, вживає заходи з профілактики захворювань та підтримання громадського здоров'я. У ТМО «Клінічна лікарня планового лікування, реабілітації та паліативної допомоги» об'єднано чотири міські лікарні:

«Львівська 1-а міська клінічна лікарня імені Князя Лева»,

«4-а міська клінічна лікарня Львова»,

«5-а міська клінічна лікарня Львова»

«Лікарня «Госпіс» Львова».

з профілактики захворювань та підтримання громадського здоров'я.

КП «Львівське територіальне медичне об'єднання «Клінічна лікарня планового лікування, реабілітації та паліативної допомоги» створене з метою надання первинної медичної допомоги та здійснення управління медичним обслуговуванням населення, що постійно проживає (перебуває) на території

міста Львова, а також вжиття заходів з профілактики захворювань населення та підтримки громадського здоров'я.

Структура підприємства, порядок внутрішньої організації та сфери діяльності структурних підрозділів підприємства затверджуються Директором. Функціональні обов'язки та посадові інструкції працівників підприємства затверджуються його керівником. Організаційна структура КП «Львівське територіальне медичне об'єднання «Клінічна лікарня планового лікування, реабілітації та паліативної допомоги» відображено у додатку А.

Внутрішній контроль за обробкою та реєстрацією медико-діагностичної інформації 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 [24]. Призначення системи внутрішнього контролю за обробкою та реєстрацією медико-діагностичної інформації КП «Львівське територіальне медичне об'єднання «Клінічна лікарня планового лікування, реабілітації та паліативної допомоги» 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 внутрішнього контролю за обробкою та реєстрацією медико-діагностичної інформації КП «Львівське територіальне медичне об'єднання «Клінічна лікарня планового лікування, реабілітації та паліативної допомоги» обумовлюються його призначенням і полягають у:

- забезпеченні безпечного, надійного зберігання і передачі інформації в електронному та друкованому вигляді, розташованій на різних носіях;
- організації надійного доступу до інформації;
- обмеження і контроль доступу до інформації, з якою працюють працівники, 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 внутрішнього контролю за обробкою та реєстрацією медико-діагностичної інформації КП «Львівське територіальне медичне об'єднання «Клінічна лікарня планового лікування, реабілітації та паліативної допомоги» а 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 внутрішнього контролю за збереженням інформації 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 [44].

Внутрішній контроль за обробкою та реєстрацією медико-діагностичної інформації органу охорони здоров'я відображає захищеність інформаційного середовища та ефективність інформаційного забезпечення процесу управління в установі [1; 14].

Процес забезпечення внутрішнього контролю за обробкою та реєстрацією медико-діагностичної інформації 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 безпеки обробки та реєстрації медико-діагностичної інформації КП «Львівське територіальне медичне об'єднання «Клінічна лікарня планового лікування, реабілітації та паліативної допомоги» необхідне систематичне виконання наступних етапів (рис. 2.1.):

- аналіз загроз збереженню інформації;
- планування та розробка заходів щодо забезпечення внутрішнього контролю за збереженням інформації;
- оперативна реалізація запланованих дій.

Функції щодо внутрішнього контролю за обробкою та реєстрацією медико-діагностичної інформації КП «Львівське територіальне медичне об'єднання «Клінічна лікарня планового лікування, реабілітації та паліативної допомоги» розподілено між керівником, керівниками відокремлених підрозділів, їх заступниками та інформаційно-аналітичним відділом медичного закладу. Основний перелік функції щодо інформатизації та захисту інформації закладу охорони здоров'я покладено на інформаційно-аналітичний відділ КП «Львівське територіальне медичне об'єднання «Клінічна лікарня планового лікування, реабілітації та паліативної допомоги».

Інформаційно-аналітичний відділ КП «Львівське територіальне медичне об'єднання «Клінічна лікарня планового лікування, реабілітації та паліативної допомоги» 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 «Львівське територіальне медичне об'єднання «Клінічна лікарня планового лікування, реабілітації та паліативної допомоги» .

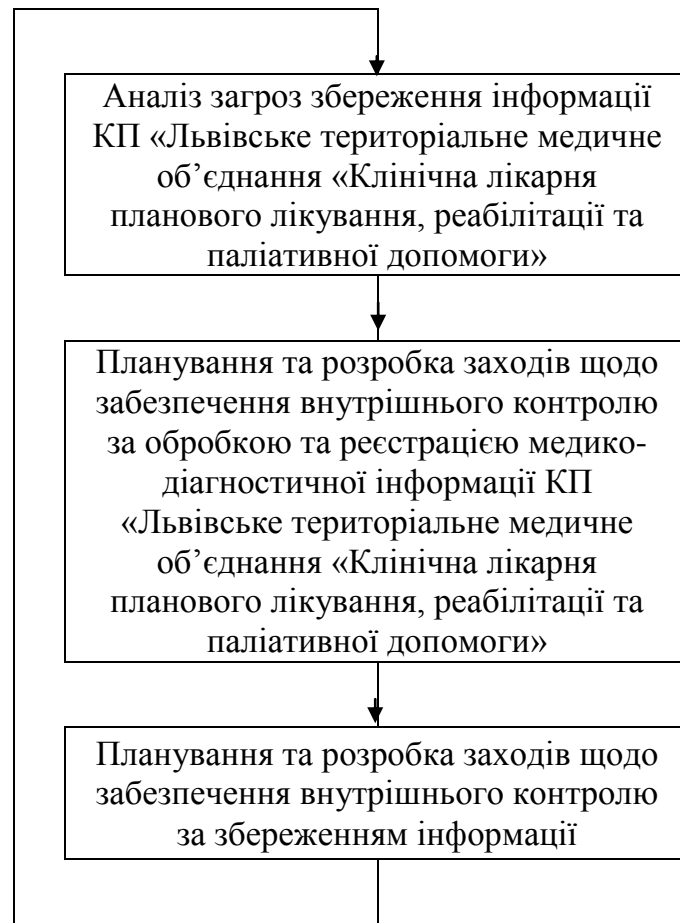


Рисунок 2.1 - Схема функціонування системи внутрішнього контролю за обробкою та реєстрацією медико-діагностичної інформації КП «Львівське територіальне медичне об'єднання «Клінічна лікарня планового лікування, реабілітації та паліативної допомоги»

Примітка. Складено автором.

Відділ у своїй діяльності керується Конституцією України, законами України, Указами Президента України, постановами Кабінету Міністрів України, наказами МОЗ України, начальника Бюро, та іншими нормативно-правовими актами України, а також Положенням про відділ.

Відділ підпорядкований начальнику. 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 інформаційно-аналітичного відділу КП «Львівське територіальне медичне об'єднання «Клінічна лікарня планового лікування, реабілітації та паліативної допомоги» є:

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

2.Централізований збір медико-статистичної та адміністративної інформації від підрозділів лікарні, обробка та аналіз інформації.

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

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

Опишемо більш детально функціональні повноваження інформаційно-аналітичної відділу КП «Львівське територіальне медичне об'єднання «Клінічна лікарня планового лікування, реабілітації та паліативної допомоги». 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 такого відділу (кабінету).

Відповідно до вимог вищевказаних стандартів у територіальному медичному об'єднанні передбачено наявність: інформаційно-аналітичного відділу у штатному розписі; положення про відділ; посадових інструкцій всіх працівників відділу, у тому числі працівників відділу, звільнених із роботи за останні п'ять років; табеля оснащення та паспорта відділу; переліку працівників відділу з визначенням відповідального за окремий розділ роботи та взаємозаміну працівників у разі відпустки, курсів, хвороби; планів роботи відділу та кожного працівника за останні три роки із позначками про виконання.

Відповідно до статті 9 Закону України «Про інформацію» від 02.10.1992 № 2657XII основними видами інформаційної діяльності є

створення, збирання, одержання, зберігання, використання, поширення, охорона та захист інформації. У цьому ж законі (ст. 18) міститься визначення статистичної інформації — це документована інформація, що дає кількісну характеристику масових явищ та процесів, які відбуваються в економічній, соціальній, культурній та інших сферах життя суспільства.

Одним із завдань інформаційно-аналітичного відділу КП «Львівське територіальне медичне об'єднання «Клінічна лікарня планового лікування, реабілітації та паліативної допомоги» , передбачених Наказом № 592, 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 «Львівське територіальне медичне об'єднання «Клінічна лікарня планового лікування, реабілітації та паліативної допомоги» 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 звірення інформації з первинною документацією осіб, а також строки подання інформації, осіб, яким надається інформація, споживачів та особу, що аналізує інформацію; схему взаємодії відділу з трирівневим джерелом інформації; схему інформаційного медичного статистичного забезпечення закладу; схему руху директивної інформації.

Однією із функцій інформаційно-аналітичного відділу КП «Львівське територіальне медичне об'єднання «Клінічна лікарня планового лікування, реабілітації та паліативної допомоги» є інформування керівників

структурних підрозділів про результати аналізу даних щодо діяльності закладу охорони здоров'я. Начальник або його заступники можуть використати статистичну інформацію для: поточного та перспективного планування роботи закладу охорони здоров'я (фінансового, організаційного, клінічного); здійснення ефективного адміністративного контролю та оперативного керівництва службами і окремими підрозділами закладу охорони здоров'я; вивчення різних форм надання медичної допомоги населенню та оцінювання ефективності проведення оздоровчих заходів; оцінювання ефективності прийнятих управлінських рішень.

За підсумками збирання та оброблення первинної медичної документації інформаційно-аналітичний відділ КП «Львівське територіальне медичне об'єднання «Клінічна лікарня планового лікування, реабілітації та паліативної допомоги» надає адміністрації закладу аналітичні таблиці з висновками щодо роботи підрозділів та окремих служб, щоквартально узагальнює і аналізує державні та галузеві звітні форми, передає звіти про роботу закладу охорони здоров'я до регіонального медико-статистичного аналітичного центру. Кожний завідувач підрозділу отримує аналітичну таблицю за підсумками роботи свого підрозділу.

Під час аналізу діяльності інформаційно-аналітичний відділ КП «Львівське територіальне медичне об'єднання «Клінічна лікарня планового лікування, реабілітації та паліативної допомоги» поєднує показники у групи, характеризуючи певний напрям діяльності, розділ роботи, підрозділ закладу або контингент населення, яке обслуговує заклад. При проведенні статистичної ревізії лікар-статистик відділу має змогу перевірити наявність директивних і регламентувальних документів та розроблених заходів щодо їх виконання у конкретному підрозділі, наявність бланків первинної медичної документації, правильність оформлення первинної медичної документації персоналом закладу, особисто пояснити медичним працівникам необхідність ведення певної форми первинної медичної

документації. Підсумки проведення статистичної ревізії оформлюють у вигляді акту та надають адміністрації закладу.

