ХМЕЛЬНИЦЬКИЙ УНІВЕРСИТЕТ УПРАВЛІННЯ ТА ПРАВА ІМЕНІ ЛЕОНІДА ЮЗЬКОВА

ФАКУЛЬТЕТ УПРАВЛІННЯ ТА ЕКОНОМІКИ

Кафедра: менеджменту, фінансів, банківської справи та страхування

МАГІСТЕРСЬКА РОБОТА

на здобуття освітнього ступеня магістра
на тему:

«Внутрішній контроль за збереженням медичної інформації в закладі охорони здоров'я (на матеріалах комунальної установи «Хмельницьке обласне бюро судово-медичної експертизи» Хмельницької обласної ради)»

Виконав: студент магістратури за спеціальністю 073 Менеджмент
О. Шандига-Глушко
(прізвище та ініціали)

Керівник: к.е.н., доцент,
Д.А. Арзянцева
(науковий ступінь, вчене звання, прізвище та ініціали)

Рецензент: **Н.В. Козицька,**
начальник Хмельницького обласного бюро судово-медичної експертизи

Хмельницький – 2021 рік

Анотація

Шандига-ГлушкоО. Внутрішній контроль за збереженням медичної інформації в закладі охорони здоров'я (на матеріалах комунальної установи «Хмельницьке обласне бюро судово-медичної експертизи» Хмельницької обласної ради). 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, 2020. – 71 с.

Метою роботи є поглиблення теоретичних і практичних аспектів організації внутрішнього контролю за збереженням медичної інформації в закладі охорони здоров'я.

Опрацьовано теоретичні основи організації внутрішнього контролю за збереженням медичної інформації в закладі охорони здоров'я. Встановлено, що внутрішній контроль за збереженням медичної інформації – це процес отримання об'єктивних якісних та кількісних оцінок про поточний стан захисту медичної інформації організації у відповідності до певних критеріїв та вимог законодавства. Виділено види контролювання, що рекомендовані для застосування у системі внутрішнього контролю за збереженням медичної інформації в закладі охорони здоров'я: попередній, поточний, самоконтроль, проміжний, завершальний. Охарактеризовано методики внутрішнього контролю за збереженням медичної інформації, засновані на побудові моделі загроз та вразливостей.

Розглянуто правові аспекти регулювання роботи із персональними даними у сфері медичної діяльності в Хмельницькому обласному бюро судово-медичної.

Процес упровадження внутрішнього контролю в систему управління Хмельницького обласного бюро судово-медичної експертизи систематизовано у відповідній організаційної моделі: представлено інформаційно-аналітичне забезпечення внутрішнього контролю (запропоновано структуру реєстру інформаційних активів, структуру реєстру

інформаційних ризиків у контексті збереження медичної інформації), обґрунтовано доцільність створення посади фахівця (контролера) із захисту персональних даних, підпорядкування та основні завдання такої служби.

Ключові слова: медична інформація, персональні дані, внутрішній контроль, ризик.

Summary

Shandyga-Glushko O. Internal control over the preservation of medical information in the health care institution (on the materials of the municipal institution "Khmelnytsky Regional Bureau of Forensic Medical Examination" of the Khmelnytsky Regional Council). Qualification scientific work on the rights of the manuscript. Master's degree in 073 Management. - Khmelnytsky University of Management and Law named after Leonid Yuzkov, Khmelnytsky, 2020. - 71 p.

The aim of the work is to deepen the theoretical and practical aspects of the organization of internal control over the preservation of medical information in the health care institution.

Theoretical bases of the organization of internal control over the preservation of medical information in the health care institution have been developed. It is established that internal control over the preservation of medical information is a process of obtaining objective qualitative and quantitative assessments of the current state of protection of medical information of the organization in accordance with certain criteria and legal requirements.

The process of introducing internal control into the management system of Khmelnytsky Regional Bureau of Forensic Medical Examination is systematized in the appropriate organizational model: information and analytical support of internal control is presented (proposed structure of the register of information assets, structure of the register of information risks in the context of medical information preservation). (controller) for personal data protection, subordination and main tasks of such service.

Key words: medical information, personal data, internal control, risk.

ЗМІСТ:

ВСТУП

Актуальність теми. Дотримання вимог до захисту медичної інформації є складним завданням для сфери охорони здоров'я та особливо – для всіх медичних установ, які активно беруть участь у роботі із персональними даними. Забезпечення захисту даних у сфері охорони здоров'я пов'язане з вирішенням нових і важливих завдань, що виникають у міру того, як технічний прогрес розширює межі великих даних, хмарного зберігання даних та інших складових систем охорони здоров'я. Внаслідок цього надзвичайно важливо, щоб заклади охорони здоров'я мали можливість підтримувати рівновагу між загальновизнаним постулатом про захист персональних даних та необхідністю використання такої інформації для виконання своїх функцій. У зв’язку з цим, актуалізується проблема формування дієвої системи внутрішнього контролю за збереженням медичної інформації в закладі охорони здоров’я.

Серед провідних вітчизняних та зарубіжних дослідників проблематики варто виділити таких: Бем М. В. [2], Гавловський В. Д. [5], Дегтярьова Л.М. [7], Дзьобань О. П.[9], Коц Д.В. [20], Курченко О. А. [2], Лапінська Є. І. [24], Мельник С.І. [29], Овчаренко Я.О. [33], Панасюк А.В. [36]. Більшість наукових праць присвячується дослідженню інформаційної безпеки організації. В той же час розробці практичних аспектів управління внутрішнім контролем за збереженням медичної інформації в закладі охорони здоров’я приділено недостатньо уваги.

Мета й завдання дослідження. Мета роботи полягає в поглибленні теоретичних і практичних аспектів організації внутрішнього контролю за збереженням медичної інформації в закладі охорони здоров’я. Визначена мету зумовила необхідність виконання таких завдань:

– визначити сутність внутрішнього контролю за збереженням медичної інформації в закладі охорони здоров’я;

– розглянути теоретичні аспекти організацію внутрішнього контролю за збереженням медичної інформації в закладі охорони здоров’я;

– надати загальну характеристику Хмельницького обласного бюро судово-медичної експертизи та проаналізувати організаційне забезпечення внутрішнього контролю за збереженням інформації в закладі;

– оцінити рівень захищеності інформації в закладі охорони здоров'я;

– визначити напрями підвищення ефективності внутрішнього контролю за збереженням інформації в закладі охорони здоров'я.

Об'єктом дослідження є процеси внутрішнього контролю за збереженням медичної інформації в закладі охорони здоров'я**.**

Предметом дослідження є теоретичні та практичні аспекти організації внутрішнього контролю за збереженням медичної інформації в КП «Хмельницьке обласне бюро судово-медичної експертизи» Хмельницької обласної ради**.**

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

У процесі вирішення поставлених завдань використано такі методи наукового дослідження: теоретичного узагальнення, системного аналізу, синтезу (для дослідження теоретичних основ внутрішнього контролю за збереженням медичної інформації); аналітичний метод та експертне опитування – для оцінювання рівня захищеності медичної інформації КП «Хмельницьке обласне бюро судово-медичної експертизи»; системний метод – для обґрунтування перспективних напрямів розвитку внутрішнього контролю за збереженням медичної інформації та оцінки ефективності їх реалізації; абстрактно-логічний - для теоретичних узагальнень і висновків за результатами дослідження.

Інформаційну базу дослідження склали Конституція України, закони України: «Про основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки», «Про інформацію», «Про Концепцію Національної програми інформатизації», «Про захист інформації в інформаційно-

телекомунікаційних системах», «Про захист персональних даних», конвенції, угоди, які регулюють інформаційну безпеку, як суспільні відносини в інформаційному середовищі, законодавство зарубіжних країни, локальні акти внутрішнього контролю за збереженням медичної інформації. Емпіричну базу дослідженнястановлять статистичні матеріали, що характеризують стан інформаційної безпеки та внутрішнього контролю за збереженням медичної інформації, довідкові видання, наукові публікації з досліджуваної проблематики.

Апробація результатів дослідження. Окремі положення та отриманні результати магістерської роботи були оприлюднені на Всеукраїнській науково-практичній Інтернет-конференції молодих учених та студентів «Міждисциплінарні дослідження науки XXI століття» (1 грудня, 2021 р., м.Київ) [53].

Практичне значення одержаних результатів полягає в узагальненні теоретичних основ внутрішнього контролю за збереженням медичної інформації, опрацюванні конкретних пропозицій щодо удосконалення управління і цій сфері.

РОЗДІЛ 1. ТЕОРЕТИЧНІ ОСНОВИ ВНУТРІШНЬОГО КОНТРОЛЮ ЗА ЗБЕРЕЖЕННЯМ МЕДИЧНОЇ ІНФОРМАЦІЇ В ЗАКЛАДІ ОХОРОНИ ЗДОРОВ'Я

1.1. Сутність медичної інформації та на необхідність її захисту як складової інформаційної безпеки закладу охорони здоров'я

Сучасні інформаційні технології відіграють найважливішу роль у медичній галузі, але однією з найбільш серйозних проблем, що перешкоджають їх повсюдному впровадженню, є забезпечення захисту інформації, у тому числі захисту персональних даних громадян та відомостей, що становлять медичну таємницю, – персональних медичних даних. Актуальність проблеми захисту персональних медичних даних сьогодні не викликає сумнівів. Кібертероризм, доступ фізичних осіб до баз персональних даних посилюють ризик вторгнення у сферу приватного життя та порушення права на її недоторканність [9, с.65]. Захист медичних даних є однією з найбільш гострі проблеми в інформатизації організацій медичної області.

Медична інформація, у широкому значенні, – це будь-яка інформація, що стосується медицини. У вужчому, - це інформація, що відноситься безпосередньо до людини як пацієнту, тобто інформація про його здоров'я, особливості організму, перенесені захворюваннях та ін. Виділяють такі види медичної інформації [28]:

1. Алфавітно-цифрова інформація становить велику змістову частину медичної інформації (друковані та рукописні документи).

2. Візуальна інформація:

статична: різні зображення (рентгенограми, ехокардіограми та ін.).

динамічна: хода та міміка пацієнта, сухожильні рефлекси, реакція зіниці на світло, що генерується діагностичним обладнанням, динамічне зображення та ін.

3. Звукова інформація:

мова: коментарі лікаря, мова пацієнта з неврологічною або психічною патологією та ін;

звукові сигнали, що генеруються медичним обладнанням: доплерівські сигнали кровотоку при ЕхоКГ, флоуметричні сигнали та ін;

природні звуки організму людини, посилені електронним способом.

4. Комбіновані види інформації – це будь-які поєднання алфавітно-цифрової, візуальної чи звукової інформації.

Медична інформація має характерні особливості. Розглянемо їх.

Об'єктивність медичної інформації. Всю інформацію, що циркулює у медичних закладах, прийнято розділяти на: об'єктивну та суб'єктивну. Об'єктивною вважається така інформація, яка створюється шляхом реєстрації апаратними засобами при дослідженні пацієнта та діагностики захворювань. Такими дослідженнями є, наприклад, різні датчики біопотенціалів людини, термометрія, ендоскопія, біопсія. До них відносяться також різні способи отримання зображення внутрішніх органів – рентгенографія, комп'ютерна томографія, ультразвукова біолокація. До об'єктивної інформації можна віднести статистичні показники роботи лікувальних установ, цифрові дані діяльності органів охорони здоров'я [59, с.45].

Суб'єктивною вважається така інформація, яка виходить при аналізі сигналів безпосередньо людиною, без застосування якихось складних електронних пристроїв [16, с.167]. Суб'єктивними даними є, наприклад, результати огляду хворого, пальпація його органів тощо.

Слід врахувати, що розподіл на об'єктивну та суб'єктивну інформацію не завжди можна чітко розмежувати. Для розмежування ступеня об'єктивності одержуваних під час обстеження пацієнта даних вводиться поняття «золотого стандарту». Золотий стандарт – це медичний діагноз, встановлений максимально об'єктивним шляхом дослідження, тобто тим, що з найбільшою ймовірністю відображає справжній стан пацієнта, що досліджується [27, с.56]. Зазвичай як золотий стандарт виступають дані розтину (аутопсії),

прижиттєвої біопсії, іноді коректно виконаних складних методів дослідження.

Достовірність медичної інформації. Достовірність медичної інформації пов'язана насамперед із якістю сигналу та зареєстрованими даними. Під час реєстрації біологічного сигналу від пацієнта неминуче виникають перешкоди, чи «інформаційні» шуми [7, с.80]. Співвідношення між величиною сигналу кількістю шумів визначає якість роботи реєструючої системи. Чим вищий рівень реєстрованого сигналу і чим слабші сторонні шуми, тим достовірніша інформація. Якщо рівень шуму високий, корисний сигнал може бути не зареєстрований.

Доступність медичної інформації. Доступність медичної інформації – це міра можливості отримати ту чи іншу інформацію [57]. На ступінь доступності інформації впливають одночасно як доступність даних, і доступність адекватних методів їхнього інтерпретації. Відсутність доступу до даних або відсутність адекватних методів обробки даних призводять до однакового результату: інформація виявляється недоступною.

Доступність інформації визначається можливістю отримати від медичного працівника ту чи іншу інформацію. Деякі дані можуть мати обмежувальні грифи різного ступеня таємності. Доступ до них дозволено лише обмеженому контингенту медичних працівників, спеціально визначених регламентом роботи медичного закладу.

Актуальність медичної інформації. Під актуальністю медичної інформації мається на увазі ступінь її відповідності поточного часу. У медичній практиці завжди слід враховувати ту обставину, що достовірна та адекватна медична інформація, наприклад, лабораторні аналізи, результати інструментального діагностичного дослідження, опитування хворого, втратять свою актуальність, якщо інформаційний процес довго розтягнутий за часом. За рівнем актуальності вся медична інформація може бути поділена на кілька груп [49, с.70]:

1. Медична інформація негайного застосування.

2. Медична інформація середньострокової актуальності.

3. Медична інформація довгостроково застосування.

Розглянуті особливості медичної інформації обумовлюють складність розв'язання задач захисту інформації в медичних інформаційних системах (МІС), що характеризується такими факторами [39, с.56]:

перехід на безпаперову технологію вимагає забезпечення юридичної значущості електронних документів

використання ресурсів медичних інформаційних системи вимагає забезпечення безпеки інформації на рівні розмежування доступу;

низка електронних документів вимагають забезпечення безпеки на рівні приховування змістового змісту, а деяких випадках і недопущення несанкціонованого розмноження;

робота в територіально-розподіленій мережі висуває високі вимоги до автентичності інформації та джерел даних;

висуваються високі вимоги до цілісності програмного забезпечення (системного та прикладного), систем управління базами даних та цілого ряду електронних документів.

Велика концентрація масивів медичної інформації, відсутність елементарного контролю над її збереженням і низький рівень надійності технічних засобів викликають серйозну тривогу у забезпеченні безпеки інформації. У процесі експлуатації МІС, накопичувана та оброблена інформація є досить вразливою, схильною до несанкціонованого використання. А велика кількість різних компонентів, операцій, ресурсів і об'єктів МІС створює дуже привабливе середовище для різноманітних вторгнень та несанкціонованих дій [10, с.32].

Основними проблемами у процесі захисту інформації в МІС є [55]:

· запобігання витоку, розкрадання, втрати, спотворення, підробки інформації;

· запобігання загрозам безпеці інформації особи, суспільства, держави;

· запобігання несанкціонованим діям зі знищення, модифікації, спотворення, копіювання, блокування інформації;

· запобігання різним формам незаконного втручання в інформаційні та інформаційні ресурси системи;

· забезпечення правового режиму використання документованої інформації як об'єкта власності;

· захист конституційних прав громадян на збереження особистої таємниці та конфіденційності персональних даних, що є в інформаційних системах;

· збереження лікарської таємниці, конфіденційності документованої інформації відповідно до законодавства;

· гарантія прав суб'єктів в інформаційних процесах та при розробці, створенні та застосуванні інформаційних систем, технологій та засобів їх забезпечення [2, с.156].

Під системою захисту інформації розуміється сукупність органів та або виконавців, що використовують техніки захисту інформації, а також об'єктів захисту інформації, що організована та функціонує за правилами і нормами, встановленими відповідними документами в галузі захисту інформації [1]. При цьому в загальному випадку під об'єктом захисту слід розуміти сукупність інформації, носіїв що її містять, а також персоналу та засобів обчислювальної техніки, що забезпечують або здійснюють її обробку.

Слід відмітити, що забезпечення інформаційної безпеки та захист інформації є по суті всім близькими поняттями, що мають на увазі особливу діяльність, спрямовану на запобігання витоку інформації, що захищається, несанкціонованих і ненавмисних впливів на інформацію, що захищається, а також діяльність спрямовану на усунення (нейтралізацію, парірування) внутрішніх та зовнішніх загроз інформаційній на мінімізацію збитків від можливої реалізації таких загроз [5, с.108]. Таким чином, особлива увага повинна приділятися забезпеченню захисту інформації в закладі охорони здоров’я, ступінь ефективності якого буде залежити від організації системи

внутрішнього контролю за збереженням медичної інформації в закладі охорони здоров'я.

1.2. Організація внутрішнього контролю за збереженням медичної інформації в закладі охорони здоров'я

Забезпечити повноцінний та надійний захист персональних даних, зокрема медичної інформації можна лише за умови застосування комплексного та системного підходу. Одним із найважливіших компонентів процесів управління закладом охорони здоров'я є внутрішній контроль за збереженням медичної інформації. Внутрішній контроль за збереженням медичної інформації дозволяє керівництву закладу охорони здоров'я визначити реальний стан інформаційних активів, оцінити їхню захищеність, провести оцінку ризиків, спричинених невідповідністю захищеності нормативним вимогам, коректно та обґрунтовано підійти до питання забезпечення захисту. Система захисту персональних даних пеки має бути побудована з урахуванням усіх актуальних загроз та уразливостей, а також з урахуванням тих загроз, які можуть виникнути в майбутньому.

Підходи до розуміння внутрішнього контролю за збереженням медичної інформації в організації відображено табл.1.1.

Таблиця 1.1 Підходи до розуміння поняття «Внутрішній контроль за збереженням медичної інформації»

Автори	Зміст поняття
В.С. Іфтемчук, В.А. Григорьев, М.І. Маниліч, Г.Д. Шутак [32, с. 55]	Внутрішній контроль за збереженням медичної інформації – незалежна перевірка організації та управління інформаційною безпекою та її реалізації через певні проміжки часу або при появі істотних змін у способи реалізації загроз витоку за збереженням медичної інформації.
А.Н. Азрилиян [29, с. 56]	Внутрішній контроль за збереженням медичної інформації - систематичний, незалежний та документований процес отримання свідоцтва аудиту діяльності організації забезпечення за збереження медичної інформації

	(персональних даних) та встановлення ступеня виконання встановлених критеріїв організаційно-юридичного аудиту
С.І. Мельник, М.Ю. Цуп [48]	Внутрішній контроль за збереженням медичної інформації – процес отримання об'єктивних якісних та кількісних оцінок про поточний стан захисту медичної інформації організації у відповідності до певних критеріїв та вимог законодавства.

Внутрішній контроль за збереженням медичної інформації в закладі охорони здоров'я охоплює [25]:

управління ризиками та загрозами витоку персональних даних;

управління документацією та інформаційною довідковою системою в організації;

управління організаційно-юридичним аудитом за збереженням медичної інформації;

аналіз ефективності системи захисту медичної інформації;

управління завданнями та діяльністю співробітників, які здійснюють роботу із персональними даними в організації;

управління процесами забезпечення безперервності роботи інформаційних систем та інформаційно телекомунікаційних послуг, що задіяні у роботі з персональними даними;

управління процесами забезпечення моніторингу, виявлення та реагування на ризики у цій сфері;

управління процесами збереження медичної інформації шляхом здійснення роботи зі співробітниками організації, підвищення загальної компетенції з питань інформаційної безпеки;

управління процесами забезпечення збереженням медичної інформації при здійсненні інформаційного обміну та взаємодії з третіми сторонами;

управління процесами забезпечення розмежування прав доступу до інформації та інформаційних систем користувачів організації, а також подальшого контролю за даним процесом.

Дані напрями у забезпеченні захисту є основними, і будь-який процес у межах діяльності із захисту інформації можна до них віднесено, таким чином вводячи єдину систему класифікації діяльності із забезпечення

інформаційної безпеки. Необхідність пропорційного розвитку кожного з цих напрямів зумовлюється їхньою взаємопов'язаністю. Відсутність належного рівня розвитку одного з напрямків, порівняно з іншими, неминуче призведе до нераціонального та слабоефективного використання ресурсів системи захисту інформації, а також до фінансових втрат з боку організації, не кажучи вже про збільшення ймовірності реалізації загроз інформаційної безпеки та супутнього збільшення рівня ризику для активів організації [18].

Управління цими напрямами дозволить істотно спростити реалізацію механізмів системи захисту інформації в закладі охорони здоров’я, простежити за планомірністю розвитку кожного з напрямків та дасть можливість грамото перерозподілити матеріальні ресурси між напрямами, що допоможуть суттєво збільшити ефективність реалізованих механізмів захисту інформації при збереженні поточного рівня витрат організації на захист інформації.

Залежно від рівня зрілості організації у питаннях інформаційних технологій та захисту медичної інформації, а також з огляду на різницю у специфіці роду діяльності кожної організації, у зв'язку з чим до них можуть бути застосовні різні нормативно-правові вимоги в галузі захисту інформації, окремі напрямки можуть мати різні пріоритети [30, с.5].

Характеристика видів контролювання, що рекомендовані для застосування у системі внутрішнього контролю за збереженням медичної інформації в закладі охорони здоров’я, здійснена в табл. 1.2.

Таблиця 1.2 Характеристика видів контролювання системи збереженням медичної інформації в закладі охорони здоров’я

Види контролювання	Характеристика
1	2
Попередній	Відбувається на вході у систему управління інформаційною діяльністю підприємства та передбачає те, що встановлюються правила збереженням медичної інформації в закладі охорони здоров’я, процедури щодо її здійснення тощо. Особливу вагу на вході до системи управління інформаційною діяльністю слід приділити інформаційним ресурсам (повинні бути достовірними, своєчасними, повними тощо), людським ресурсам (визначають кадрове забезпечення та інформаційну озброєність праці), матеріальним ресурсам (комп’ютеризація інформаційної

	діяльності, інформаційні технології) підприємства
Поточний	Відбувається у процесі діяльності закладу, спрямований на усі види ресурсів підприємства, які використовується для реалізації технологічних операцій щодо одержання, використання,

Продовж.табл.1.2.

1	2
	поширення, зберігання чи вилучення інформації. Якщо інформаційна діяльність підприємства пов'язана із реалізацією та передаванням медичної інформації, то увагу слід звернути на технічні ресурси підприємства
Самоконтроль	Відбувається у процесі діяльності підприємств та реалізується у працівником, який відповідальний за збір, аналіз, використання відповідної медичної інформації шляхом самоперевірки встановленим вимогам
Проміжний	Передбачає визначення рівня досягнення результатів окремих перевірок, відбувається у процесі інформаційної діяльності підприємства
Завершальний	Здійснюється на виході із системи інформаційної діяльності підприємства, пов'язаний із оцінюванням результатів інформаційної діяльності

Джерело: [45, с.160].

Слід звернути увагу, що реалізація внутрішнього контролю за збереженням медичної інформації в закладі охорони здоров'я не повинна переслідувати за собою мету забезпечення інформаційної безпеки та поєднувати або дублювати засоби захисту інформації, а повинна бути спрямована лише на збільшення ефективності діючих засобів захисту медичної інформації, підтримувати процеси розвитку інформаційної безпеки телекомунікаційної структури організації та надавати актуальну інформаційно довідкову підтримку з питань забезпечення збереження персональних даних, з метою своєчасного прийняття коригувальних та попереджувальних впливів та рішень, ґрунтуючись на [33, с.67]:

регламентації процесів захисту інформації;

обліку та класифікації активів, що захищаються;

обліку та класифікації ресурсів системи захисту інформації;

постійному аналізі ризиків інформаційної безпеки та актуалізації моделі загроз інформації

моніторинг подій інформаційної безпеки;

рівні компетенції та професійних можливостей співробітників організації та обслуговуючого персоналу;

ступеня навантаження зайнятості та професійної історії фахівців із захисту інформації;

аналіз накопичених даних з питань інформаційної безпеки.