Виконання функцій контролю за впровадженням і використанням територіального медичного об'єднання форм державної та галузевої статистичної звітності, передбаченої чинним законодавством, працівниками організаційно-методичного відділу КП «Львівське територіальне медичне об'єднання «Клінічна лікарня планового лікування, реабілітації та паліативної допомоги» здійснюється шляхом забезпечення своєчасного та якісного складання і подання до обласних медико-статистичних аналітичних центрів системи Міністерства охорони здоров'я України державних та галузевих статистичних звітів та отримання результатів діяльності закладу охорони здоров'я. При складанні та поданні звітів працівники відділу керуються наказом Міністерства охорони здоров'я України «Про подання установами і закладами охорони здоров'я України статистичних звітів».

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, внутрішній контроль за обробкою та реєстрацією медико-діагностичної інформації медичного закладу здійснюється організаційно-методичним відділом КП «Львівське територіальне медичне об'єднання «Клінічна лікарня планового лікування, реабілітації та паліативної допомоги», 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. Заходи забезпечення інформаційної безпеки в процесі обробки та реєстрації медико-діагностичної інформації в закладах охорони здоров'я

Високий рівень захищеності інформації 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.

Забезпечення інформаційної безпеки в процесі обробки та реєстрації медико-діагностичної інформації в закладах охорони здоров'я є критично важливим завданням для збереження конфіденційності, цілісності та доступності медичних даних. Враховуючи особливості цієї сфери, основні заходи забезпечення в процесі обробки та реєстрації медико-діагностичної інформації в КП «Львівське територіальне медичне об'єднання «Клінічна лікарня планового лікування, реабілітації та паліативної допомоги» включають (табл.2.1):

Таблиця 2.1. Заходи внутрішнього контролю за обробкою та реєстрацією медико-діагностичної інформації

Критерії внутрішнього контролю	Опис заходів контролю	Відповідальна особа	Регулярність перевірок
Захист конфіденційності	Проведення аудитів доступу до медичних даних; Застосування шифрування при передачі і зберіганні інформації; Введення правил обмеженого доступу.	інформаційно-аналітичний відділ, Відповідальний за ІБ	Раз на півроку
Забезпечення цілісності	Використання автоматизованих систем для виявлення помилок; Проведення регулярних перевірок наявності дублювання даних; Оновлення програмного та апаратного забезпечення.	інформаційно-аналітичний відділ, відповідальний за ІБ	Щомісячно
Системи виявлення вторгнень	Встановлення та підтримка систем виявлення вторгнень; Постійний моніторинг мережі на підозрілу активність.	інформаційно-аналітичний відділ, Відповідальний за ІБ	Постійно
Аудит інформаційної безпеки	Проведення регулярних аудитів стану інформаційної безпеки; Виявлення та усунення потенційних порушень.	внутрішній аудитор, відповідальний за ІБ	Раз на рік
Навчання персоналу	Проведення регулярних навчань з інформаційної безпеки; Підготовка персоналу до виявлення та запобігання загрозам.	аналітичний відділ, відповідальний за ІБ	Раз на рік, позапланово за потреби
Передача даних та програмного забезпечення	Визначення і дотримання правил щодо використання програмного забезпечення; Контроль передачі медичної інформації за допомогою електронного зв'язку, забезпечення згоди пацієнтів на передачу їхніх даних.	аналітичний відділ, відповідальний за ІБ	Раз на півроку
Резервне копіювання та відновлення	Проведення систематичних резервних копіювань даних; Перевірка можливості відновлення з резервних копій; Забезпечення доступу тільки авторизованим особам до резервних копій.	аналітичний відділ, відповідальний за ІБ	Регулярно, згідно з графіком
Використання системи аудиту та моніторингу	Впровадження систем аудиту та моніторингу для фіксації дій персоналу та виявлення незвичайної активності; Періодична перевірка журналів аудиту та реагування на виявлені аномалії.	аналітичний відділ, відповідальний за ІБ	Щоденно, позапланово за потреби

Примітка. Систематизовано автором.

1. Застосування шифрування для захисту конфіденційної інформації під час її передачі та зберігання. Це включає шифрування файлів, баз даних та комунікаційних каналів. В досліджуваному закладі передача конфіденційної інформації відбувається шляхом використання електронних засобів зв'язку, цифрових носіїв або у паперовій формі. Передача цієї інформації відбувається під час виконання службових обов'язків від однієї особи до іншої. Особа, яка отримала конфіденційну інформацію, зобов'язана зберігати її відповідно до умов, визначених постачальником цієї інформації. Усі члени персоналу повинні розуміти чутливий характер медичних та особистих даних, отриманих закладом у ході його діяльності, і утримуватися від розголошення такої інформації. Будь-яке навмисне розголошення конфіденційних даних, до яких працівник має доступ, вважається порушенням, що може призвести до наказу і, можливо, юридичної відповідальності перед порушеним.

2. Передача даних та програмного забезпечення. Використання програмного забезпечення, яке не отримало затвердження для використання в закладі, заборонено на робочих станціях, комп'ютерах та в локальній мережі КП «Львівське територіальне медичне об'єднання «Клінічна лікарня планового лікування, реабілітації та паліативної допомоги». Якщо виникає необхідність у використанні конкретного програмного забезпечення, користувач повинен подати запит на отримання дозволу своєму безпосередньому керівнику. Використання програмного забезпечення, встановленого на робочих станціях, особистих комп'ютерах чи комп'ютерному обладнанні під час дистанційної роботи без належного дозволу, заборонено.

Дані, які є власністю лікарні, включаючи медико-діагностичну інформацію про пацієнтів, ІТ-системи, фінансову інформацію чи дані про людські ресурси, не повинні знаходитися на будь-якому комп'ютері, який не є власністю лікарні, без письмової згоди відповідного керівника.

3. Контроль доступу - становлення систем контролю доступу, які обмежують доступ до медичної інформації тільки авторизованим особам. Це може включати в себе ідентифікацію та аутентифікацію користувачів. Вимоги безпеки для ідентифікації користувача включають наступне:

кожному користувачеві надається унікальний обліковий запис;

користувачі несуть відповідальність за правомірне та неправомірне використання свого індивідуального облікового запису користувача.

Усі облікові записи користувачів перевіряються принаймні один раз на рік, і всі неактивні облікові записи користувача блокуються. Відділ кадрів лікарні повідомляє відповідального за інформаційну безпеку або відповідного фахівця ІТ-відділу про звільнення працівника або припинення співробітництва з персоналом підрядника. Після отримання такого сповіщення неактивні облікові записи блокуються. Обліковий запис автоматично блокується після трьох невдалих спроб входу в систему. Щоб відновити доступ у цьому випадку, необхідно звертатися до адміністратора.

Користувачі інформаційних ресурсів лікарні при працевлаштуванні підписують угоду про конфіденційність. Тимчасово влаштовані працівники та підрядники, які не підписували угоди про конфіденційність, підписують такий документ при отриманні доступу до інформаційних ресурсів лікарні.

4. Обмеження доступу до персональних даних. У закладі запроваджено процес класифікації особистих даних, де збір таких даних відбувається лише на підставі особистої згоди або у випадках, визначених чинним законодавством, і обмежується цілями та обсягом, визначеними відповідно до згоди чи законодавства. Обробка та зберігання особистих даних відбуваються лише протягом необхідного часу для досягнення заданих цілей. Послідовно виконуються такі процедури:

отримання згоди фізичних осіб на збір особистих даних;

надання доступу до особистих даних;

обробка та зберігання особистих даних;

безпечна передача особистих даних третім особам;

деперсоналізація особистих даних;
безпечне видалення особистих даних;
обробка запитів та претензій від осіб щодо обробки їхніх особистих даних, а також експорт та імпорт даних;
повідомлення про інциденти несанкціонованого доступу чи цілісності особистих даних.

Доступ до особистих даних надається обмеженій групі осіб, а їх експорт обмежено за межами захищеної системи чи сервісу. Доступ на базі службових обов'язків забезпечується в частині медичного обслуговування пацієнтів. Експорт великої кількості особистих даних можливий лише за погодженням керівництва.

Місце збереження особистих даних, включаючи медичні, зведено до мінімуму для зменшення вразливості перед кіберзагрозами. ІТ-процеси та архітектура періодично переглядаються для поліпшення захисту особистих даних. Доступ до особистих даних надається мінімально необхідній кількості працівників, а передача таких даних третім сторонам дозволяється лише за наявності згоди пацієнта чи відповідно до законодавства. Всі процеси, пов'язані з третіми сторонами, чітко визначають ролі та обов'язки володільця та розпорядника даних. Після досягнення мети обробки особисті дані деперсоналізуються або безпечно видаляються, включаючи медичні дані. Процес затвердження доступу до інформаційних систем включає перевірку відповідності політиці захисту особистих даних пацієнтів. Всі процедури та місце збереження особистих даних задокументовані та регулярно оновлюються відповідно до змін в інформаційних системах, процесах та законодавстві з питань захисту особистих даних.

5. Захист фізичного доступу до інформаційних ресурсів, таких як серверні приміщення, дата-центри та комп'ютерні системи, що передбачає такі заходи:

вхід до адміністративних приміщень будівлі в неробочий період закритий та піддаваний контролю з боку охорони;

особа, яка не є визнаною, і перебуває в службових приміщеннях Лікарні під час неробочого часу, має бути негайно виведена з робочої зони персоналом, який її виявив, та супроводжена до охоронного пункту;

серверне та мережеве обладнання оснащено основним і резервним безперебійним живленням;

будівля обладнана відеокамерами спостереження на входах та виходах, фіксуючи всі особи, які входять чи виходять протягом 24 годин на добу, 365 днів на рік;

протипожежний захист будівлі встановлено відповідно до стандартів Державної служби з надзвичайних ситуацій України.

6. Використання системи аудиту та моніторингу для виявлення неповноважних або підозрілих активностей. Це дозволяє оперативно реагувати на можливі загрози безпеки. У КП «Львівське територіальне медичне об'єднання «Клінічна лікарня планового лікування, реабілітації та паліативної допомоги» регулярно, один раз на рік, здійснюється аудит стану інформаційної безпеки, що включає, але не обмежується, такими заходами як перевірка облікових записів користувачів та їх прав доступу до ІТ-систем і мереж, перевірка доступу до файлів, аналіз інцидентів безпеки, а також перегляд журналів моніторингу. Аудит може бути проведений як внутрішнім персоналом Лікарні, так і залученням зовнішніх аудиторів. Головна мета аудиту - зниження ризику порушень безпеки та забезпечення належного рівня інформаційної безпеки Лікарні.

7. Резервне копіювання та відновлення. В лікарні здійснюється регулярне створення резервних копій медичних даних та розробка планів відновлення після аварій для забезпечення доступності даних у випадку непередбачених ситуацій. В закладі впроваджені заходи та процедури реагування на надзвичайні події, які можуть завдати шкоди ІТ-системам та мережам, а також інформації. Для цього розроблений План аварійного відновлення та План резервного копіювання. Заклад періодично (один раз на

рік) переглядає цей план з метою аналізу його ефективності та оцінки ризиків для внесення відповідних корегувань.

8. Навчання та освіта персоналу. В закладі відбувається систематичне проведення навчань для медичного персоналу та інших працівників щодо правил і процедур інформаційної безпеки, а також створення свідомості щодо можливих загроз. Навчання з інформаційну безпеку для всього персоналу проводиться раз на рік, або позапланово при необхідності. Відповідальний за інформаційну безпеку організовує та проводить навчання з інформаційної безпеки. Відвідування та/або участь у такому навчанні є обов'язковим для всього персоналу. Відповідальний за інформаційну безпеку веде відповідну документацію про всі навчальні заходи. Відповідальний з інформаційної безпеки, при необхідності, може організовувати позапланові навчання при змінах у апаратному або програмному забезпеченні, збільшені загроз, внесені змін у політику інформаційної безпеки, за результатами аудиту, тощо.

Таким чином, КП «Львівське територіальне медичне об'єднання «Клінічна лікарня планового лікування, реабілітації та паліативної допомоги» впроваджує та утримує відповідні організаційні та технологічні заходи для підтвердження того, що медичні дані пацієнтів та інша конфіденційна інформація, пов'язана з пацієнтами, не піддавались несанкціонованим змінам чи знищенню. Головною метою цих заходів є забезпечення цілісності даних пацієнтів. Заклад використовує автоматизовані системи та програмне забезпечення, включаючи штучний інтелект, для автоматичної перевірки можливості людських помилок при обробці даних пацієнтів. Для виявлення можливих вторгнень застосовуються відповідні мережеві та хост-системи. Відповідальна особа за інформаційну безпеку забезпечує встановлення, контроль обслуговування та оновлення таких систем.

Збереження цілісності даних у медичних інформаційних системах здійснюється провайдерами цих систем. Для забезпечення цілісності даних

при їх передачі використовується шифрування, і також шифрування використовується при зберіганні цих даних.

Заклад ретельно перевіряє можливе дублювання даних у своїх комп'ютерних системах та мережах, щоб уникнути некоректної інтеграції даних між різними системами.

З метою запобігання можливим збоєм в ІТ-системах, які можуть призвести до порушення цілісності даних, заклад проводить перевірку інформаційних систем на їх точність та функціональність перед використанням. ІТ-системи та мережеве обладнання регулярно оновлюються з випуском виробниками виправлень та оновлених версій програмного та апаратного забезпечення для усунення виявлених помилок та недоліків.

КП «Львівське територіальне медичне об'єднання «Клінічна лікарня планового лікування, реабілітації та паліативної допомоги» встановлює та періодично оновлює антивірусне програмне забезпечення на всіх робочих станціях та серверах, щоб своєчасно виявляти та запобігати зміні або знищенню даних шкідливим програмним забезпеченням.

Оцінювання рівня захищеності медико-діагностичної інформації в закладі охорони здоров'я є комплексним підходом, який враховує організаційно-методичне та технічне забезпечення внутрішнього контролю. При оцінці дієвості внутрішнього контролю враховується ефективність заходів, спрямованих на збереження медичної інформації та управління ризиками її втрати чи несанкціонованого доступу. Крім того, оцінка включає перевірку компетентності персоналу, який працює з медико-діагностичною інформацією, забезпечуючи високий ступінь надійності та конфіденційності цих даних. У зв'язку із зазначеним пропонуємо наступні напрями оцінювання рівня захищеності медико-діагностичної інформації в КП «Львівське територіальне медичне об'єднання «Клінічна лікарня планового лікування, реабілітації та паліативної допомоги» (табл. 2.2).

Експертне оцінювання є одним з ключових методів оцінки рівня захищеності медико-діагностичної інформації в закладі охорони здоров'я.

Цей підхід базується на залученні кваліфікованих експертів, які мають глибокі знання в галузі інформаційної безпеки та роботи з медичною інформацією.

Таблиця 2.2. Результати оцінювання рівня захищеності медико-діагностичної інформації в КП «Львівське територіальне медичне об'єднання «Клінічна лікарня планового лікування, реабілітації та паліативної допомоги»

Напрямок оцінки	Оцінка (1-5)	Примітка
Оцінка організаційно-методичного забезпечення	4	
Визначення політик та процедур захисту медичної інформації	4	Існує положення про інформаційну безпеку, але доцільно чітко визначити відповідальності персоналу за дотримання політик, а також врегулювати випадки з обміном медичної інформації з іншими установами
Наявність та відповідність стандартам технічного захисту	5	Всі технічні заходи відповідають сучасним стандартам.
Захищення від втрати та несанкціонованого доступу до інформації	4	Механізми захисту існують, необхідне регулярне оновлення та аудит існуючих заходів для відповідності сучасним стандартам та найновішим загрозам в галузі інформаційної безпеки.
Оцінка дієвості внутрішнього контролю	4,7	
Регулярне тестування та аудит систем безпеки	5	Систематичні перевірки ефективності контрольних заходів.
Швидкість виявлення та реагування на інциденти	4	Доцільно розробити більш детальні процедури виявлення та створити швидкі канали комунікації для ефективного спілкування між відповідальними структурами під час інцидентів..
Ефективність заходів з криптографічного захисту	5	Шифрування ефективно використовується у всіх аспектах.
Оцінка компетенцій персоналу	4	
Рівень навчання та оновлення знань персоналу з інформаційної безпеки	4	Регулярне оновлення, розширити теми занять для більш широкого охоплення сучасних загроз, визначити конкретні критерії успішності для перевірки знань, а також врахувати можливість індивідуальних програм навчання для різних груп персоналу
Компетенція персоналу у виявленні та реагуванні на інциденти	4	Хоча персонал виявляє високий рівень компетенції у виявленні та реагуванні на інциденти, можливість подальшого удосконалення може включати проведення додаткових тренувань та симуляційних вправ для ще більш ефективної реакції в надзвичайних ситуаціях
Своєчасне та вірне застосування процедур захисту інформації	4	Більшість персоналу своєчасно та вірно дотримується процедур.

Примітка. Систематизовано автором за даними анкетування.

Експерти проводять детальний аналіз організаційно-методичного та технічного забезпечення внутрішнього контролю, визначають його дієвість у збереженні медико-діагностичної інформації та виявленні загроз її безпеці. Вони також оцінюють компетенції персоналу, перевіряючи їх здатність ефективно взаємодіяти з системами обробки даних та забезпечувати конфіденційність інформації. Експертне оцінювання дозволяє отримати об'єктивний погляд на рівень захищеності медичної інформації, ініціювати необхідні зміни та вдосконалення в системі безпеки та забезпечити відповідність високим стандартам у сфері охорони здоров'я.

В закладі охорони здоров'я внутрішніми експертами з інформаційної безпеки можуть бути спеціалізовані фахівці, які мають глибокі знання та досвід у сфері інформаційної безпеки та обробки медичної інформації. Відповідно нами для оцінювання було залучені наступні категорій фахівців в якості внутрішніх експертів: адміністратор баз даних з медичною експертизою, фахівець із з інформаційної безпеки.

Отже, використання запропонованого підходу до аналізу стану захищеності інформації в КП «Львівське територіальне медичне об'єднання «Клінічна лікарня планового лікування, реабілітації та паліативної допомоги» дозволило не лише виявити рівень захищеності установи, але й визначити шляхи підвищення ефективності використання інформаційних ресурсів та уточнити напрями посилення захисту медичної інформації. Після впровадження заходів з підвищення ефективності захисту медичної інформації, такий процес оцінювання рекомендується провести повторно.

Належний рівень інформаційної безпеки, це такий стан фізичного, інформаційного середовища та середовища користувачів інформаційних та цифрових активів лікарні, який гарантує конфіденційність, доступність, цілісність інформації лікарні та спостережність і контрольованість систем/підсистем, в яких ця інформація циркулює. Належний рівень

інформаційної безпеки досягається за рахунок вмілого застосування комплексу програмних/технічних засобів та організаційних заходів, спрямованих на забезпечення захищеності даних від зловмисного використання.

РОЗДІЛ 3. НАПРЯМИ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ВНУТРІШНЬОГО КОНТРОЛЮ ЗА ОБРОБКОЮ ТА РЕЄСТРАЦІЄЮ МЕДИКО-ДІАГНОСТИЧНОЇ ІНФОРМАЦІЇ В ЗАКЛАДІ ОХОРОНИ ЗДОРОВ'Я

3.1. Організаційні заходи удосконалення внутрішнього контролю за обробкою та реєстрацією медико-діагностичної інформації в закладі охорони здоров'я

Проблема внутрішнього контролю за обробкою та реєстрацією медико-діагностичної інформації в закладі охорони здоров'я дійсно стає дуже актуальною, особливо враховуючи значну чисельність персоналу та розгалужену структуру закладу. Здійснення як клінічних, так і управлінських бізнес-процесів пов'язано із обробкою та реєстрацією значного масиву медико-діагностичної інформації. У зв'язку з цим необхідним є розробка та впровадження медичних інформаційних систем, що забезпечить реалізацію наступних завдань [37; 49]:

розробка стандартизованих процедури та протоколи для обробки та реєстрації медичної інформації. Це допоможе уникнути недорозуміння та помилок при обробці даних;

впровадження сучасних систем ЕМІ може спростити збір, збереження та обмін медичною інформацією між відділеннями та співробітниками. Це також допоможе покращити доступність даних та їхню точність;

навчання та підвищення кваліфікації з питань обробки медичної інформації можуть забезпечити, що персонал правильно використовує системи та дотримується процедур;

проведення аудитів та періодичний контроль за обробкою даних може виявити можливі проблеми та допомогти вчасно їх виправити;

визначення відповідальних осіб та створення внутрішніх комітетів чи

груп, які будуть відповідати за контроль та вдосконалення процесів обробки інформації;

забезпечення безпеки та конфіденційності медичної інформації є надзвичайно важливим аспектом, особливо в умовах розгалуженої структури закладу;

автоматизація та інформаційні технології, використання сучасних технологій, таких як штучний інтелект та аналітика даних, може покращити якість обробки інформації та допомогти виявляти та передбачати можливі проблеми;

створення ефективних механізмів співпраці та комунікації між різними відділеннями та рівнями управління.

Завданням керівництва закладу є визначення пріоритетів та виділення ресурсів для вирішення цих проблем. Тільки впровадження комплексних заходів та систематична робота над покращенням внутрішнього контролю можуть допомогти забезпечити ефективну обробку та реєстрацію медичної інформації в такому великому та розгалуженому закладі охорони здоров'я.

Вдосконалення внутрішнього контролю за обробкою та реєстрацією медико-діагностичної інформації в закладі охорони здоров'я вимагає комплексного підходу та впровадження різноманітних заходів. Ці заходи повинні бути спрямовані на забезпечення [38]:

Достовірності, повноти та своєчасності обробки та реєстрації медико-діагностичної інформації. Це означає, що інформація повинна бути правильною, повною та доступною вчасно.

Захист медико-діагностичної інформації від несанкціонованого доступу, використання, модифікації або знищення. Медико-діагностична інформація є конфіденційною та повинна бути захищена від несанкціонованого доступу.