Таким чином, одними з невід'ємних складових будь-якої системи внутрішнього контролю за збереженням медичної інформації в закладі охорони здоров’я повинні бути регламентація та реалізація механізмів щодо [8, с.250]:

централізованого сигналізування та повідомлення співробітників організації та фахівців із захисту інформації про події всередині системи управління зокрема та системи захисту медичної інформації в цілому;

аналізу подій усередині системи управління та системи захисту медичної інформації, що дозволить суттєво спростити управління інформаційною безпекою та знизити навантаження на аналітиків з інформаційної безпеки.

Специфіка медичної інформації вимагає вибору адекватних методів розв'язання задач, пов'язаних із їх захистом. В даний час відомо безліч методів і алгоритмів підтримки прийняття рішень під час проведення внутрішнього контролю за збереженням медичної інформації в організації.

Багато методів проведення внутрішнього контролю за збереженням медичної інформації в організації засновані на побудові моделі загроз та вразливостей [21;54]. При цьому виділяють методики аудиту, засновані на якісних та кількісних оцінках ризику витоку медичної інформації. У таблиці 1.3 наведено їх порівняльну характеристику.

Методики внутрішнього контролю за збереженням медичної інформації, засновані на якісних оцінках ризику, розроблено на основі вимог міжнародного стандарту ІСО/МЕК 27005-2010. В їх основі лежить використання експертних систем, що включають великі бази знань з загроз і вразливостей і велика кількість запитальників. Відповіді автоматично обробляються, та за допомогою відповідних правил логічного висновку формується підсумковий звіт з поточними оцінками інформаційних ризиків компанії та рекомендаціями щодо їх управлінню.

Таблиця 1.3 - Методики внутрішнього контролю за збереженням медичної інформації, засновані на побудові моделі загроз та вразливостей

Методики, засновані на якісних оцінках ризику	Методики, засновані на кількісній оцінці ризику
Визначають ступінь важливості ризику та вибирають спосіб реагування	Визначають ймовірність виникнення ризиків та вплив наслідків ризиків (втрат)
Дозволяють: проводити аналіз із високою швидкістю; одразу усунути або знизити найнебезпечніші загрози.	Дозволяють: створювати моделі інформаційних активів підприємства; класифікувати та оцінювати цінності активів; складати списки найбільш значущих загроз та вразливостей безпеки; ранжувати загрози та вразливості безпеки; обґрунтовувати засоби та заходи контролю ризиків; оцінювати ефективність/вартість різних варіантів захисту; формалізувати та автоматизувати процедури оцінювання та управління ризиками.
Програмні системи: COBRA, RA Software Tool, CRAMM	Програмні системи: RiskWatch

Джерело: [4;24].

Методики внутрішнього контролю, засновані на кількісних оцінках ризику, дозволяють вирішувати завдання пошуку найкращого (раціонального) рішення з безлічі існуючих [52].

Внутрішній контроль здійснюється у формі планових та позапланових перевірок, що проводяться як у відкритій, так і в негласній формі. Планові перевірки повинні проводитися в закладі з періодичністю згідно прийнятого відповідальним за забезпечення інформаційної безпеки графіка, але не рідше двох разів на рік.

Позапланові перевірки проводяться в закладі у таких випадках: за фактами виникнення інцидентів інформаційної безпеки; при виникненні обставин, що дають підстави вважати, що в закладі може мати місце порушення співробітниками законодавства та внутрішніх документів закладу у частині, що стосується збереженням медичної інформації;

Форма проведення планової чи позапланової перевірки у гласній чи негласній формі вибирається відповідальним за внутрішній контроль на власний розсуд. Гласна перевірка проводиться відкрито для працівників закладу. Негласна перевірка проводиться потай від співробітників закладу, у тому числі тих співробітників, діяльність з збереження медичної інформації яких піддається перевірці.

Таким чином, здійснення внутрішнього контролю гарантує здатність контролерів даних, таких як заклади охорони здоров'я, продемонструвати, що їх діяльність повною мірою підзвітна, а обробка даних здійснюється справедливим і збалансованим чином, що стосується права на інформаційне самовизначення чи право на конфіденційність лише тією мірою, якою це необхідно для дотримання суспільних інтересів у сфері охорони здоров'я.

РОЗДІЛ 2. СУЧАСНИЙ СТАН ОРГАНІЗАЦІЇ ВНУТРІШНЬОГО КОНТРОЛЮ ЗА ЗБЕРЕЖЕННЯМ МЕДИЧНОЇ ІНФОРМАЦІЇ В КП «ХМЕЛЬНИЦЬКЕ ОБЛАСНЕ БЮРО СУДОВО-МЕДИЧНОЇ ЕКСПЕРТИЗИ» ХМЕЛЬНИЦЬКОЇ ОБЛАСНОЇ РАДИ

2.1.Загальна характеристика Хмельницького обласного бюро судово-медичної експертизи та його організаційне забезпечення внутрішнього контролю за збереженням інформації

Хмельницьке обласне бюро судово-медичної експертизи перебуває у комунальній власності, є об’єктом спільної власності територіальних громад сіл, селищ, міст Хмельницької області. Управління Бюро здійснює Хмельницька обласна рада (далі - Орган управління майном). Бюро підзвітне і підконтрольне Органу управління майном.

Хмельницьке обласне бюро судово-медичної експертизи є юридичною особою, має самостійний баланс, поточні та інші рахунки у відповідних установах, печатку із зображенням Державного Герба України і своїм найменуванням, штамп, ідентифікаційний код, інші реквізити відповідно до чинного законодавства, право відкривати рахунки у відповідних установах, укладати правочини (господарські договори і угоди), набувати майнових та особистих немайнових прав, нести обов’язки, бути позивачем та відповідачем в суді, господарському, третейському та адміністративному судах.

Основною діяльністю Бюро є проведення судово-медичної експертизи, що призначається особою, яка проводить дізнання, слідчим, прокурором, суддею чи судом з метою дослідження на підставі спеціальних знань матеріальних об’єктів, що містять інформацію про обставини справи. Головними завданнями Бюро є: забезпечення та проведення судово-медичних експертиз трупів у випадках насильницької смерті або при підозрі

на застосування насильства, а також за інших обставин, що обумовлюють необхідність проведення такої експертизи, для вирішення питань, поставлених особою, яка проводить дізнання, слідчим, прокурором, суддею чи судом; забезпечення та проведення судово-медичної експертизи потерпілих, звинувачених та інших осіб для вирішення характеру та ступеня тяжкості тілесних ушкоджень, з приводу статевих злочинів та вирішення інших питань, поставлених особою, яка проводить дізнання, слідчим, прокурором, суддею чи судом; забезпечення та проведення судово-медичної експертизи речових доказів; забезпечення та проведення судово-медичної експертизи за матеріалами кримінальних та цивільних справ; забезпечення участі судово-медичних експертів у судових засіданнях, а також як фахівців у галузі судової медицини при проведенні невідкладних та інших слідчих дій; Систематичне інформування керівництва закладів охорони здоров'я про всі дефекти та недоліки у наданні медичної допомоги населенню, що були виявлені при проведенні судово-медичних експертиз [47].

Основні фінансові показники діяльності підприємства свідчать, що незважаючи на те, що величина доходів у 2020 р. збільшилась майже в 1,7 рази порівняно із 2019 р. витрати зростали ще вищими темпами (у 2,04 рази) така ситуація відобразилась на зміні величини чистого прибутку, який скоротився на 3,3 млн. грн. або на 36% проти рівня базового року. У структурі доходів найбільшу частку складають доходи від реалізації робіт та послуг (89,8%), водночас в структурі витрат найвагомішою статтею є собівартість реалізованих послуг (74,01%) у т.ч. витрати на оплату праці персоналу – 45,84%. Слід також відзначити, що при зростанні валового прибутку на 5,7 млн. грн. спостерігається скорочення фінансових результатів від операційної діяльності на 3,3 млн. грн. та фінансових результатів від звичайної діяльності до оподаткування на 3,3 млн. грн. [50; 51]. Отже, має місце зниження результативності господарської діяльності комунального підприємства.

Перейдемо до аналізу окремих показників роботи підприємства. Так, за 2020 рік порівняно із 2019 роком в штатному розписі закладу значних змін не відбулося. Кількість штатних одиниць у штатному розкладі становить 169,0 одиниць, які займають 103 фізичні особи, з них: 58,5 штатних одиниць займають 37 лікарів, 51,5 штатних одиниці займають 33 особи середнього медичного персоналу, 40,5 штатних одиниць займає 22 особи молодшого медичного персоналу; 18,5 ставок займає 11 осіб адміністративно-господарського персоналу. Рівень укомплектованості штатних посад по закладу наведено в табл. 2.1.

Таблиця 2.1. Рівень укомплектованості штатних посад

Назва посад згідно штатного розпису	2019 рік		2020 рік	
	по штатному розпису	зайнято	по штатному розпису	зайнято
Лікарі	58,5	53,5	58,5	54,5
Середній медичний персонал	51,5	49,5	51,5	49,5
Молодший медичний персонал	40,5	37,0	40,5	37,25
Адміністративно-господарський персонал	18,5	16,0	18,5	15,0

Примітка. Складено автором за даними Хмельницьке обласне бюро СМЕ.

Як бачимо жодна група посад не укомплектована на 100%, що пов’язано зі специфікою роботи в закладі. В свою чергу укомплектованість судово-медичними експертами і спеціалістами судово-медичної лабораторії виглядає наступним чином (табл. 2.2).

Таблиця 2.2. Укомплектованість судово-медичними експертами і спеціалістами судово-медичної лабораторії у 2020 р.

Назва відділення	штатні одиниці	зайнято	фізичні особи	вакансії
судово-медичної гістології	3,0	3,0	2	-
судово-медичної імунології	6,0	6,0	4	-
судово-медичної цитології	3,0	3,0	2	-
судово-медичної токсикології	8,0	7,0	5	0,5
судово-медичної криміналістики	2,5	2,5	2	-

Примітка. Складено автором за даними Хмельницьке обласне бюро СМЕ.

Укомплектованість судово-медичними експертами у обласному бюро судово-медичної експертизи та міжрайонних (районних) відділеннях виглядає наступним чином (табл. 2.3):

Таблиця 2.3. Укомплектованість судово-медичними експертами у обласному бюро судово-медичної експертизи та міжрайонних (районних) відділеннях у 2020 р.

Районні та міжрайонні відділення	штатні одиниці	фізичні особи
обласне бюро СМЕ в тому числі керівного складу	18,25	10
Волочиське міжрайонне відділення	1,25	1
Дунаєвецьке міжрайонне відділення	2,0	2
Кам'янець-Подільське міжрайонне відділення	3,0	2
Летичівське міжрайонне відділення	1,5	1
Шепетівське міжрайонне відділення Нетішинська філія	3,0 1,5	2 1
Ярмолинецьке міжрайонне відділення	1,5	1
Старокостянтинівське районне відділення	1,5	1
Красилівське районне відділення	1,5	1
Городоцьке районне відділення	1,0	1

Примітка. Складено автором за даними Хмельницьке обласне бюро СМЕ.

За 2020 рік у бюро було виконано наступну кількість експертиз відповідно по відділах та відділеннях (табл. 2.4).

Таблиця 2.4. Кількість висновків експертиз відповідно по відділах та відділеннях Хмельницького обласного бюро судово-медичної експертизи

Назва структурного підрозділу	2019 рік		2020 рік		Збільшено об'єму роботи	Зменшено об'єму роботи
1	2		3		4	5
Відділ судово-медичної експертизи трупів	розтини	додаткові	розтини	додаткові	14%	
	2039	40	2232	137		
Відділ судово-медичної експертизи потерпілих, звинувачених та інших осіб	2832		4472		58%	
Відділ комісійних судово-медичних експертиз	161		44			73%
Відділення судово-медичної токсикології	2355		2564		9%	
Відділення судово-медичної криміналістики	80		70			12,5%

Продовж.табл.2.4

1	2	3	4	5
Відділення судово-медичної цитології	200	353	76,5%	
Відділення судово-медичної імунології	840	1660	97,6%	
Відділення судово-медичної гістології	1664	1780	7%	
ВСЬОГО:	10171	13312	31%	

Примітка. Складено автором за даними Хмельницьке обласне бюро СМЕ.

Тепер перейдемо до дослідження сучасного стану організації внутрішнього контролю за збереженням інформації в закладі охорони здоров'я

Призначення системи внутрішнього контролю за збереженням інформації Хмельницького обласного бюро судово-медичної експертизи 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 збереженням інформації Хмельницького обласного бюро судово-медичної експертизи обумовлюються його призначенням і полягають у:

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

– організації надійного доступу до інформації;

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

– створенні правил безпечної роботи з інформацією;

– проведенні заходів щодо резервування інформації;

– забезпеченні відновлення інформації в аварійних ситуаціях;

– підтримці інформаційної безпеки на заданому рівні.

В нинішній час для забезпечення належного стану внутрішнього контролю за збереженням інформації Хмельницького обласного бюро судово-медичної експертизи 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.).

Для забезпечення захисту інформаційного середовища Хмельницького обласного бюро судово-медичної експертизи 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.

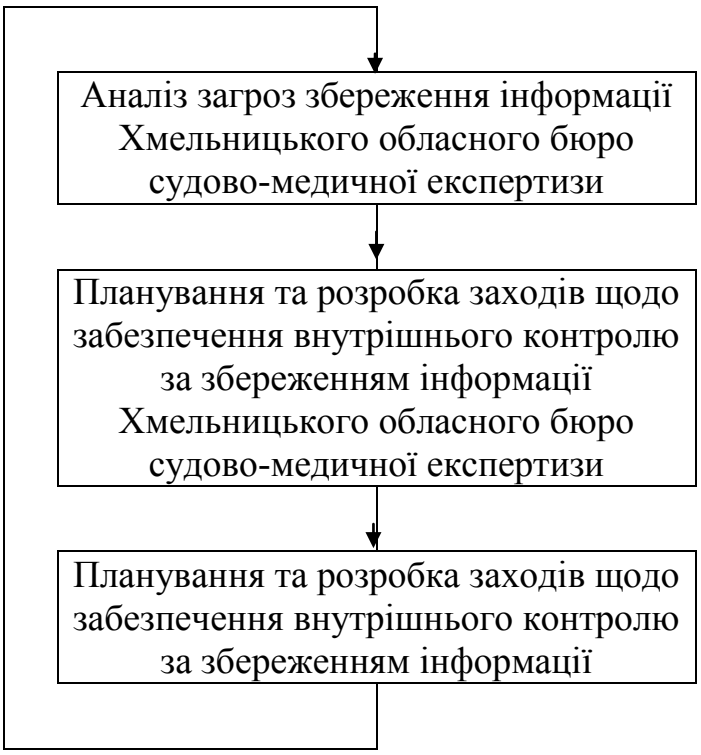

Рисунок 2.1 - Схема функціонування системи внутрішнього контролю за збереженням інформації Хмельницького обласного бюро судово-медичної експертизи

Примітка. Складено автором.

Функції щодо внутрішнього контролю за збереженням інформації Хмельницького обласного бюро судово-медичної експертизи розподілено між начальником, його заступниками та організаційно-методичним відділом медичного закладу. Основний перелік функції щодо інформатизації та захисту інформації закладу охорони здоров’я покладено на організаційно-методичний відділ Хмельницького обласного бюро судово-медичної експертизи.

Організаційно-методичний відділ Хмельницького обласного бюро судово-медичної експертизи здійснює реалізацію державної політики в службі медичної статистики та інформатизації галузі охорони здоров'я. Відділ очолює завідувач, який призначається та звільняється з посади начальником Хмельницького обласного бюро судово-медичної експертизи.

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 організаційно-методичний відділ Хмельницького обласного бюро судово-медичної експертизи 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, 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 організаційно-методичного відділу Хмельницького обласного бюро судово-медичної експертизи. 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 Хмельницькому обласному бюро судово-медичної експертизи передбачено наявність: організаційно-методичного 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 [43] 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 [20, с.171].

Одним із завдань організаційно-методичного відділу Хмельницького обласного бюро судово-медичної експертизи, 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 організаційно-методичного відділу Хмельницького обласного бюро судово-медичної експертизи передбачено такі регламентувальні документи: перелік нормативно-правових актів щодо обліку та звітності у закладах охорони здоров'я; графік надання звітної інформації підрозділами та службами до інформаційно-аналітичного відділу. У цьому графіку визначають відповідальних за збирання та звіряння інформації з первинною документацією осіб, а також строки подання інформації, осіб, яким надається інформація, споживачів та особу, що аналізує інформацію; схему взаємодії відділу з трирівневим джерелом інформації; схему інформаційного медичного статистичного забезпечення закладу; схему руху директивної інформації.

Однією із функцій організаційно-методичного відділу Хмельницького обласного бюро судово-медичної експертизи 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 організаційно-методичний відділ Хмельницького обласного бюро судово-медичної експертизи 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 організаційно-методичний відділ Хмельницького обласного бюро судово-медичної експертизи 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 Хмельницькому обласному бюро судово-медичної експертизи форм державної та галузевої статистичної звітності, передбаченої чинним законодавством, працівниками організаційно-методичного відділу Хмельницького обласного бюро судово-медичної експертизи 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 збереженням інформації медичного закладу здійснюється організаційно-методичним відділом Хмельницького обласного бюро судово-медичної експертизи, діяльність якого тісно пов'язана з іншими підрозділами. Від організації роботи організаційно-методичного відділу, підбору фахівців, їхніх особистих якостей залежить якість лікувально-діагностичного процесу та наявність достовірної перевіреної інформації у менеджменту закладу.

2.2. Оцінювання рівня захищеності інформації в закладі охорони здоров'я

Питання можливості надання інформації, що становить лікарську. таємницю в медичних закладах є досить актуальним, оскільки у зв'язку з

незнанням норм права, медичний персонал чітко не може зорієнтуватися яка саме інформація становить лікарську таємницю та в яких випадках і в якому обсязі вона може бути надана особам, які звертаються з усними та письмовими запитами щодо такої інформації.

Для ефективного здійснення оцінювання рівня захищеності інформації у Хмельницькому обласному бюро судово-медичної експертизи необхідно чітко визначити межі предмета такого захисту. У нашому випадку йдеться про сукупність певних відомостей (інформації) медичного характеру в першу чергу щодо пацієнта.

Особливість правового статусу пацієнта, тобто фізичної особи, яка звернулася за медичною допомогою та (або) якій надається така допомога, як суб'єкта персональних даних має свої особливості. Насамперед, інформація про стан здоров'я, належать до так званої «чутливої» інформації [3, с. 190], а тому підпадає під дію особливих вимог до обробки персональних даних (ст. 7 Закону України «Про захист персональних даних»).

Більше того, персональні дані пацієнта, а саме: відомості про стан свого здоров'я, факт звернення за медичною допомогою, діагноз, а також про відомості, одержані при його медичному обстеженні, охоплюються правом на таємницю про стан здоров'я (ст. 391 Основ законодавства України про охорону здоров'я [35]); відомості про хворобу, медичне обстеження, огляд та їх результати, інтимну і сімейну сторони життя громадянина підпадають під правовий режим лікарської таємниці (ст. 40 Основ законодавства України про охорону здоров'я [35]).

Дотримання конфіденційності відомостей про здоров'я становить основний принцип діяльності Хмельницького обласного бюро судово-медичної експертизи. Він є важливим не лише для захисту приватного життя хворих, а й для збереження їхньої довіри до працівників медичних закладів і системи охорони здоров'я загалом.

Саме тому в Україні запроваджено електронну систему охорони здоров'я (ст. 11 Закону України «Про державні фінансові гарантії медичного

обслуговування населення» [40]) – інформаційно-телекомунікаційну систему, що забезпечує автоматизацію ведення обліку медичних послуг та управління медичною інформацією шляхом створення, розміщення, оприлюднення та обміну інформацією, даними і документами в електронному вигляді, до складу якої входять центральна база даних та електронні медичні інформаційні системи, між якими забезпечено автоматичний обмін інформацією, даними та документами через відкритий програмний інтерфейс (API).

Пацієнт (чи його законний представник) шляхом підписання декларації про вибір лікаря, який надає первинну медичну допомогу, підтверджує те, що усвідомлює мету збирання і обробки своїх персональних даних. Тобто, підписуючи декларацію з терапевтом, педіатром чи сімейним лікарем, людина погоджується, що її персональні дані (чи дані її дитини/підопічного (недієздатної особи)) в електронній системі будуть доступні для обробки лікарем, з яким укладено декларацію, та лікарями, до яких вона звертатиметься за медичною допомогою за направленням свого лікаря. У подальшому в межах компетенції та напрямків діяльності Хмельницького обласного бюро судово-медичної експертизи зазначені дані підлягають використанню та обробці на тих саме правових засадах.

Так, пацієнт особисто і законний представник мають право:

1) знати про місцезнаходження персональних даних, яка містить його персональні дані, її призначення та найменування, місцезнаходження та/або місце проживання (перебування) володільця чи розпорядника персональних даних або дати відповідне доручення щодо отримання цієї інформації уповноваженим ним особам, крім випадків, встановлених законом;

2) отримувати інформацію про умови надання доступу до персональних даних, зокрема інформацію про третіх осіб, яким передаються його персональні дані;

3) на доступ до своїх персональних даних;

4) отримувати не пізніш як за тридцять календарних днів з дня надходження запиту, крім випадків, передбачених законом, відповідь про те, чи зберігаються його персональні дані у відповідній базі персональних даних, а також отримувати зміст його персональних даних, які зберігаються;

5) пред'являти вмотивовану вимогу володільцю персональних даних із запереченням проти обробки своїх персональних даних;

6) пред'являти вмотивовану вимогу щодо зміни або знищення своїх персональних даних будь-яким володільцем та розпорядником персональних даних, якщо ці дані обробляються незаконно чи є недостовірними;

7) на захист своїх персональних даних від незаконної обробки та випадкової втрати, знищення, пошкодження у зв'язку з умисним приховуванням, ненаданням чи несвоєчасним їх наданням, а також на захист від надання відомостей, що є недостовірними чи ганьблять честь, гідність та ділову репутацію фізичної особи;

8) звертатися із скаргами на обробку своїх персональних даних до органів державної влади та посадових осіб, до повноважень яких належить забезпечення захисту персональних даних, або до суду;

9) застосовувати засоби правового захисту в разі порушення законодавства про захист персональних даних;

10) вносити застереження стосовно обмеження права на обробку своїх персональних даних під час надання згоди;

11) відкликати згоду на обробку персональних даних;

12) знати механізм автоматичної обробки персональних даних;

13) на захист від автоматизованого рішення, яке має для нього правові наслідки [13].

Персональні дані пацієнта обробляються різноманітними за своїм правовим статусом суб'єктами, а саме: медичним працівником або іншою особою закладу охорони здоров'я чи фізичною особою-підприємцем, яка одержала ліцензію на провадження господарської діяльності з медичної практики, та її працівниками, на яких покладено обов'язки щодо

забезпечення захисту персональних даних та на яких поширюється дія законодавства про лікарську таємницю, працівниками центрального органу виконавчої влади, що реалізує державну політику у сфері державних фінансових гарантій медичного обслуговування населення, на яких покладено обов'язки щодо забезпечення захисту персональних даних.

Персональні дані пацієнтів у електронну систему охорони здоров'я можуть вводити визначені медичним закладом уповноважені особи. Це може бути медичний працівник або інша уповноважена особа закладу охорони здоров'я, лікар-ФОП, який має ліцензію на провадження господарської діяльності з медичної практики, та його працівники. На них має поширюватися дія законодавства про лікарську таємницю і вони повинні забезпечувати захист цих персональних даних. Ці працівники зобов'язані не допускати розголошення у будь-який спосіб персональних даних, які їм було довірено або які стали відомі у зв'язку з виконанням професійних чи службових, чи трудових обов'язків, крім випадків, передбачених законом.

Персоналізовані дані (усі дані про пацієнта, які містяться в декларації, а із запровадженням електронного рецепта й електронної медичної картки — медична інформація та призначення) доступні тільки лікарю, з яким підписана декларація, та лікарю, до якого пацієнт приходить за направленням. Коли у системі з'являться медичні дані, пацієнт зможе сам вирішувати, кому він додатково надає доступ.

Слід зазначити, що дія Закону України «Про захист персональних даних» поширюється на всіх суб'єктів господарської діяльності в медичній сфері не залежно від форми власності та відомчого підпорядкування у тому числі і у Хмельницькому обласному бюро судово-медичної експертизи.

У зв'язку з цим прийнята Постанова Кабінетом Міністрів України від 06.06.2012 р. № 546 «Про затвердження електронного реєстру пацієнтів» (далі – реєстр) [41], яка прийнята на виконання Національного плану дій на 2012 рік щодо впровадження Програми економічних реформ на 2012-2014 роки, [44] якою передбачено створення Електронного реєстру пацієнтів.