Виявлення та усунення порушень вимог законодавства, нормативно-правових актів МОЗ України, а також внутрішніх документів закладу охорони здоров'я. Внутрішній контроль повинен забезпечувати виявлення та

усунення будь-яких порушень у сфері обробки та реєстрації медико-діагностичної інформації.

Комплексний підхід до удосконалення внутрішнього контролю передбачає впровадження організаційних, технічних та кадрових заходів [29].

Організаційні заходи спрямовані на розробку та впровадження внутрішніх документів, що регулюють обробку та реєстрацію медико-діагностичної інформації, а також на навчання персоналу закладу охорони здоров'я правилам і процедурам обробки та реєстрації медико-діагностичної інформації [18].

Технічні заходи спрямовані на використання сучасних інформаційних технологій для обробки та реєстрації медико-діагностичної інформації, а також на встановлення системи захисту інформації від несанкціонованого доступу, використання, модифікації або знищення [19].

Кадрові заходи спрямовані на формування в закладі охорони здоров'я культури дотримання вимог законодавства та внутрішніх документів у сфері обробки та реєстрації медико-діагностичної інформації [36].

Сформуємо комплекс заходів вдосконалення внутрішнього контролю за обробкою та реєстрацією медико-діагностичної інформації в закладі охорони здоров'я, що дозволить створити чітку і злагоджену систему організації роботи з кадрами, здатну захистити інформацію та інформаційні системи закладу (табл.3.1).

Внутрішній контроль за обробкою та реєстрацією медико-діагностичної інформації в закладі охорони здоров'я повинен 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 [3, с.82].

Таблиця 3.1 Організаційні заходи удосконалення внутрішнього контролю за обробкою та реєстрацією медико-діагностичної інформації в КП «Львівське територіальне медичне об'єднання «Клінічна лікарня планового лікування, реабілітації та паліативної допомоги»

Захід	Необхідні процедури	Результат	Витрати
1	2	3	4
1. Розробка та впровадження внутрішніх документів, що регулюють обробку та реєстрацію медико-діагностичної інформації.	- створення робочої групи з розробки внутрішніх документів; - аналіз чинного законодавства та нормативно-правових актів у сфері охорони здоров'я; - розробка проектів внутрішніх документів; - затвердження внутрішніх документів керівником закладу охорони здоров'я.	Уніфікація процедур обробки та реєстрації медико-діагностичної інформації. Покращення ефективності внутрішнього контролю.	доплати до заробітної плати за здійснення аудиту чи оплата послуг зовнішнього аудитора.
2. Організація тренінгів для персоналу інформаційно-аналітичного відділу	- розробка програми тренінгу, включаючи теоретичні та практичні аспекти роботи інформаційно-аналітичного відділу; - Проведення практичних занять та симуляцій інцидентів. Визначення критеріїв успішності та оцінка засвоєння матеріалу.	Підвищення кваліфікації та компетентності персоналу.	Витрати на тренерів, оренду приміщення, матеріали та обладнання для тренінгів.
3. Впровадження системи корпоративних носіїв інформації (захищені флеш-накопичувачі)	- встановлення програмного забезпечення на усі комп'ютери, що блокує використання стороннього флеш-накопичувача.; - закупівля корпоративних носіїв інформації	Підвищення рівня безпеки зберігання та передачі інформації.	Витрати на закупівлю та налаштування програмного забезпечення, закупівлю корпоративних накопичувачів.
4. Організація навчання персоналу з питань захисту інформації	- визначення посад і структурних підрозділів, які повинні пройти навчання; - складання планів та графіків навчання; - визначення організаторів (персонал інформаційно-аналітичного відділу або запрошені фахівці); - проведення занять; - перевірка знань.	Формування моделі поведінки працівників на конкретні загрози та запобігання витоку інформації, включаючи особисті дані працівників та пацієнтів.	Витрати на розробку планів навчання, зарплату організаторам та тренерам.
5. Розвиток цифрових компетенцій	- визначення вимог і критеріїв оцінки цифрових навичок, консультації з представниками різних відділів; - розробка методик тестування, проведення оцінювання	Створення уніфікованого стандарту цифрових компетенцій, який буде враховувати потреби всіх відділів	Витрати на навчальні матеріали, заробітну плату тренерам

Продовж.табл.3.1

1	2	3	4
6. Здійснення інформаційного аудиту інформаційних систем закладу охорони здоров'я	- визначення об'єктів аудиту, розробка методик та плану аудиту; - аналіз результатів інформаційного аудиту; - співставлення зі стандартами безпеки, визначення пріоритетів для усунення виявлених проблем; - впровадження рекомендацій з інформаційного аудиту; - моніторинг інформаційної безпеки після впровадження змін	Виявлення слабких місць та потенційних загроз інформаційній безпеці, підготовка рекомендацій для подальших вдосконалень. Постійний контроль за рівнем та своєчасна реакція на події	Витрати на розробку системи моніторингу, підготовку персоналу
7. Розробка процедури розгляду скарг і заяв на порушення вимог законодавства щодо захисту персональних даних, нормативно-правових актів МОЗ України, а також внутрішніх документів закладу охорони здоров'я	- аналіз вимог законодавства, внутрішніх нормативів, розробка структури процедури; - створення системи контролю та аналіз показників, аудит процедури; - впровадження змін у процедуру з урахуванням результатів моніторингу; - моніторинг та оцінка ефективності	Забезпечення своєчасного та ефективного розгляду скарг і заяв на порушення вимог законодавства, нормативно-правових актів МОЗ України, а також внутрішніх документів закладу охорони здоров'я	Витрати на розробку системи моніторингу, підготовку персоналу

Примітка. Складено автором.

Впровадження цих заходів дозволить забезпечити належний рівень внутрішнього контролю за обробкою та реєстрацією медико-діагностичної інформації в закладі охорони здоров'я.

Навчання персоналу закладу охорони здоров'я правилам і процедурам обробки та реєстрації медико-діагностичної інформації є одним з важливих напрямків удосконалення внутрішнього контролю за цими процесами. Метою навчання є забезпечення персоналу необхідними знаннями та навичками для належного виконання своїх обов'язків у сфері обробки та реєстрації медико-діагностичної інформації. Навчання персоналу повинно включати в себе такі теми [36]:

правове регулювання обробки та реєстрації медико-діагностичної інформації;

порядок обробки та реєстрації медико-діагностичної інформації;
правила захисту медико-діагностичної інформації від несанкціонованого доступу, використання, модифікації або знищення;
практичні навички обробки та реєстрації медико-діагностичної інформації;

Вибір способу навчання залежить від масштабів закладу охорони здоров'я, а також від потреб персоналу. Навчання персоналу має бути регулярним, оскільки правила і процедури обробки та реєстрації медико-діагностичної інформації можуть змінюватися. Важливо, щоб навчання персоналу проводилося кваліфікованими спеціалістами, які мають досвід роботи в сфері охорони здоров'я. Ефективність навчання персоналу можна оцінити за такими критеріями:

знання персоналу правил і процедур обробки та реєстрації медико-діагностичної інформації;

практичні навички персоналу в галузі обробки та реєстрації медико-діагностичної інформації;

дотримання персоналом правил і процедур обробки та реєстрації медико-діагностичної інформації в процесі роботи.

Навчання персоналу закладу охорони здоров'я правилам і процедурам обробки та реєстрації медико-діагностичної інформації є важливим заходом, який сприяє забезпеченню належного рівня внутрішнього контролю за цими процесами.

Слід наголосити, цифрова трансформація охорони здоров'я в даний час стала світовою тенденцією. Розробники ІТ-технологій та продуктів створюють нові рішення для підвищення доступності медичних послуг та підвищення їх ефективності. В останні кілька років у медичній практиці активно використовуються електронні пристрої, що дозволяють віддалено контролювати показники здоров'я пацієнтів, проводити онлайн-консультації та відеоконференції. Прискорена комп'ютерна аналітика великих обсягів інформації підвищує рівень якості діагностики та лікування різних

захворювань. Цифрові медичні технології змінюють поширені раніше моделі споживання медичних послуг, формують нові способи створення «цінності» на основі медицини «чотирьох П» (Предиктивна, Профілактична, Персоналізована та Пацієнтоорієнтована), яка базується саме на мобільній медицині і неможлива без тісної співпраці між пацієнтом та лікарем з використанням цифрових технологічних рішень [22].

Персоналізація передбачає індивідуальний підхід до пацієнта на основі аналізу його генетичних та фізіологічних особливостей з використанням новітніх наукових розробок.

Предикція має на увазі виявлення схильностей конкретної людини до виникнення того чи іншого захворювання (прогноз здоров'я) на основі виділення факторів ризику та визначення ступеня ймовірності розвитку захворювання.

Превентивність - ключовий принцип усієї концепції, суть якого полягає у зниженні ризику розвитку захворювання або в повному його запобіганні на основі комплексу профілактичних заходів, розроблених під конкретну людину з урахуванням її індивідуальних особливостей.

Партисипативність передбачає залучення пацієнта до процесу надання медичної послуги, прийняття ним відповідальності за своє здоров'я, мотивування до профілактики.

У секторі приватних медичних послуг широко застосовуються такі сервіси, як вибір лікаря та запис на прийом, особистий кабінет пацієнта, персональні медичні карти, отримання другої думки (у тому числі закордонного фахівця), віддалений моніторинг стану здоров'я, формування рейтингів клінік та медичного персоналу на основі відгуки пацієнтів.

Найбільш значущим напрямом цифровізації за своїм впливом на ефективність діяльності медичної установи є цифровізація зберігання, обміну та обробки медичних даних. В даний час для встановлення вірного діагнозу лікар використовує доступний йому обсяг знань про стан здоров'я пацієнта, інформацію про потенційні захворювання і спирається на свій досвід.

Удосконалення збору медичної статистики та збільшення обчислювальних потужностей та поширення технологій обробки та аналізу «великих даних» (BigDataAdvancedAnalytics) зумовили затребуваність когнітивної аналітики. Розвиток та вдосконалення технологій когнітивного аналізу сприятиме підвищенню якості діагностики та зниженню витрат на її проведення, а також скорочення економічних втрат, пов'язаних із лікарськими помилками та низькою ефективністю лікування при пізній або неправильній постановці діагнозу. Зазначене обумовлює необхідність формування напрямів удосконалення медичних інформаційних систем в діяльності закладів охорони здоров'я.

3.2. Напрями підтримки прийняття лікарських рішень у медичних інформаційних систем на основі медико-діагностичної інформації

Сучасний рівень розвитку медичної науки надає у розпорядження лікуючого лікаря тисячі різноманітних діагностичних і лікувальних методик, лікарських засобів та багато іншого. У їх практичному застосуванні лікарю доводиться враховувати різні чинники: показання та протипоказання методики або способу лікування, особливості пацієнта та перебігу захворювання, сумісність або посилення впливу тих чи інших методів обстеження або лікарських препаратів один на одного, індивідуальну лікарську непереносимість у пацієнта, протипоказання та багато іншого. В результаті, під час прийому пацієнта з урахуванням високого навантаження лікарю доводиться при призначенні обстеження та лікуванні брати до уваги всі ці особливості, будувати свою роботу на підставі досвіду, знань, клінічного уявлення про хворого та багатотомних клінічних посібників.