Електронний реєстр пацієнтів – це єдина державна інформаційна система збирання, реєстрації, накопичення відомостей про пацієнта та отриману медичну допомогу. Реєстр створюється з метою підвищення ефективності медичної допомоги, забезпечення своєчасності її надання, модернізації первинної медичної допомоги. Електронний реєстр пацієнтів не відміняє ведення облікових форм на паперових носіях. Збір, обробка та внесення до Реєстру даних про пацієнта буде здійснюватися виключно за його згодою. Реєстр створюється з метою підвищення ефективності медичної допомоги, забезпечення своєчасності її надання та достовірності статистичної інформації. Він є єдиною інформаційною системою збирання, реєстрації, накопичення, зберігання, оновлення, використання і поширення шляхом розповсюдження, реалізації, передачі, а також знищення відомостей про фізичну особу та отриману нею медичну допомогу.

Реєстр є інформаційним ресурсом Міністерства охорони здоров'я (далі – МОЗ), який ведеться з використанням інформаційних технологій, електронного документообігу та електронного цифрового підпису. Зазначу, що заклади охорони здоров'я усіх форм власності зобов'язані вносити до Реєстру відомості про: 1) фізичну особу, що містяться у затверджених наказами МОЗ медичних облікових формах; 2) заклад охорони здоров'я, в якому пацієнтові надано медичну допомогу; 3) вид наданої пацієнтові медичної допомоги; 4) лікарські засоби та вироби медичного призначення, закуплені для лікування пацієнта за кошти державного та місцевих бюджетів; 5) згоду пацієнта на обробку персональних даних за встановленою МОЗ формою. Основною інформаційною одиницею для Реєстру є форма первинної облікової документації № 025/о «Медична карта амбулаторного хворого», затверджена наказом Міністерства охорони здоров'я України від 14 лютого 2012 року № 110, зареєстрованим у Міністерстві юстиції України 28 квітня 2012 року за № 661/20974 [15]. Володільцями реєстру є заклади охорони здоров'я.

Таким чином, функціонування електронної системи охорони здоров'я на рівні Хмельницького обласного бюро судово-медичної експертизи повинно здійснюватися з урахуванням вимог законодавства про захист персональних даних. Особливості обробки персональних даних пацієнтів спонукають науковців виділити кілька ключових положень, які формуватимуть алгоритм дій при обробці персональних даних у сфері охорони здоров'я [46, с. 218–220].

Покладання на володільців, розпорядників персональних даних та третіх осіб ризику випадкових втрати або знищення персональних даних має ще одне значення, а саме розподіл обов'язку доказування.

Електронна система охорони здоров'я спроектована для роботи з персональними даними з дотриманням кращих світових практик у сфері захисту даних. Система знаходиться на серверах дата-центру в Україні, який має комплексну систему захисту інформації (КСЗІ) та пройшов атестацію у Державній службі спеціального зв'язку та захисту інформації (ДССЗЗІ).

Володільці реєстру за наявності згоди пацієнтів на обробку їх персональних даних вносять інформацію до реєстру, обробляють її та забезпечують захист персональних даних, що вносяться до реєстру. Обмін відомостями між ЗОЗ ведеться за допомогою телекомунікаційної мережі із забезпеченням захисту інформації відповідно до вимог законодавства. Важливим аспектом є й те, що впровадження електронного реєстру пацієнтів розпочалося з Вінницької, Дніпропетровської, Донецької областей та м. Києва [42]. Джерелами формування Реєстру є паспортні документи або інші документи, що ідентифікують особу, та первинна облікова документація закладів охорони здоров'я. Реєстр формується шляхом створення електронних баз даних з метою максимальної автоматизації накопичення і обробки інформації. Підставою для внесення фізичної особи (пацієнта) до Реєстру є факт звернення пацієнта до закладу охорони здоров'я та наявність його письмової згоди на обробку персональних даних.

Введення електронного реєстру пацієнтів викликає ряд проблем через високу вартість утримання бази даних, неврегульованість відмови та конкретного порядку знищення персональних даних медичних працівників та пацієнтів.

Визначення вимог до безпеки системи захисту персональних даних проводиться шляхом методичної оцінки ризиків. Витрати на підтримку безпеки необхідно збалансувати з шкодою для установи, який може виникнути при порушенні безпеки. Методи оцінки небезпек можуть застосовуватися до всієї організації або лише до її частин, а також до окремих інформаційних систем, системних компонентів і сервісів, в залежності від того, що виявиться найбільш практичним, реалістичним і корисним. Враховуючи відсутність затверджено на національному чи відомчому рівні методики оцінки захищеності медичної інформації, розглянемо можливість використання для такої цілі вХмельницькому обласному бюро судово-медичної експертизи метод експертного оцінювання. Суть методу полягає в тому, що експерти проводять інтуїтивнологічне дослідження проблеми, у межах якого дають кількісну оцінку суджень, що завершується формальною обробкою результатів. Вирішенням проблеми при застосуванні цього методу вважається отримана в в результаті обробки узагальнена думка експертів. Ефективність такого рішення досягається за рахунок того, що інтуїція, логічне мислення та кількісні оцінки з їхньою формальною обробкою використовуються в комплексі.

Враховуючи класифікацію медичної інформації за рівнем доступу, вимогами щодо її зберігання та особливостями організації процесу збереження та контролю оцінимо рівень захищеності інформації в закладі охорони здоров’я за критеріями, наведеними у додатку А. Результати оцінювання представимо у таблиці 2.5.

Оцінювання пропонується здійснювати в рамках двох складових: оцінка організаційно-методичного та технічного забезпечення внутрішнього контролю (наявність відповідних процедур, регламентів, технічних засобів

тощо) та оцінка дієвості внутрішнього контролю за збереженням медичної інформації (підтверджується кількістю скарг ти позовів до закладу через випадки порушення законодавства у сфері захисту персональних даних).

Таблиця 2.5 Результати оцінювання рівня захищеності медичної інформації в Хмельницькому обласному бюро судово-медичної експертизи

Параметр	Показники параметру	Значення показника параметра
Оцінка організаційно-методичного та технічного забезпечення внутрішнього контролю		
Вид носія інформації (Документації).	Використовуються паперові та електронні версії документів. Централізований архів документів відсутній.	4
Ступінь безпеки (захищеності) інформаційного потоку	Конфіденційна інформація зберігається без використання спеціалізованого ПЗ. Регламент доступу розроблено Використовуються засоби захисту конфіденційної інформації, що озвучується. Ступінь захисту не достатній. Регламент відсутній	2
Ступінь відповідності комплексної системи захисту інформаційної системи (КСЗІ) вимогам нормативних документів системи технічного захисту інформації	використовуються комп'ютерні програми (їх оновлення), в яких немає недокументованих функцій, однак це не підтверджено результатами державної експертизи у сфері захисту інформації. Наявні випадки циркуляції інформаційні потоки з обмеженим доступом циркулюють із використанням неслужбових ПО	3
Ступінь розвитку організаційного забезпечення внутрішнього контролю за збереженням медичної інформації	Рішення про організацію внутрішнього контролю за збереженням медичної інформації відсутнє. Здійснюється окремі процедури у сфері контролю за збереженням медичної інформації, однак відповідні регламенти відсутні.	2
Оцінка дієвості внутрішнього контролю за збереженням медичної інформації		
Наявність скарг, пов'язаних з недотриманням вимог захисту персональних даних	Наявні протягом звітного періоду та знайшли своє підтвердження	0
Наявність звернень до Уповноваженого ВРУ з прав людини щодо випадків недотримання вимог захисту персональних даних	Відсутні протягом звітного періоду або не знайшли своє підтвердження	5
Юрисдикційні звернення (позови до судів) щодо випадків недотримання вимог захисту персональних даних	Наявні протягом звітного періоду та знайшли своє підтвердження	0
Притягнення до відповідальності працівників	Відсутні через відсутність складу правопорушення або обставин, що виключають відповідальність або змінено (скасовано) за рішенням суду	5

Примітка. Запропоновано автором.

Таким чином, використання пропонованого підходу до оцінювання стану захищеності інформації вХмельницькому обласному бюро судово-медичної експертизи дозволило не лише ідентифікувати рівень інформаційної захищеності установи, але й визначити напрями підвищення ефективності використання інформаційних ресурсів та окреслити напрями посилення захищеності медичної інформації. Після завершення заходів щодо підвищення ефективності захисту медичної інформації, таку процедуру оцінювання необхідно здійснити повторно.

РОЗДІЛ 3. НАПРЯМИ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ВНУТРІШНЬОГО КОНТРОЛЮ ЗА ЗБЕРЕЖЕННЯМ ІНФОРМАЦІЇ В ЗАКЛАДІ ОХОРОНИ ЗДОРОВ'Я

3.1. Удосконалення організаційного забезпечення внутрішнього контролю за збереженням інформації в закладі охорони здоров'я

Наявність діючої ефективної системи внутрішнього контролю за збереженням інформації в закладі охорони здоров'я є основою для дієвого управління інформаційною безпекою в цілому через посилення захисту та недопущення витоку медичної інформації, використання її в особистих цілях тощо. Специфіка медичної інформації полягає у тому, що її безпеку гарантується на рівні законодавства, так само, як і на рівні законодавства встановлюються певні заборони та юридична відповідальність за її розголошення. Як розглядалось вище, у вітчизняному законодавстві не визначено конкретні вимоги захисту відомостей, які стосуються лікарської таємниці, дані вимоги визначено законодавством у сфері персональних даних.

Необхідність удосконалення організації внутрішнього контролю викликане прагненням власника економічного суб'єкту - обласної ради - отримати об'єктивну і незалежну оцінку дій керівників усіх рівнів управління; необхідністю дотримання законодавства у сфері захисту інформації, зокрема персональних даних; підвищенням ступеню довіри з боку третіх сторін; зниженням інформаційних ризиків тощо. В нових умовах внутрішній контроль повинен активно інтегрувати в усі функції менеджменту, організаційну діяльність підприємства, забезпечуючи не лише інформацію про якість системи управління інформаційною безпекою, але й формування пропозицій щодо удосконалення процесів збереження інформації в закладі охорони здоров'я [12, с.215].

Питання організації внутрішнього контролю за збереженням інформації в закладі охорони здоров'я потребує вирішення наступного кола питань: форми організації, функціональних обов'язків осіб, що здійснюють внутрішній контроль, підпорядкованість внутрішнього контролю в системі управління підприємством, напрями контрольної діяльності на підприємстві. Вирішення цих питань повинно здійснюватися із врахуванням інтересів всіх зацікавлених сторін [11, с.76].

Виходячи зі проведеного дослідження теоретичних засад забезпечення інформаційної безпеки в закладі охорони здоров'я, можемо визначити наступні пріоритетні напрями удосконалення організаційного забезпечення внутрішнього контролю за збереженням інформації (табл.3.1).

Таблиця 3.1 Напрями удосконалення організаційного забезпечення внутрішнього контролю за збереженням медичної інформації

Складові	Напрями удосконалення	Результат
1	2	3
Інформаційно-аналітичне забезпечення внутрішнього контролю	Впровадження сучасних інформаційних систем аудиту КСЗІ	Підвищення точності аудиту стану збереження інформації. Виявлення потенційних ризиків втрат внаслідок розголошення/ витоку і несанкціонованого доступу до джерел інформації
Систематичне здійснення аудиту КСЗІ	Залучення зовнішніх аудиторів або організація служби (введення посади)	Зменшення ризиків інформаційної та кібербезпеки в установі. Уникнення втрат внаслідок розголошення/ витоку і несанкціонованого доступу до джерел інформації
Методичне забезпечення внутрішнього контролю за збереженням інформації та організації аудиту КСЗІ	Розробка алгоритмів, прийомів, методів, способів і засобів внутрішнього контролю за збереженням медичної інформації та системи управління інформаційною безпеки	Формалізація процедур внутрішнього контролю за збереженням медичної інформації Контроль ефективності профілів ризику та внесення змін на підставі оновлених даних. Визначення чинників ризику інформаційної та кібернебезпеки, надання пропозицій щодо розробки та формалізації конкретних профілів ризику

Продовж.табл.3.1

1	2	3
Кадрове забезпечення	Забезпечення установи компетентними працівниками у сфері внутрішнього контролю за збереженням медичної інформації.	Належне виконання покладених обов'язків та забезпечення бажаного рівня інформаційної та кібербезпеки безпеки Можливість оперативного та прямого втручання в діяльність структурних підрозділів з питань медичної інформації
Формування культури користування медичною інформацією	Проведення тренінгів/вебінарів з питань захисту персональних даних та кібербезпеки	Забезпечення безпеки робочого середовища, попередження ризиків, пов'язаних із зовнішніми атаками та внутрішніми вразливостями . Зменшення загроз та вразливостей

Примітка. Складено автором.