Все це тримати в пам'яті і приймати без помилкових, правильних і своєчасних рішень стає все складнішим і складнішим. Причому ситуація стрімко посилюється тим, що обсяг знань у медицині зростає лавиноподібно, а час на прийняття лікарем відповідного рішення при цьому не збільшується.

Зростає кількість лікарських помилок, які призводять до різних негативних явищ – від зниження ефективності роботи систем охорони здоров'я до зростання смертності.

У лікарнях США щодня реєструють близько 40 тис. випадків заподіяння шкоди здоров'ю пацієнтів внаслідок лікарських помилок, що становить близько 15 млн. таких випадків на рік [51]. Жертвами помилок, пов'язаних з неправильним вживанням ліків, стають півтора мільйони американців. Близько 7 тис. з них помирають через недогляд медиків і фармацевтів. За даними Інституту Медицини, що входить до структури Національної Академії наук США (Institute of Medicine of the National Academy of Science), збитки сягають 3,5 млрд. доларів [49]. У Європейському Союзі (ЄС) у кожному десятому випадку звернення за медичною допомогою ставлять помилковий діагноз або призначають неправильне лікування [47]. Згідно з даними Комісії ЄС, у Німеччині щороку від лікарських помилок помирають близько 25 тис. німців. Щорічно у країні відзначають до 100 тис. випадків помилок діагностики, неправильного призначення ліків та інших дефектів надання медичної допомоги [50].

Одним з найбільш перспективних та ефективних методів запобігання таким помилкам є впровадження у клінічну практику різних ІТ-рішень. Їхнє основне завдання полягає в аналізі та запобіганні діям, здатних завдати шкоди життю та здоров'ю пацієнта. Основне завдання медичних інформаційних систем (МІС) на поточному етапі – це перехід на переважне ведення електронних медичних карт пацієнтів (ЕМК), накопичення первинної медичної інформації в електронному вигляді та автоматизація базових завдань, таких як скорочення непрофільних витрат медичного персоналу на ведення документації, автоматичне формування медичної статистики, автоматизація обліку лікарських засобів і т.д. Завдання найближчого майбутнього – це розвиток МІС в інтелектуального помічника лікаря, включаючи впровадження клінічних посібників, автоматичний

контроль якості медичної допомоги та інші напрямки, здатні істотно покращити якість медичної допомоги, що надається та скоротити кількість лікарських помилок, тобто мова йде про систему підтримки прийняття лікарських рішень.

Система підтримки прийняття лікарських рішень (СППР) – це програмне забезпечення, що дозволяє шляхом збору та аналізу медико-діагностичної інформації впливати на прийняття лікарем рішення під час обстеження пацієнта, діагностики, призначення лікування з метою зниження помилок та підвищення якості медичної допомоги». Далі розглянемо різні приклади реалізації функцій системи підтримки прийняття лікарських рішень у медичній інформаційній системі закладу охорони здоров'я (табл.3.2).

Таблиця 3.2. Перспективні напрями розвитку системи підтримки прийняття лікарських рішень у медичній інформаційній системі закладу охорони здоров'я на основі медико-діагностичної інформації

Напрямок підтримки	Призначені функції	Очікуваний результат
1	2	3
Ведення електронної медичної картки	Зберігання основної пацієнтської інформації, такої як особисті дані, історія хвороб, результати обстежень. Можливість додавання та оновлення медичних записів у реальному часі. Доступ пацієнтів та лікарів до актуальної та повної інформації..	Забезпечення доступу до повної та актуальної інформації про пацієнта для лікарів та медичного персоналу.
Довідково-бібліотечні функції	Забезпечення доступу до медичних довідників, стандартів та літератури. Актуалізація та підтримка бібліотеки з наукових статей, клінічних вказівок та рекомендацій. Пошук інформації з використанням ключових слів та фільтрів.	Підвищення рівня інформованості медичного персоналу, забезпечення доступу до актуальної медичної інформації.
Формування «інтегрального анамнезу»	Збір та агрегація інформації з різних джерел для створення повного анамнезу пацієнта. Автоматичне оновлення анамнезу при додаванні нових даних. Відображення інтегрального анамнезу у зручному та зрозумілому форматі.	Покращення обґрунтування прийняття рішень на основі повного медичного контексту пацієнта.
Автоматизація лікарських призначень	Електронне формування та зберігання лікарських призначень. Попередження про можливі взаємодії	Забезпечення точності та своєчасності призначень, уникнення

	між ліками та алергічні реакції. Відстеження виконання лікарських призначень та їх ефективності.	помилки у лікуванні.
--	--	----------------------

Продовж.табл.3.2

1	2	3
Автоматичний контроль за вимогами нормативно-правових актів	Визначення та виконання лікарських дій у відповідності з чинним законодавством та стандартами. Автоматичне оновлення системи відповідно до змін в законодавстві. Ведення аудиту для перевірки відповідності нормативам.	Забезпечення відповідності лікарської практики чинним законодавчим нормам.
Автоматичний контроль «клінічного мінімуму»	Система, що перевіряє відповідність медичних дій установленим клінічним стандартам. Сповіщення про можливі невідповідності та рекомендації для досягнення клінічного мінімуму. Забезпечення надання стандартної медичної допомоги.	Забезпечення надання медичної допомоги відповідно до визначених стандартів та клінічних протоколів.
Автоматична підтримка клінічних посібників	Інтеграція та використання клінічних довідників та стандартів. Використання системи для підтримки прийняття лікарських рішень у відповідності з клінічними стандартами. Оновлення посібників згідно з останніми дослідженнями та медичною практикою.	Підтримка лікарів у виборі оптимального лікування, відповідно до актуальних клінічних рекомендацій.
Автоматичний контроль критеріїв якості медичної допомоги	Визначення критеріїв якості медичної допомоги відповідно до стандартів. Система моніторингу та сповіщення про невідповідності. Забезпечення постійного вдосконалення процесів для досягнення встановлених критеріїв..	Забезпечення високого рівня якості медичної допомоги та виявлення можливих покращень.

Примітка. Запропоновано автором.

Представлені перспективні напрями розвитку системи підтримки прийняття лікарських рішень у медичній інформаційній системі закладу охорони здоров'я на основі медико-діагностичної інформації можуть сприяти підвищенню ефективності системи внутрішнього контролю за обробкою та реєстрацією медико-діагностичної інформації. Так, використання системи підтримки прийняття лікарських рішень (зокрема штучного інтелекту) може підвищити точність діагностики, що призведе до зменшення кількості помилок у медичних висновках. Це, своєю чергою, сприятиме підвищенню

якості медичної допомоги та безпеки пацієнтів. Крім того, використання ШІ може автоматизувати деякі процеси обробки та реєстрації медико-діагностичної інформації, що може зменшити ризик людських помилок. Доступність СППР для всіх лікарів, незалежно від їхнього місця розташування, може сприяти підвищенню якості та доступності медичної допомоги. Це, своєю чергою, може призвести до зменшення кількості помилок у процесах обробки та реєстрації медико-діагностичної інформації. СППР можна використовувати для навчання персоналу правилам та процедурам обробки та реєстрації медико-діагностичної інформації. Наприклад, СППР можна використовувати для симуляції різних сценаріїв обробки та реєстрації інформації, щоб персонал міг навчитися розпізнавати та уникати помилок.

В той же час, розробка нових функцій системи СППР та впровадження нових технологій може вимагати вдосконалення процесів роботи з медичною інформацією (рис.3.1).



Рисунок 3.1. Взаємодія між системою внутрішнього контролю та системою підтримки прийняття лікарських рішень

Примітка. Запропоновано автором.

Система внутрішнього контролю має забезпечити ефективний внутрішній аудит та оптимізацію робочих процесів. Також, розробка та впровадження нових функцій системи підтримки прийняття лікарських рішень вимагає валідації та тестування. Система внутрішнього контролю має забезпечувати ефективне тестування, яке гарантує правильність та надійність програмних засобів. Обидві системи повинні підтримувати адаптацію до швидкого темпу технологічних змін у галузі охорони здоров'я та інформатики. Внутрішній контроль має забезпечити гнучкість та легкість впровадження нововведень.

Комплексний підхід до автоматизації системи обробки та реєстрації медико-діагностичної інформації в КП «Львівське територіальне медичне об'єднання «Клінічна лікарня планового лікування, реабілітації та паліативної допомоги» забезпечує керівництво медичного закладу ефективним інструментом розвитку. Реальні доходи закладу при експлуатації МІС (медичних інформаційних систем) збільшуються: по-перше, за рахунок зростання продуктивності праці лікарів-діагностів при використанні формалізованих бланків (наприклад, лікар ультразвукової діагностики може ефективно працювати без медичної сестри, що забезпечує, з одного боку, економію фонду заробітної плати, а з іншого – збільшення заробітку лікаря, так як за роботу без медсестри він отримує доплату); по-друге, завдяки більш інтенсивному використанню такого дорогого устаткування, як комп'ютерний томограф, мамограф або УЗД-сканер; по-третє, в силу раціоналізації витрат на медикаменти, реагенти, необхідні для проведення лабораторних досліджень, та інші матеріали; по-четверте, завдяки контролю розрахунків зі страховими компаніями за послуги, надані по системі обов'язкового медичного страхування (ОМС), що дозволяє виключити необґрунтовані

недоплати; і, нарешті, за рахунок можливості керівництва закладу контролювати роботу установи в реальному часі.

Істотно поліпшити економічну ситуацію в закладі можна за рахунок автоматизації комплексу завдань по оптимізації роботи з медикаментами. Впровадження в закладах охорони здоров'я персоніфікованого обліку медикаментів, коли на всіх стадіях лікувального процесу, починаючи з лікарняної аптеки, та закінчуючи стаціонаром, з'являється можливість контролювати: який саме препарат, якого виробника, якого постачальника, якому пацієнтові, в якій кількості, на яку суму, яким лікарем був призначений, яка сестра його видала тощо. А це в свою чергу дозволяє практично виключити нецільове використання медичних препаратів і домогтися економії коштів, що протягом двох-трьох років окупить витрати на створення і підтримку комплексної МІС, яка має в складі сотні автоматизованих робочих місць. А зменшення за рахунок автоматизованого контролю призначень медикаментів числа передозувань медикаментів, призначень препаратів без урахування їх сумісності та протипоказань, а також інших лікарських помилок може окупити всі витрати на інформатизацію установи тільки за рахунок зниження витрат від судових позовів [20].

Враховуючи специфіку МІС при оцінці результату автоматизації закладу не слід забувати також про клінічну та організаційну складові ефективності. В якості критеріїв клінічної ефективності експерти називають такі показники, як зменшення кількості лікарських помилок при призначенні препаратів і направленні пацієнта на обстеження, підвищення точності, оперативності та інформативності діагностичних досліджень, зменшення числа загострень хронічних захворювань за певний період часу, загальне зниження захворюваності, підвищення ступеня відповідності лікування встановленим стандартам. Тут, знову ж таки, найбільш важливим показником є зведення до мінімуму кількості лікарських помилок [46].

Впровадження МІС має забезпечити лікаря оперативною високоякісною інформацією для правильної постановки діагнозу і визначення тактики лікування. Чим раніше лікар отримає відповідь діагностичної служби і чим інформативнішою і наочнішою буде ця відповідь, тим чіткіше і достовірніше лікар складе свій висновок і тим результативнішою буде його праця. Для аналізу та узагальнення результатів досліджень він може скористатися шаблонами, стандартами, довідковою інформацією, а система допоможе йому не забути важливі деталі.

Можна виділити дві групи показників з метою оцінки ефективності інформатизації охорони здоров'я: соціальні та економічні. Соціальні характеристики ефективності інформатизації охорони здоров'я [33, с.20]:

1) збільшення оперативності та якості прийнятих рішень, скорочення витрат на управління з допомогою створення відповідних інформаційно-аналітичних систем;

2) вдосконалення лікувально-діагностичних та профілактичних заходів на всіх рівнях надання медичної допомоги;

3) підвищення ефективності медичної допомоги за рахунок покращення якості постановки діагнозу та підвищення обґрунтованості прийнятих медичних рішень;

4) збільшення доступності висококваліфікованої медичної допомоги;

5) створення (розвиток) систем моніторингу стану здоров'я населення;

6) підвищення ефективності праці медичного персоналу за рахунок автоматизації трудомістких та рутинних операцій, підвищення достовірності даних та оперативності інформаційного обслуговування;

7) поліпшення взаємодії медичних служб та установ.

Економічні показники ефективності впровадження ІТ у системі охорони здоров'я [55]:

1) зниження витрат, що з наданням медичної допомоги пацієнтам, завдяки зменшенню числа помилкових діагнозів та неправильно обраних схем лікування;

2) збільшення обсягу використання трудомістких лабораторних та діагностичних методів досліджень без збільшення штатної чисельності персоналу за рахунок зростання продуктивності праці в автоматизованих лабораторіях, діагностичних кабінетах та інших медичних підрозділах.

Головний соціально-економічний ефект інформатизації у охороні здоров'я полягає у запобіганні втратам трудових ресурсів, пов'язаних з передчасною смертністю.

Крім того, велику допомогу в постановці діагнозу надають вбудовані в МІС функції обробки показників. Наприклад, на основі виміряних первинних даних система розрахує індекс маси тіла і дасть висновок, чи нормальною є вага пацієнта, надмірною чи вже існує загроза ожиріння (лікарю немає необхідності пам'ятати всі формули і показники). І як тільки результати будуть внесені в електронну карту і підтверджені електронним цифровим підписом, вони стануть доступні іншим лікарям. Додаткова автоматизована обробка отриманих результатів за допомогою оригінальних методик повинна підвищити саме інформативність досліджень. Але це якраз найважче. Необхідно створити ефективні експертні системи з великим об'ємом відповідних «знань», хоча їх побудова вимагає значно більших витрат часу і коштів, ніж автоматизація процесів реєстрації пацієнтів, обліку медичних послуг та їх оплати, формування звітів і т. п. [54].

Надання лікарю інструменту, що містить всі необхідні елементи для оперативного прийняття правильного рішення при постановці діагнозу, - одне із завдань найближчого майбутнього. За даними досліджень бостонської клініки Brigham and Women's Hospital, сьогодні налічується понад 10000 захворювань, 3000 міжнародних непатентованих назв лікарських препаратів, 300 різних радіологічних процедур і 1000 лабораторних досліджень. Практикуючий лікар повинен пам'ятати про 4000 медикаментів, які активно використовуються у світі, серед яких зафіксовано понад 2000 взаємодій, що істотно впливають на можливість їх застосування при тій чи іншій патології [50]. Зрозуміло, що головне завдання інформаційно-комунікаційних

технологій в охороні здоров'я полягає в забезпеченні безпеки пацієнта. Виходячи з цього, інформатизація охорони здоров'я в країнах Європейської співдружності йде по шляху створення систем підтримки лікарських рішень, створення нового інформаційного середовища його діяльності, що дозволяє звертатися до професійних інформаційних ресурсів (інформаційно-довідкових систем і тематичних форумів), здійснювати навігацію між професійними асоціаціями та визнаними експертами. Це створює середовище безперервної освіти лікарів за допомогою регулярного моніторингу останніх досягнень в області медицини і фармацевтики.

Системи комп'ютерної підтримки лікарських призначень дозволяють майже на 80% скоротити кількість лікарських помилок при призначенні ліків і на 55% знизити несприятливі побічні реакції. В окремих країнах лікар не може отримати ліцензії на професійну діяльність без відповідних знань в області інформаційних технологій (наприклад – в Нідерландах) [50].

Експерти, спираючись на багаторічний досвід створення і використання МІС для роботи з візуальними зображеннями, отриманими в результаті рентгенологічних, томографічних, мамографічних, ультразвукових та інших досліджень, стверджують, що користь від автоматизації відділень інструментальної діагностики є очевидною, оскільки при цьому значно розширюються професійні можливості лікарів різних спеціальностей [50].

У підвищенні якості медичного обслуговування велике значення надається автоматизації клініко-лабораторних досліджень. Істотно підвищується продуктивність лабораторії, створюється єдина база даних результатів досліджень, які при інтеграції лабораторної інформаційної системи з МІС ЛПУ стають доступними відразу всім лікарям, кому це необхідно.

Найбільш адекватним показником організаційної ефективності системи, на думку більшості експертів [50], можна вважати зменшення витрат робочого часу медичного персоналу при підготовці звітної документації. Оформлення великої кількості різних документів і підготовка

звітів стали вузьким місцем в роботі ЛПУ, що не може не відбитися на якості лікування, і тому користь від автоматизації на даний момент зв'язують з вирішенням цієї проблеми.

По мірі подальшого розвитку МІС цей розділ роботи можна буде взагалі виключити з кола обов'язків медичного працівника. Система сама повинна автоматично забирати всю необхідну інформацію з медичної документації і передавати її фахівцям, відповідальним за оформлення звітів. Впровадження МІС можна вважати успішним, якщо через якийсь час після його початку – а цей період може вимірюватися і місяцями, і роками – системою буде користуватися практично весь медичний персонал ЛПУ, і в такому випадку вже ставиться питання про кількісне оцінювання ефективності.

Поряд з клінічними, економічними, технологічними, управлінськими та організаційними показниками ефективності існують і такі, які неможливо оцінити кількісно, але тим не менше вони важливі для ЛПУ і в певній мірі відображають результат впровадження МІС. Це, наприклад, створений інформаційний комфорт в роботі співробітників, формування корпоративної спільноти, оптимального психологічного клімату, більш відповідального ставлення до прийняття управлінських рішень. Усе це в комплексі назвемо ергономічною ефективністю [49].

Крім загальних критеріїв ефективності впровадження МІС, про які вже говорилося, є також пов'язані зі спеціалізацією закладу або його підрозділів та пріоритетними завданнями. У будь-якого підприємства, в тому числі медичного, існує своя стратегія. Наприклад, необхідно знизити смертність серед пацієнтів, які потрапляють в реанімаційні відділення лікарень, або тривалість лікування хворих по основним захворюванням без зниження якості медичної допомоги, або скоротити відмови в оплаті за рахунками ОМС і т.п. Інформатизація є лише підтримкою стратегії засобами комп'ютерних технологій, а її результативність визначається якістю вирішення конкретних завдань закладу. Виходячи з викладеного вище,

складові ефективності впровадження медичної інформаційної системи в закладах охорони здоров'я та її функціонування показані на рис. 3.2.

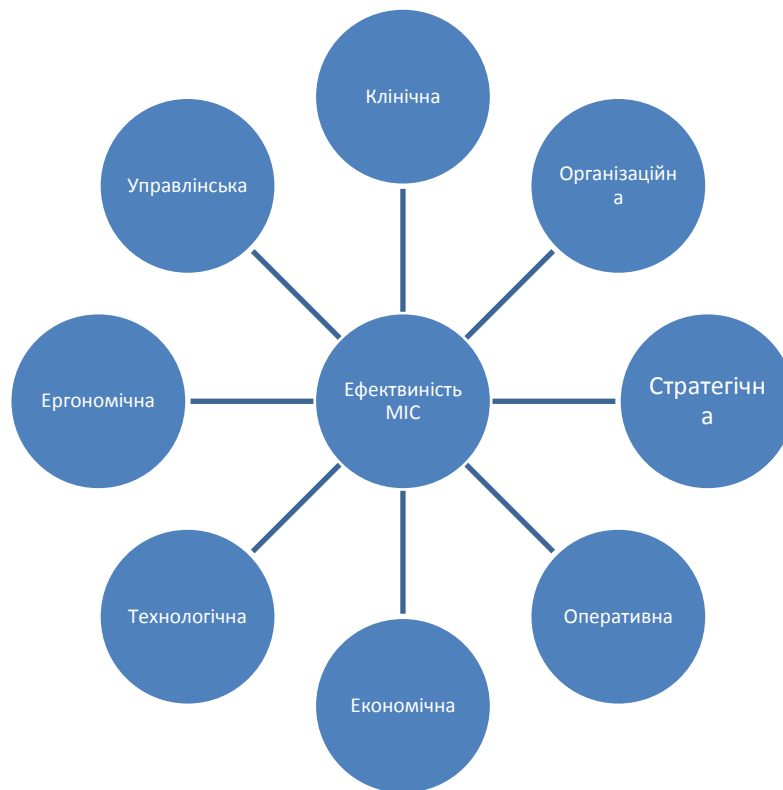


Рисунок 3.2 - Складові ефективності впровадження та функціонування МІС

Слід зазначити, що вибір лікувальним закладом критеріїв ефективності залежить також від форми власності. Для більшості комерційних підприємств витрати на автоматизацію повинні окупитися в прийнятний термін. Так, замовників з приватної клініки зазвичай цікавить, яка фінансова віддача від системи, наскільки будуть виправдані витрати на покупку комп'ютерів і МІС, і критерії тут цілком традиційні: скорочення собівартості послуг, оптимізація потоку пацієнтів, більш ефективного використання ресурсів (препаратів, витратних матеріалів, обладнання, приміщень, персоналу). Для керівництва КП «Львівське територіальне медичне об'єднання «Клінічна лікарня планового лікування, реабілітації та паліативної допомоги» превалюють організаційна та клінічна складові. Тут МІС є інструментом, що дозволяє скоротити трудомісткість персоналу на

оформлення документації, знизити число лікарських помилок, підвищити пропускну здатність закладу, скоротити час, який пацієнт витрачає на очікування в чергах, підвищити доступність медичної інформації для персоналу, і головний лікар вибирає ту систему, яка максимально повно відповідає поставленим завданням і має зручний інтерфейс [26].