Ми пропонуємо такі варіанти створення служби внутрішнього контролю вХмельницькому обласному бюро судово-медичної експертизи: включення функцій контролю в посадові інструкції працівників інформаційно-аналітичного відділу; формування окремого підрозділу (служби) внутрішнього контролю, що підпорядковується безпосередньо власнику закладу; впровадження посади – фахівця (контролера) із захисту персональних даних. Альтернативним варіантом також може бути укладання угоди на надання відповідних послуг незалежним аудиторським фірмами (аутсорсинг), однак на нашу думку такі підприємства не повною мірою можуть враховувати специфіку діяльності бюро судово-медичної експертизи, крім того це призводитиме до підвищення ризику витоку інформації за межі закладу.

Перший варіант організації внутрішнього контролю (включення функцій аудиту в посадові інструкції існуючих посад інформаційно-аналітичного відділу) не вирішить проблеми, яка притаманна контрольній діяльності за збереженням медичної інформації – поєднання як функцій забезпечення інформаційної безпеки, так і здійснення організаційно-юридичного аудиту, контрольних процедур і заходів усунення проблем в межах одного суб'єкта.

Враховуючи, що Хмельницьке обласне бюро судово-медичної експертизи відноситься до малих за чисельністю працівників підприємств, найбільш адекватним варіантом є введення в організаційну структуру окремої посади. Головним аргументом на користь такого рішення є те, що забезпечити ґрунтовний аналіз та контроль за збереженням медичної інформації спроможний лише структурно відокремлений підрозділ внутрішнього аудиту. При цьому необхідно враховувати наявність територіально відокремлених структурних підрозділів - міжрайонних відділень, які також будуть об'єктами внутрішнього контролю.

Для забезпечення об'єктивності оцінок та неупередженості висновків щодо стану збереження медичної інформації та інформаційної безпеки вцілому під час перевірок така служба повинна підпорядковуватись безпосередньо власнику підприємства - Хмельницькій обласній раді. Місце підрозділу внутрішнього контролю за збереженням медичної інформації в організаційно-управлінській структурі закладі охорони здоров'я виходить з того, що це самостійний підрозділ, який підпорядковуватиметься виключно власнику (Хмельницькій обласній раді), що забезпечить його функціонування на основі принципів об'єктивності та незалежності. У випадку підпорядкування власнику (а не директору) служба за своїми повноваженнями не лише безпосередньо контролює стан захищеності об'єктів аудиту, але і опосередковано контролює дії керівництва підприємства, інших структурних підрозділів тощо. При такій організації внутрішні аудитори набувають широких повноважень, право оперативного та прямого втручання в діяльність всіх підрозділів підприємства.

Підпорядкованість та сфера впливу підрозділу внутрішнього контролю зображено на рис. 3.1. Рішення про впровадження внутрішнього контролю за збереженням медичної інформації в закладі охорони здоров'я, а також уся документація щодо його функціонування затверджується відповідним наказом.

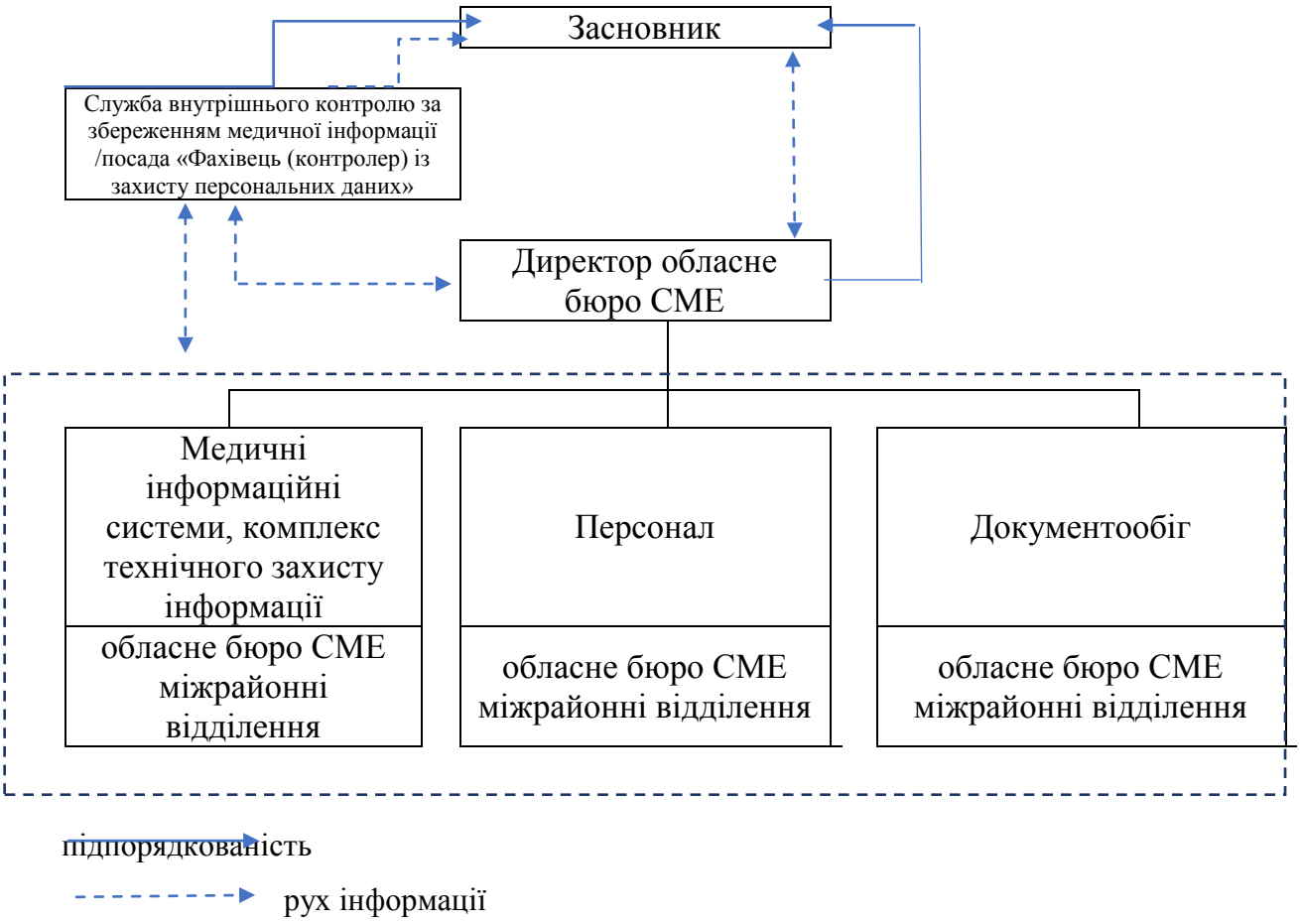

Рисунок 3.1 – Підпорядкованість служби внутрішнього контролю за збереженням медичної інформації в закладі охорони здоров’я

Примітка. Запропоновано автором.

Контролер даних повинен також забезпечувати наявність відповідних можливостей для аудиту захисту даних та сприяти аудиторам, які проводять перевірку від імені органів захисту даних. Під аудитом захисту даних мається на увазі систематична та незалежна перевірка відповідності діяльності, пов'язаної з обробкою персональних даних, внутрішньої політики та процедур у сфері захисту даних, а також вимогам відповідної нормативної бази.

Основними внутрішніми документами щодо організації внутрішнього контролю за збереженням медичної інформації в закладі охорони здоров’я повинно стати Положення про службу внутрішнього контролю за збереженням медичної інформації в закладі охорони здоров’я та посадові

інструкції внутрішніх аудиторів (працівників відділу внутрішнього контролю за збереженням медичної інформації).

Необхідні організаційні процедури створення в Хмельницькому обласному бюро судово-медичної експертизи служби внутрішнього контролю можливо представити таким чином (табл. 3.2).

Таблиця 3.2. Організаційні процедури створення служби внутрішнього контролю за збереженням медичної інформації в закладі охорони здоров'я

Етап	Характеристика
Початковий етап	Регламентування діяльності служби внутрішнього контролю (визначення місця в організаційній структурі, встановлення чітких завдань і функцій служби)
	Методичне та технічне забезпечення служби (регламентів, планів, програм, робочих документів, посадових інструкцій працівників служби, графіків аудиторських перевірок тощо; програмне та інформаційне забезпечення)
	Оцінка ризиків на основі ризикоутворюючих факторів
Планування діяльності	Визначення та вибір об'єктів організаційно-юридичного аудиту
	Вибір показників, які будуть використані при здійсненні організаційно-юридичного аудиту
	Розробка плану, програми організаційно-юридичного аудиту
	Визначення термінів здійснення організаційно-юридичного аудиту певного об'єкту
	Вибір джерел інформації
	Визначення робочих документів
Здійснення	За допомогою прийомів документального або фактичного контролю
Оцінка та аналіз результатів	Визначення факторів та причин відхилень (помилка чи шахрайство); винних осіб, які призвели до відхилень
	Вивчення отриманих результатів, їх систематизація, аналіз та оцінка
	Розробка рекомендацій
Підготовка пропозицій	Оформлення та представлення результатів користувачам інформації у вигляді аналітичний звітів із пропозиціями по усуненню виявлених невідповідностей.
Моніторинг упровадження рекомендацій	Подальший контроль, згідно з прийнятим календарним графіком, за впровадженням змін.

Примітка. Запропоновано автором.

На початковому етапі повинні бути забезпечені необхідні умови для ефективного функціонування служби внутрішнього контролю (або окремої посадової особи). Так, мають бути розроблені та затверджені регламенти щодо діяльності та правового статусу підрозділу внутрішнього контролю або посади фахівця (контролера) із захисту персональних даних, сформовано методичне забезпечення його проведення. Підрозділ внутрішнього контролю або фахівець (контролер) із захисту персональних даних повинні бути

забезпечені необхідними технічними засобами для належного виконання своїх обов’язків.

Для того, щоб внутрішній контроль був ефективним, необхідним є здійснення планування діяльності, формування плану-графіку перевірок тощо. На даному етапі необхідно здійснити вибір об’єктів контролю, визначити обсяг та складність роботи відповідно до мети, поставленої перед підрозділом внутрішнього контролю та специфіки діяльності закладу охорони здоров’я. Етап планування внутрішнього контролю за збереженням медичної інформації в закладі охорони здоров’я включає також розробку планів-графіків, програми та форм робочих документів для здійснення перевірок на підприємстві, що затверджуються власником підприємства.

На цьому етапі необхідним є здійснення інвентаризації інформаційних активів та оцінки інформаційних ризиків, які властиві діяльності закладу. Інформаційний актив – інформація з реквізитами, які дозволяють її ідентифікувати та яка має цінність для організації та представлена на будь-якому матеріальному носії в придатній для її обробки, зберігання чи передачі формі. Основними цілями категорування та інвентаризації інформаційних активів є [17, с.45]:

- ведення обліку активів та забезпечення впевненості у їх захищеності;

- ідентифікація власників ресурсів та визначення їх відповідальності за підтримання відповідних заходів щодо виконання вимог інформаційної безпеки;

- ідентифікації відносної цінності та важливості ресурсів для управління ризиками;

- надійне зберігання та захист інформаційних активів;

- ефективне використання інформаційних активів у діяльності Університету.

- створення основи для диференційованого підходу до захисту активів автоматизованої системи (інформації, завдань, каналів, робочих місць) на

основі їхньої класифікації за ступенем ризику у разі порушення їх доступності, цілісності чи конфіденційності.

Інвентаризація інформаційних ресурсів повинна здійснюватися інвентаризаційною групою на чолі із фахівцем (контролер) із захисту персональних даних. Така група затверджується директором підприємства, до її складу може входити працівники організаційно-методичного відділу або інші працівники, що знають особливості збереження медичної інформації. У процесі категорування активів необхідно оцінити критичність активів медичного закладу, іншими словами, визначити, яку шкоду зазнає заклад у разі порушення інформаційної безпеки. Результатом інвентаризації є формування «Переліку інформаційних ресурсів» підприємства, яке постійно підтримується в актуальному стані та дозволяє забезпечити документоване відображення складу та структури інформаційних активів. «Перелік інформаційних ресурсів» пропонуємо формувати у формі таблиці (табл.3.3).