Проте для ЛПУ будь-якої форми власності в однаковій мірі важливо, як позначиться впровадження МІС на вдосконаленні лікувально-діагностичного процесу, а зростання доходів установи є засобом досягнення основної мети – надання пацієнту високоякісної медичної допомоги. Названі критерії ефективності впровадження МІС в основному являють собою інтегральні показники, і тому отримати кількісну оцінку вельми складно, для цього необхідно виключити або хоча б звести до мінімуму вплив інших факторів і узагальнити дані, накопичені за великий термін. Найпростіше показати ефект від автоматизації окремих рутинних операцій: легко оцінити час, який витрачався, наприклад, на оформлення окремих документів, до впровадження і після того, як МІС запрацювала в штатному режимі і користувачі освоїли більшу частину функціональних можливостей. Складніше оцінити економічну ефективність, для цього треба мати доступ до фінансової інформації закладу за період, що передує впровадженню, що можливо далеко не завжди. Ключову роль повинен відігравати порівняльний аналіз: порівняння показників роботи закладу на початку інформатизації і на наступних стадіях; оцінювати результативність різних етапів; зіставляти з іншими закладами, в яких проходила автоматизація.

ВИСНОВКИ

У дослідженні вирішено наукове завдання, пов'язане з теоретичним обґрунтуванням та розробкою конкретних практичних рекомендацій щодо впровадження ефективного внутрішнього контролю за збереженням медичної інформації в установі охорони здоров'я. Отримані результати дослідження свідчать про успішне досягнення поставленої мети, виконання поставлених завдань і надають підстави для формулювання ряду важливих висновків:

1. Встановлено, що медико-діагностична інформація є ключовою для надання якісної та ефективної медичної допомоги, а також використовується для статистичного аналізу, досліджень та планування медичних заходів. Забезпечення безпеки, цілісності та конфіденційності цих даних вимагає впровадження високих стандартів і систем внутрішнього контролю. Основною метою цього контролю є виявлення та усунення можливих недоліків у роботі з медичною інформацією, а також запобігання її втраті чи несанкціонованому доступу. Проаналізовано теоретичні засади впровадження системи внутрішнього контролю за збереженням медичної інформації в установі охорони здоров'я. Визначено, що внутрішній контроль за збереженням медико-діагностичної інформації представляє собою процес отримання об'єктивних оцінок, якісних і кількісних, щодо поточного рівня захисту такої інформації організації відповідно до визначених критеріїв та вимог законодавства. Охарактеризовано методи та інструменти внутрішнього контролю за обробкою та реєстрацією медико-діагностичної інформації (МДІ) спрямовані на виявлення та усунення недоліків у роботі з МДІ, запобігання її втраті або несанкціонованому доступу.

2. Охарактеризовано нормативно-правові аспекти захисту медико-діагностичної інформації в Україні. Основні нормативні документи у цій сфері включають Закон України «Про захист персональних даних», Закон

України «Про державні фінансові гарантії медичного обслуговування населення», Постанова Кабінету Міністрів України «Деякі питання електронної системи охорони здоров'я». Гармонізація українського законодавства до європейських стандартів у сфері захисту персональних даних здійснюється шляхом імплементації Регламенту Європейського Парламенту та Ради про захист фізичних осіб у зв'язку з обробкою персональних даних і про вільний рух таких даних 2016/679 (Загальний регламент про захист персональних даних). Регламент зобов'язує заклади охорони здоров'я за вжиття всіх необхідних заходів для забезпечення конфіденційності, цілісності та доступності персональних даних. Ці вимоги значно підвищують відповідальність медичних закладів за організацію внутрішнього контролю за обробкою та реєстрацією медико-діагностичної інформації

3. Особливості організації внутрішнього контролю за обробкою та реєстрацією медико-діагностичної інформації здійснено на матеріалах КП «Львівське територіальне медичне об'єднання «Клінічна лікарня планового лікування, реабілітації та паліативної допомоги» Львівської міської ради. Враховуючи, що значну чисельність персоналу закладу та його розгалужену структуру, проблема внутрішнього контролю за обробкою та реєстрацією медико-діагностичної інформації в закладі охорони здоров'я набуває значної актуальності. Визначено завдання системи внутрішнього контролю за обробкою та реєстрацією медико-діагностичної інформації в закладі охорони здоров'я; охарактеризовано суб'єктні та функціональні складові такої системи.

4. Охарактеризовано практичні аспекти забезпечення інформаційної безпеки в процесі обробки та реєстрації медико-діагностичної інформації в закладі охорони здоров'я. Заходи контролю передбачає розробку та використання рекомендацій, інструкцій, програмних та технічних засобів, що спрямовані на захист конфіденційності, забезпечення цілісності медико-діагностичної інформації, систему виявлення вторгнень, аудит інформаційної

безпеки, навчання персоналу, резервне копіювання та відновлення. Результати оцінювання рівня захищеності медико-діагностичної інформації показує його достатній рівень, в той же час окреслено напрями покращення по ключовим проблемним питанням, зокрема щодо навчання та оновлення знань персоналу з інформаційної безпеки.

5. Сформовано комплекс заходів із забезпечення внутрішнього контролю за обробкою та реєстрацією медико-діагностичної інформації в закладі охорони здоров'я, який передбачає зниження інформаційних загроз, що пов'язані із людським фактором. До таких заходів віднесено: організація тренінгів для персоналу інформаційно-аналітичного відділу; впровадження системи корпоративних накопичувачів інформації; організація навчання персоналу підприємства з питань захисту інформації (зокрема тих, хто працює з медичними інформаційними системами), розвиток цифрових компетенцій тощо. Визначено, що успішне впровадження МІС на практиці, які і будь-якої інформаційної системи має супроводжуватися оцінюванням ефективності її функціонування. Виділені такі складові ефективності впровадження та функціонування МІС, як клінічна, організаційна, управлінська, економічна, технологічна, оперативна, ергономічна та стратегічна ефективність.

6. Розглянуто перспективні напрями розвитку системи підтримки прийняття лікарських рішень у медичній інформаційній системі закладу охорони здоров'я на основі медико-діагностичної інформації, що дозволяє істотно покращити якість медичної допомоги та скоротити кількість лікарських помилок. Обґрунтовано, що розробка нових функцій системи СППР та впровадження нових технологій вимагає вдосконалення процесів роботи з медичною інформацією, отже внутрішній контроль має забезпечити гнучкість та легкість впровадження нововведень, ефективний внутрішній аудит та оптимізацію робочих процесів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Аналіз законодавства про захист персональних даних України. URL: https://ecpl.com.ua/wp-content/uploads/2020/09/UKR_09142020_CEP_Finalnyy-zvit.pdf
2. Батюк Л.В., Кізілова Н.М. Система моніторингу біофізичних властивостей еритроцитів крові пацієнтів для цілей медичної діагностики. Системи обробки інформації. 2020. № 3(162). С. 13-20. DOI: 10.30748/soi.2020.162.02
3. 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.
4. Бем М., Городиський І. Захист персональних даних: правове регулювання та практичні аспекти : науково-практичний посібник. «К.І.С.» : Council of Europe Publishing, 2021. 158 с.
5. Гавловський В. Д. Захист інформації шляхом посилення ефективності протидії кібератакам. *Інформація і право*. 2019. № 3(30). С. 105-110.
6. Грищук Р. В. Технологічні аспекти інформаційного протиборства на сучасному етапі. *Захист інформації*. 2015. Т. 17, № 1. С. 80–86.
7. Грищук Р. В. Технологічні аспекти інформаційного протиборства на сучасному етапі. *Захист інформації*. 2015. Т. 17, № 1. С. 80–86.
8. Деякі питання електронної системи охорони здоров'я: Постанова Кабінету Міністрів України від 25.04.2018 р. №411 URL:
9. Дзьобань О. П. Від "інформаційного суспільства" до "інформаційної безпеки": до проблеми концептуалізації сутності понять. *Інформація і право*. 2019. № 2(29). С. 60-73.
10. ДСТУ ISO/IEC 27005:2019. Інформаційні технології. Метод захисту. Управління ризиками інформаційної безпеки / Нац. стандарт України. Вид. офіц. [Чинний від 2019-11-01]. Київ : ДП «УкрНДНЦ», 2019. 76 с.

11. Дегтярєва Л.М. Аналіз структури систем захисту інформації. Системи управління, навігації та зв'язку. Збірник наукових праць. Полтава: ПНТУ, 2019. Т. 2 (54). С. 78-82.
12. Дудатьєв А. В. Комплексна інформаційна безпека соціотехнічних систем: моделі впливу та захисту : монографія. Вінниця : ВНТУ, 2017. 128 с.
13. Духовна О. Захищені та здорові: як регламентується захист персональних даних пацієнтів в Україні URL: <https://yur-gazeta.com/dumka-eksperta/zahishcheni-ta-zdorovi-yak-reglamentuetsya-zahist-personalnih-danih-pacientiv-v-ukrayini.html>
14. Захаренко К. Основні суб'єкти та інститути інформаційної безпеки. *Науковий вісник. Серія «Філософія»*. Харків: ХНПУ. 2017. Вип.48 (частина І). С. 212–219.
15. Інструкція щодо заповнення форми первинної облікової документації № 025/о «Медична карта амбулаторного хворого МОЗ України» ; Наказ, Форма, Інструкція від 14.02.2012 № 110. URL : <http://zakon1.rada.gov.ua/laws/show/z0669-12>
16. 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.
17. 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.
18. Керівництво з управління ризиками для систем інформаційних технологій. Рекомендації Національного інституту Стандартів і технологій (Guide for Conducting Risk Assessments. National Institute of Standards and Technology). Gaithersburg: National Institute of Standards and Technology, 2003. 95 с.
19. Коваленко С. В. Технологія аудиту кібербезпеки корпоративної інформаційної системи за методикою ISO/IEC: 27001. *Сучасний захист інформації*. 2021. №3. DOI: 10.31673/2409-7292.2021.032935

20. Копняк К.В.

Оцінювання ефективності впровадження медичних інформаційних систем. *Економіка і організація управління*. 2017. №2. URL: <https://jeou.donnu.edu.ua/article/view/4784>

21. Корольов В.Ю. Захист інформації в корпоративних USB-флешнакопичувачах для хмарних обчислень. *Мат. машини і системи*. 2012. № 2. С. 60-69.

22. Коц Д.В. Правові питання системи захисту інформації. Актуальні проблеми управління інформаційною безпекою держави : зб. тез доп. наук.-практ. конф., м. Київ, 4 квітня 2019 р. Київ, 2019. No 10. С. 170–172.

23. Куперштейн Л.М., Ясінська Я.О. Аналіз загроз інформаційної безпеки в медицині. URL: <https://ir.lib.vntu.edu.ua/bitstream/handle/123456789/30909/WORK-IES-2020-242-243.pdf?sequence=1>.