Таблиця 3.3 Реєстр інформаційних активів в Хмельницькому обласному бюро судово-медичної експертизи

Назва	Короткий зміст	Рівень безпеки			Місце зберігання	Відповідальна особа
		К*	Ц**	Д***		
Матеріали СМЕ (кримінальні впровадження)	Дослідження зразків, виявлених на місцях вчинення кримінальних правопорушень, осіб, причетних до кримінальних правопорушень, потерпілих	Т	В	ВД	_____ (матеріальний носій інформації, місце зберігання на ньому тощо)	_____ *(Прізвище І., посада)*
Матеріали СМЕ (цивільні впровадження)	Дослідження зразків та висновки у цивільних справах	К	В	ВД	_____ (матеріальний носій інформації, місце зберігання на ньому тощо)	_____ *(Прізвище І., посада)*
…..						

* відомості про рівень конфіденційності інформації, що міститься в даному інформаційному активів („таємна“ (Т), „конфіденційна“ (К), „відкрита“ (В)),

** відомості про рівень цілісності („висока“ (ВЦ), „середня“ (СЦ), „низька“ (НЦ — немає вимог)),

** відомості про рівень доступності („висока доступність“ (ВД), „середня доступність“ (СД), „низька доступність (НД -немає вимог));

Примітка. Запропоновано автором

Основними складнощами при проведенні інвентаризаційних робіт є організаційно-технічні заходи щодо збору інформації про інформаційні активи від підрозділів, нерозуміння керівниками значимості та специфіки проведення роботи. Крім того, працівники не завжди правильно класифікують інформаційній активи за рівнем конфіденційності, цілісності та доступності. Тому інвентаризаційна група необхідно ретельно підготуватися до процесу: внести чіткість і однозначність у використовувані поняття, що стосуються призначення, змісту, складу та структури інформаційних активів; скласти попередній список можливих інформаційних активів, специфічних для підрозділу; передбачити автоматизовані засоби обробки більших обсягів отриманої інформації. Уникненню цих проблем сприяє розроблення на підприємстві відповідних Методичних інструкцій інвентаризації інформаційних активів, ознайомлення усіх працівників, проведення роз’яснень тощо.

Наступною ключовою процедурою в рамках здійснення внутрішнього контролю за збереженням медичної інформації є ідентифікація ризику. Заклади охорони здоров'я повинні пам'ятати про різноманітність ризиків, пов'язаних з порушеннями в галузі захисту даних, головним з яких є репутаційні збитки. Аналіз ризику може бути виконаний з різною ступенем деталізації залежно від критичності інформаційних активів, поширеності відомих вразливостей та колишніх інцидентів, що стосувалися організації. При аналізі ризиків визначають: шкода внаслідок порушення збереження медичної інформації; рівень ймовірності настання такого порушення з урахуванням ідентифікованих загроз та вразливостей, а також здійснених заходів захисту; величину ризику. Оцінка можливої шкоди провадиться за трирівневою якісною шкалою: максимальна, середня та мінімальна величина. Повинні бути ідентифіковані рівні ризику, які є прийнятними та прийнятими, ризики, що не перевищують прийнятного рівня.

Пропонуємо в діяльності служби внутрішнього контролю за збереженням медичної інформації в Хмельницькому обласному бюро судово-медичної експертизи розробити та вести Реєстр інформаційних ризиків, що описує поточну ситуацію з інформаційними ризиками в організації. Приклад введення такого реєстра наведено у табл.3.4.

Після того як рішення щодо обробки ризиків були прийняті, мають бути визначені та сплановані дії щодо реалізації цих рішень. Кожен захід має бути чітко визначено та розбито на таку кількість дій, які необхідні для чіткого розподілу відповідальності між виконавцями, оцінки вимог до виділення ресурсів, встановлення віх та контрольних точок, визначення критеріїв досягнення цілей та моніторингу. Реєстр ризиків також визначає терміни реалізації, виділені ресурси та відповідальних виконавців.

Ризики є статичними. Загрози, вразливості, ймовірність чи наслідки можуть змінюватися несподівано, без будь-яких ознак змін. Тому необхідний безперервний моніторинг та переоцінка ризиків та їх факторів (тобто цінність активів, вплив, загрози, вразливості, ймовірність виникнення) з метою визначення будь-яких змін у контексті організації на ранній стадії, та має підтримуватися загальне уявлення про всю картину ризику. Дані, що отримані в наслідок здійснення внутрішнього контролю, підлягають подальшій систематизації, дослідженню, аналізу та оцінці. Ідентифікуються чинники, причини відхилень (шахрайство чи помилка) та винні особи, дії або бездіяльність яких стали причиною відхилень, розробляються відповідні рекомендації по усуненню та попередженню у майбутньому.

Завершальним етапом є оформлення та презентація результатів внутрішнього контролю за збереженням медичної інформації в закладі охорони здоров’я користувачам інформації та суб’єктам прийняття відповідних управлінських рішень з метою виправлення відхилень та контролю за виконанням розроблених рішень.

Таблиця 3.4 Фрагмент Реєстру інформаційних ризиків у контексті збереження медичної інформації Хмельницькому обласному бюро судово-медичної експертизи

Загроза	Вразливості	Інформаційні активи	Заходи зниження ризику	Механізми контролю	Відповідальні
Крадіжка комп'ютерного обладнання та носіїв інформації інсайдерами	Не проводиться реєстрація обладнання та інформаційних носіїв, винесених за межі території організації Відсутні регламенти роботи з інформаційними активами	Комп'ютерне обладнання та носії інформації	Розробити систему заходів, що обмежують неконтрольоване вико-ристання зовнішніх носіїв та мобільних пристроїв поза закладом. Розробити регламенти роботи з інформа-ційними активами	Офісне обладнання та документація знаходиться суворо у зонах безпеки. Дотримання політики безпеки щодо мобільних носіїв інформації та використання зовнішніх пристроїв	_____ *(Прізвище І., посада)*
Фізичний несанкціонований доступ в приміщення організації, кабінети та серверні кімнати до обладнання, паперовим документам, іншим носіям інформації тощо.		Комп'ютерне обладнання та носії інформації	Розробити систему заходів, що обмежують несанкціонований доступ, зокрема із використанням електронних пропусків (смарткартки). Визначення та ліквідація «сірих» зон для системи відеоспостереження тощо.	Доступ до приміщень здійснюється виключно по смарткарток. Аналіз даних відеоспостереження.	_____ *(Прізвище І., посада*
Виток інформації з обмеженим доступом, що озвучується	Не достатня шумоізоляція приміщення, для проведення нарад	Матеріальні носії інформації	Обладнати приміщення пристроями для захисту акустичної інформації	Озвучування інформації з обмеженим доступом у спеціальному приміщенні.	_____ *(Прізвище І., посада*
….					

Примітка. Запропоновано автором

Наступні етапи, пов'язані з вибором засобів захисту інформації, що відповідають переліку актуальних загроз ПД, а також їх використання не викликають особливих складнощів: на ринку представлено досить велику кількість рішень, і проектувальникам залишається підібрати найбільш підходяще за вимогами та умовами застосування. Таким чином, забезпечення захисту обробки медичних біометричних даних має проводитись відповідно до чинного законодавства.

Запропоновані процедури внутрішнього контролю забезпечать не лише підвищення інформаційної безпеки та захист медичної інформації, але слугують підготовкою для проведення Державної експертизи в сфері технічного захисту інформації [37], а також проходження GDPR сертифікації. Офіційним підтвердженням того, що система захисту персональних даних (у тому числі і медичної інформації) забезпечує захист інформації відповідно до вимог нормативних документів, є Атестат відповідності вимогам безпеки інформації. В свою чергу, GDPR - Загальний регламент про захист даних (General Data Protection Regulation, GDPR; Regulation (EU) 2016/679) — регламент в межах законодавства Європейського Союзу щодо захисту персональних даних усіх осіб у межах Європейського Союзу та Європейської економічної зони. GDPR сертифікація не є обов’язковою вимогою, однак вона надає ряд переваг закладу для попередження: випадків витоку персональних даних, порушення приписів GDPR та завдання шкоди інтересам клієнтів; для зменшення імовірності накладення штрафних санкцій через порушення GDPR [56].

Досвід фахівців показує, що найважливішими етапами є передпроектне обстеження, побудова моделі загроз та класифікація інформаційних активів, оскільки є відправними точками для подальшої роботи. Одним із найбільш трудомістких етапів є розробка необхідної документації та вимог щодо захисту медичної інформації (формування моделі загроз), яка займає від трьох до шести місяців.

Наступні етапи, пов'язані з вибором засобів захисту інформації, що відповідають переліку актуальних загроз, а також їх використання не викликають особливих складнощів: на ринку представлено досить велику кількість рішень, і закладу необхідно найбільш оптимальний за вимогами та умовами застосування.

3.2. Розробка рекомендацій щодо посилення захисту медичної інформації в закладі охорони здоров’я

Сформуємо комплекс заходів щодо посилення захисту медичної інформації в Хмельницькому обласному бюро судово-медичної експертизи, що дозволить створити чітку і злагоджену систему організації роботи КСЗІ, здатну захистити медичну інформацію закладу (табл.3.5).

Внутрішній контроль за збереженням 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; та інших організаційних і інженерно-технічних заходів, програмно – апаратних засобів, які забезпечують захист інформації [6, с.81].

Розглянемо окремі заходи більш детально.

1. Навчання керівного складу та працівників вимогам Загального регламенту про захист даних GDPR у контексті плану дій щодо комплексної модернізації системи внутрішнього контролю за збереженням інформації в закладі охорони здоров’я. GDPR – це проект бізнес-змін, одним з надзвичайно важливим аспектом якого є навчання персоналу. Працівники закладу охорони здоров’я повинні розуміти важливість захисту даних всередині закладу та пройти навчання з основних принципів GDPR і процедур, здійснених в закладі для дотримання вимог GDPR.

Таблиця 3.4 Рекомендації щодо удосконалення внутрішнього контролю за збереженням інформації в Хмельницькому обласному бюро судово-медичної експертизи

Захід	Необхідні процедури	Результат	Витрати
1	2	3	4
1. Поглиблення та систематизація знань персоналу щодо реалізації законодавства про захист персональних даних	- організація тренінгів; - складання планів навчання та графіків проходження працівниками; - пошук спеціалізованих курсів/організаторів та укладання відповідних угод; - підготовка навчально-методичного матеріалу,	Підвищення рівня професіоналізму при реалізації завдань у сфері захисту персональних даних	Оплата праці залучених працівників для проведення навчання. Друк матеріалів. Проходження безкоштовних он-лайн курсів – не потребує додаткових витрат
2. Впровадження системи корпоративних носіїв інформації (USB-накопичувачі)	- встановлення програмного забезпечення на усі комп'ютери, що блокує використання сторонньої флешки; - закупівля корпоративних носіїв інформації (як мінімум 1 флешка на комп'ютер; - проведення інструктажу персоналу щодо використання носіїв;	Неможливість використання такого USB-накопичувача на сторонніх комп'ютерах та використання «сторонніх» USB-накопичувач в середині закладу	Витрати на програмне забезпечення та USB-накопичувачі.
3. Облаштування кімнати для переговорів з метою озвучування інформаціїз обмеженим доступом або такої, що містить персональні дані	- виділення приміщення (частини приміщення) для переговорів (озвучення інформації з обмеженим доступом) - визначити перелік пристроїв, необхідних для захисту акустичної інформації	Неможливість випадкового або умисного витоку інформації з обмеженим доступом або такої, що містить персональні дані	Витрати на шумоізоляцію приміщення. Витрати на спеціальне обладнання для захисту акустичної інформації
4. Встановлення програмного забезпечення на службові комп'ютери для визначення місцезнаходження службових комп'ютерів	- придбання та встановлення необхідного програмне забезпечення; - інтеграція у загальну систему безпеки закладу (повідомлення про місцезнаходження)	Неможливість винесення за межі закладу службової комп'ютерної техніки	Витрати на програмне забезпечення

Примітка. Складено автором.

Грамотність у сфері роботи з даними, що передбачає в т. ч. грамотне управління обробкою даних та грамотний захист персональних даних, що повинно стати невід'ємною частиною професійних знань фахівців закладу здоров'я. Тому бажано, щоб тренінг пройшов увесь персонал закладу,

оскільки обізнаність всього персоналу в нових упроваджених процесах щодо захисту персональних даних допоможе швидше зреагувати, якщо відбудеться витік інформації чи на компанію буде здійснено кібератаку.