24. Куперштейн Л.М., Ясінська Я.О. Дослідження політики інформаційної безпеки у розрізі нормативної документації. URL: <https://ir.lib.vntu.edu.ua/bitstream/handle/123456789/29388/9339.pdf?sequence=3>

25. Курченко О. А. Загальні принципи проведення тестування інформаційної безпеки підприємства. *Сучасний захист інформації*. 2018. № 4. С. 27-34.

26. Лемішко Я.О. Напрямок підтримки прийняття лікарських рішень у медичних інформаційних системах на основі медико-діагностичної інформації. *Матеріали Міжнародної науково-практичної конференції Інженерного навчально-наукового інституту ім. Ю.М. Потебні Запорізького національного університету «Сучасні виклики та напрямки вдосконалення в економічній та технічній науках»* (5 – 6 грудня 2023 р., м. Запоріжжя). Запоріжжя, 2023.

27. 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.

28. Ліпкан В.А. Інформаційна безпека України в умовах євроінтеграції: навчальний посібник. К.: КНТ, 2006. 280 с.

29. Лужецький В.А., Кожухівський А.Д., Войтович О.П. Основи інформаційної безпеки : навчальний посібник. Вінниця: ВНТУ, 2013. 221 с.

30. Медична інформатика : навч. посібник для студентів мед. ун-тів / В. Г. Книгавко, О. В. Зайцева, М. А. Бондаренко та ін. – Харків : ХНМУ, 2020. 64 с.

31. Медична інформація лікарська таємниця. URL: <https://advokaty.dp.ua/wp-content/uploads/2019/11/Stopina-YU.-O.-Medychna-informatsiya-ta-likarska-tayemnytsya.pdf>

32. Муравйов В. Є. Інформаційне суспільство: трансформація від індустрії знань до цифровізації. *Науковий вісник Ужгородського університету. Серія «Економіка»*. 2019. Вип. 1 (53). С. 39-47.

33. Мусієнко А. В., Мусієнко В. В. Актуальні аспекти нормативно-правових механізмів захисту персональних даних в електронних медичних реєстрах в Україні. *DictumFactum*. 2022. Вип. 1 (11). С. 17-22.

34. Нестеренко Г. Інформаційна безпека: курс лекцій. Київ: НАУ, 2022. 102 с

35. Овчаренко Я.О. Регламент захисту персональних даних Європейського Союзу. *Юридичний науковий електронний журнал*. 2018. № 3. С. 67-69.

36. Онлайн-курс «Захист персональних даних». URL: <https://euprostitir.org.ua/resources/159421>

37. Основи законодавства України про охорону здоров'я від 19 листопада 1992 року № 2801-ХІІ. *Відомості Верховної Ради України*. 1993. № 4. Ст. 19.

38. Панасюк А.В. Розроблення системи захисту інформації з обмеженим доступом, що озвучується. *Матеріали XI Міжнародної науково-практичної*

конференції молодих вчених, курсантів та студентів. URL: <https://cutt.ly/3YRbnBJ>

39. Про захист персональних даних: Закон України від 1 червня 2010 року

№ 2297-VI URL: <https://zakon.rada.gov.ua/laws/show/2297-17#Text>

40. Про основні засади забезпечення кібербезпеки України: Закон України від 17.09.2020 № 912- IX. URL: <https://zakon.rada.gov.ua/laws/show/2163-19/ed20201024#Text>.

41. Радзішевська Є. Б., Висоцька О. В. Інформаційні технології в медицині. E-health / за ред. В. Г. Книгавка. Харків : ХНМУ, 2019. 72 с.

42. Рамазанов С.К., Надьон Г.О., Кришталь Н.І., Степаненко О.П., Тимашова Л.А. Інноваційні технології антикризового управління економічними системами: монографія; під ред.. проф. С. К. Рамазанова. Луганськ-Київ: вид-во СНУ ім. В. Даля, 2009. 584 с.

43. Регламент Європейського парламенту і Ради (ЄС) 2016/679 від 27 квітня 2016 року про захист фізичних осіб у зв'язку з опрацюванням персональних даних і про вільний рух таких даних, та про скасування Директиви 95/46/ЄС URL: https://zakon.rada.gov.ua/laws/show/984_008-16#Text

44. Сопілко І. М. Механізм захисту персональних даних: проблеми та перспективи. *Юридичний вісник. Повітряне і космічне право*. 2013. № 2. С. 66-70.

45. Степашко В.С., Мельник І.М., Кваша Т.К., Волощук Р.В. Моделі розрахунку інтегрального індексу для груп первинних економічних показників. *Науково-технічна інформація*. 2005. №2. С.8-12.

46. Токарева К. С. Проблеми захисту персональних даних у сфері охорони здоров'я в умовах інформатизації. *Юридичний науковий електронний журнал*. 2022. № 11. С. 496–499. DOI <https://doi.org/10.32782/2524-0374/2022-11/120>.

47. David S. Jones, M.D., SheilaQuinn.

IntroductiontoFunctionalMedicineURL:

<http://www.thecenterforultrahealth.com/wp-content/uploads/2015/03/Functional-Medicine-Explanation.pdf>

48. 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.

49. DigitalHealth: Primarycareisnolongerprimary. URL: <https://www.accenture.com/us-en/insights/health/digital-health-primary-care>.

50. Gopal G., Suter-Crazzolara C., Toldo L., Eberhardt W. Digital transformation in healthcare - Architectures of present and future information technologies. Clinical Chemistry and Laboratory Medicine. 2018. Vol. 57. No. Pp. 328–335. DOI: 10.1515/cclm-2018-0658

51. Greenes R.A. Clinicaldecisionsupport: theroadahead. Boston: ElsevierAcademicPress, 2007. 581 p

52. Haux R., Ammenwerth E., Herzog W., Knaup P. Healthcareintheinformationsociety. A prognosisfortheyear 2013.Int. J. Med. Informatics. 2002. Vol. 66. № 1. P. 3–21

53. 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

54. Kizilova N. Multidisciplinary Approaches in Cancer Diagnosis and Treatment: Towards Patient-Specific Predictive Oncology. Acta Scientific Cancer Biology. 2019. Vol.3. No. 8. Pp. 1-2. DOI: ASCB-03-0145

55. Morze N.V., Strutynska O.V. Digital transformation in society: key aspects for model development. Journal of Physics: Conference Series. 2021. Vol. 1946. P. 012021. DOI: 10.1088/1742-6596/1946/1/012021

56. NIST Special Publication 800-61, Computer Security Incident Handling Guide. Recommendations of the National Institute of Standards and Technology, January 2004.

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

Виконала здобувачка магістратури
за спеціальністю 073 Менеджмент
зі спеціалізацією Організація і
управління охороною здоров'я за
заочною формою

« ____ » грудня 2023 р.

Підпис

Я.О. Лемішко

Ініціали, прізвище

Науковий керівник

доктор економічних наук,
професор, професор кафедри
менеджменту, економіки,
статистики та цифрових технологій

« ____ » грудня 2023 р.

Підпис

П.Г. Іжевський

Ініціали, прізвище

Робота допущена до захисту:

к.е.н., доцентка, завідувачка
менеджменту, економіки,
статистики та цифрових технологій

« ____ » грудня 2023 р.

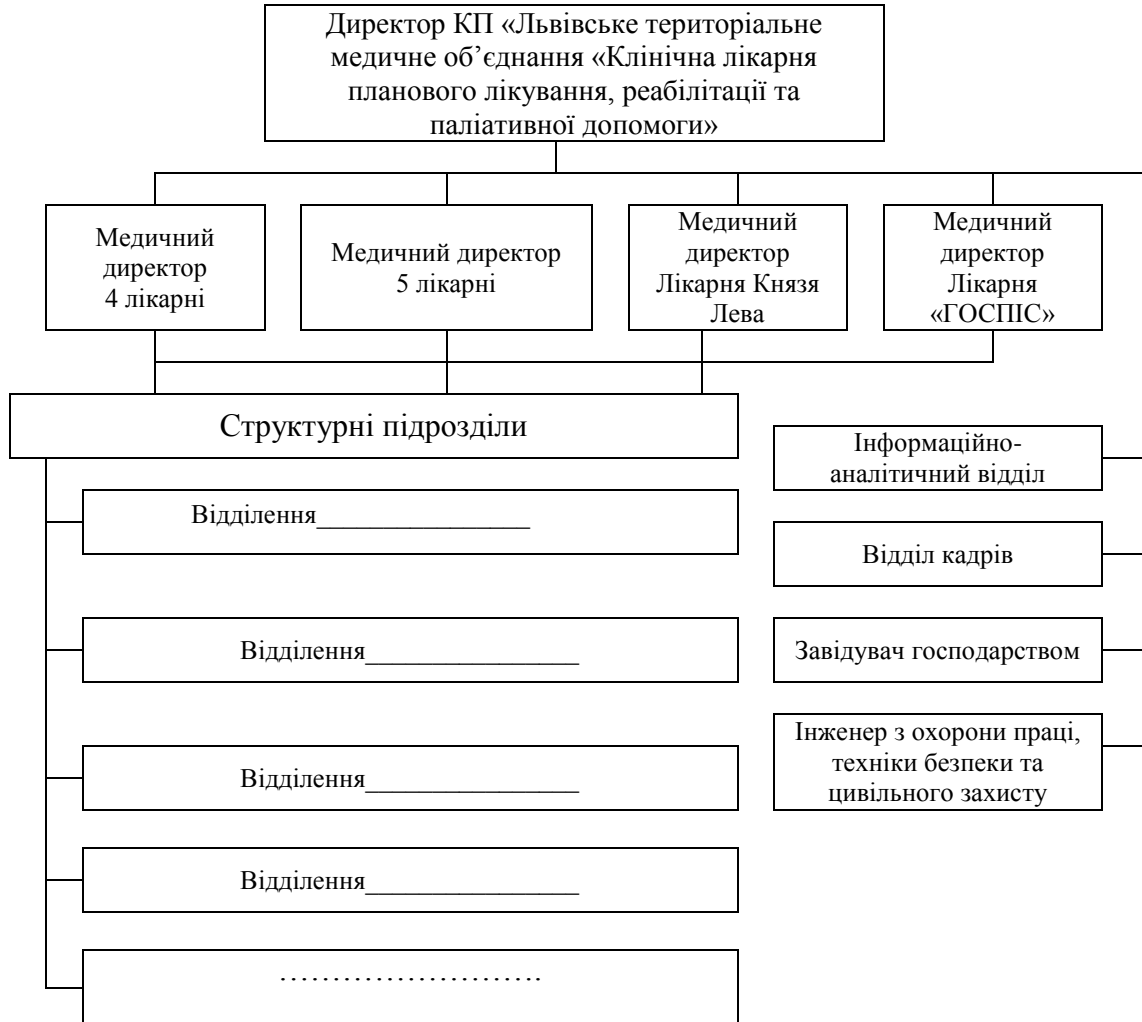
Підпис

Н.П. Захаркевич

Ініціали, прізвище

ДОДАТКИ

Додаток А



Організаційна структура КП «Львівське територіальне медичне об'єднання «Клінічна лікарня планового лікування, реабілітації та паліативної допомоги»

Примітка. Складено автором.