Безперервна освіта також надзвичайно важлива для того, щоб забезпечити компетентність спеціалістів закладу охорони здоров'я у сфері нових технологій, таких як хмарні обчислення або системи на основі блокчейну, що впроваджуються у секторі охорони здоров'я. Розширення прав та можливостей необхідне для правильного застосування принципів захисту даних у динамічному технологічному середовищі.

Слід зазначити, що на сьогоднішній день різні освітні платформи пропонують безкоштовні курси щодо захисту персональних даних, які можуть бути використані Хмельницьким обласним бюро судово-медичної експертизи для підвищення рівня професіоналізму при реалізації завдань у сфері захисту персональних даних. Наведемо приклади деяких таких курсів:

- Навчальний онлайн-курс "Захист персональних даних" створений Офісом Уповноваженого Верховної Ради України з прав людини та Офісом Ради Європи в Україні в межах Спільного проєкту "ЄС та Рада Європи працюють разом задля посилення операційної спроможності Омбудсмана у захисті прав людини" та у співпраці зі студією онлайн-освіти EdEra [34];

- Освітній серіал «Персональні дані», представлений освітньою платформою «Дія» [38];

- Онлайн-курс «Захист персональних даних» [13].

Вартість платних курсів становить:

- КУРС. GDPR В УКРАЇНІ: практика застосування – 3600 грн. [23];

- General Data Protection Regulation від компанії ITEA – 14400 грн. [58];

- онлайн-тренінг «Сертифікований фахівець із захисту персональних даних» від компанії Pecb Ukraine - вартість одного учасника складає 24 750, у вартість курсу входить оплата за Складання сертифікаційного іспиту.

Таким чином, Хмельницьке обласне бюро судово-медичної експертизи може визначити оптимальний варіант фінансування цього заходу. На нашу

думку, фахівця (контролер) із захисту персональних даних повинен пройти курс із можливістю отримання сертифікату GDPR, а в подальшому - проводити навчання персоналу організації, використання дистанційних безкоштовних курсів тощо.

Організація навчання персоналу з питань захисту персональних даних передбачатиме здійснення таких заходів:

- складання планів навчання та графіків проходження працівниками;
- проведення занять;
- перевірка знань.

Результатом запровадження такого захисту є формування моделі поведінки працівників у випадку настання реальної загрози; унеможливлення витоку медичної інформації, у тому числі персональних даних працівників та пацієнтів, зменшення кількості «успішних атак» на заклад; зменшення позовів та скарг з боку третіх осіб тощо.

2. Поява USB-накопичувачів інформації та їх широке використання, поруч зі зручністю та доступністю, стали додатковим шляхом розповсюдження шкідливого програмного забезпечення, «троянів» шпигунських агентів тощо. Наслідки такого зараження різні — починаючи від втрати інформації, її витоку і закінчуючи блокуванням роботи комп’ютера, інформаційної системи чи навіть втратою управління мережами спеціального зв’язку.Рівень інформаційної та фізичної безпеки персональних накопичувачів інформації працівників і пацієнтів закладу охорони здоров’я повинна забезпечувати належний захист. Тому до таких USB накопичувачів висуваються підвищені вимоги до реалізації систем захисту інформації. Загроза витоку інформації, що зберігається на цифрових накопичувачах, в результаті передачі накопичувача за межі організації, нині добре відома багатьом фахівцям [19]. Тому пропонуємо запровадити на підприємстві використання корпоративних USB-флеш накопичувачів, використання яких поза відповідної мережі неможлива.

Мінімальна вартість флеш накопичувачів приблизно складає 60 дол. США, з чого можна зробити висновок, що розробка таких виробів є складною технічною задачею, вироби потребують високоякісних мікросхем та проходять сертифікацію.Враховуючи, що у Хмельницькому обласному бюро судово-медичної експертизи та міжрайонних відділеннях кількість комп’ютеризованих робочих місць становить 23 од., орієнтовна вартість реалізації пропозиції при мінімальній вартості флешки 60$ та курсі НБУ 27 грн./ $ становить: 23*60*27=37260 грн.

3. Однією з загроз безпеки інформації на об'єктах інформаційної діяльності є несанкціоноване отримання конфіденційної акустичної інформації. Тому захист об’єктів інформаційної діяльності Хмельницькому обласному бюро судово-медичної експертизи від витоку інформації акустичним каналом є актуальною задачею. Інформація з обмеженим доступом (наприклад, інформація з судово-медичних експертиз) повинна озвучуватися у виділеному приміщенні, тобто спеціальному приміщені призначеному для проведення нарад. Основними заходами під час таких нарад є захист від витоків каналами через, які може бути витік інформації, що озвучується, а також захист від несанкціонованого доступу. Тому необхідним є облаштування кімнати для переговорів з метою озвучування інформації з обмеженим доступом або такої, що містить персональні дані.

Для захисту інформації з обмеженим доступом, що озвучується усі прилади повинні бути сертифікованими та мати відповідну ліцензію. У табл. 3.5 наведено короткий перелік сертифікованих приладів та від якого каналу витоку інформації вони захищають. Використання будь-яких приладів і систем не сертифікованих і без відповідних ліцензій вважається незаконним і карається як штрафами, так і кримінальною відповідальністю.

Запропоновані рекомендації дозволять забезпечити безпеку акустичної інформації у спеціально виділених для цього приміщеннях. Вважаємо, що озвучування інформації, що містить персональні дані (наприклад потерпілим, родичам потерпілого, іншим особам), також повинна здійснюватися у

такому приміщенні. Це унеможливість випадковий або умисний виток інформації, що містить персональні дані.

Таблиця 3.5 Перелік пристроїв призначених для захисту акустичної інформації

Канал витоку інформації	Пристрій призначений для захисту
Акустичний	Генератор шумових сигналів «МАРС-ТЗО-4-2»
Віброакустичний	Прилад віброакустичного захисту інформації«ОЦЗІ-ВА»
Лазерно-акустичній	Вібровипромінювач «ВИЗ»
Акустоелектричний	Колонка акустична захищена «МАРС-АКЗ»
Параметричний	Трансформатори розділові з екраною обмоткою «РІАС-4ТР/5»
Оптичний	Комплекс автоматизований радіомоніторингу і пошуку закладних пристроїв АКОР-3

Джерело: [36].

4. Встановлення програмного забезпечення на службові комп’ютери для визначення їх місцезнаходження, що унеможливіть винесення за межі закладу службової комп’ютерної техніки. Крім того, таке програмне забезпечення може здійснювати контроль за ефективністю проведення робочого часу і раціональністю використання обладнання працівниками підприємства, використання месенджерів та електронної пошти, обміну даними тощо.

Захист медичної інформації є важливим компонентом орієнтованого на дотримання інтересів людини підходу до технологій та орієнтиром для їх використання в умовах переходу на цифровий вектор. У системі охорони здоров'я описані вище заходи стають важливим інструментом, що дозволяє закладу більш ефективно здійснювати обробку персональних даних у законних цілях, правовим, справедливим та прозорим чином. Заходи захисту даних повинні бути інтегровані в розробку та здійснення програм розвитку закладу охорони здоров’я.

ВИСНОВКИ

У дослідженні вирішено наукове завдання щодо теоретичного обґрунтування та розробки практичних рекомендацій щодо організації внутрішнього контролю за збереженням медичної інформації в закладі охорони здоров’я. Результати проведеного дослідження свідчать про досягнення поставленої мети, виконання завдань і дають підстави зробити низку висновків:

1. Встановлено сутність та особливості медичної інформації, яка обумовлює необхідність встановлення особливого режиму її обробки та використання. Встановлено, що система захисту інформації - це сукупність органів та або виконавців, що використовують техніки захисту інформації, а також об'єктів захисту інформації, що організована та функціонує за правилами і нормами, встановленими відповідними документами в галузі захисту інформації. При цьому захист даних є не одиничний захід, а безперевна діяльність, яка визначається організаційною стратегією, концепцією управління та готовністю нести відповідальність; ця відповідальність, заснована на ретельній оцінки ризиків, спирається на документування всіх дій у галузі захисту даних, а також постійний внутрішній контроль за збереженням медичної інформації.

2. Опрацьовано теоретичні основи організації внутрішнього контролю за збереженням медичної інформації в закладі охорони здоров’я. Встановлено, що внутрішній контроль за збереженням медичної інформації – це процес отримання об'єктивних якісних та кількісних оцінок про поточний стан захисту медичної інформації організації у відповідності до певних критеріїв та вимог законодавства. Виділено види контролювання, що рекомендовані для застосування у системі внутрішнього контролю за збереженням медичної інформації в закладі охорони здоров’я: попередній, поточний, самоконтроль, проміжний, завершальний. Охарактеризовано

методики внутрішнього контролю за збереженням медичної інформації, засновані на побудові моделі загроз та вразливостей.

3. Враховуючи, що основною діяльністю Хмельницького обласного бюро судово-медичної експертизи є проведення судово-медичної експертизи, що передбачає активне використання персональних даних про особу, дотримання вимог щодо захисту медичної інформації є важливим аспектом, що формує репутацію та професіоналізм закладу. Охарактеризовано основні показники діяльності Хмельницького обласного бюро судово-медичної експертизи, що демонструють напрями формування персональних даних за збереженням інформації: організаційну структуру, чисельність та структуру персоналу, динаміка експертиз відповідно по відділах та відділеннях, в яких міститься медична інформація.

4. Розглянуто правові аспекти регулювання роботи із персональними даними у сфері медичної діяльності. Визначено, що комплексна система внутрішнього контролю за збереженням інформації в Хмельницькому обласному бюро судово-медичної експертизи відсутня, однак виконуються окремі функції у цій сфері: обмеження і контроль доступу до інформації, з якою працюють співробітники, зокрема забезпечення збереження персональних даних пацієнтів; створення правил безпечної роботи з інформацією; проведення заходів щодо резервування інформації тощо. Запропонована методика оцінювання захищеності інформації в закладі охорони здоров’я в рамках двох складових: оцінка організаційно-методичного та технічного забезпечення внутрішнього контролю (наявність відповідних процедур, регламентів, технічних засобів тощо) та оцінка дієвості внутрішнього контролю за збереженням медичної інформації.

5. Процес упровадження внутрішнього контролю в систему управління Хмельницького обласного бюро судово-медичної експертизи систематизовано у відповідній організаційної моделі: представлено інформаційно-аналітичне забезпечення внутрішнього контролю (запропоновано структуру реєстру інформаційних активів, структуру реєстру

інформаційних ризиків у контексті збереження медичної інформації), обґрунтовано доцільність створення посади фахівця (контролера) із захисту персональних даних, підпорядкування та основні завдання. Так, в організації він виконує роль незалежної сторони, яка консультує заклад, веде облік операцій з обробки даних та служить контактною особою для суб'єктів даних та органів влади. Крім того, фахівець із захисту персональних даних керує аудиторською діяльністю як всередині компанії, так і щодо третіх сторін, які обробляють дані по дорученню контролера даних.

6. Сформовано комплекс заходів із забезпечення внутрішнього контролю за збереженням 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 щодо реалізації законодавства про захист персональних даних; впровадження системи корпоративних носіїв інформації; облаштування кімнати для переговорів з метою озвучування інформації з обмеженим доступом або такої, що містить персональні дані. Для кожного заходу визначено необхідні процедури для реалізації, очікуваний результат, напрями витрати на їх впровадження.

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. Бем М. В., Городиський І. М., Саттон Г., Родіоненко О. М. Захист персональних даних: Правове регулювання та практичні аспекти: науково-практичний посібник. К.: К.І.С., 2015. 220 с

3. Булеца С. Б. Персональні дані пацієнта. *Науковий вісник Ужгородського національного університету*: Серія ПРАВО. Випуск 22. Частина 2. Том 1, 2014. С. 186-191.

4. Вразливості корпоративних інформаційних систем, 2019. URL: World Wide Web – URL: https://www.ptsecurity.com/ru-ru/research/analytics/corporate-vulnerabilities-2019

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. Дегтярьова Л.М. Аналіз структури системи захисту інформації. Системи управління, навігації та зв’язку. *Збірник наукових праць*. Полтава: ПНТУ, 2019. Т. 2 (54). С. 78-82.

8. Делембовський М., Шабала Є., Терентьєв О. Аналіз методів та шляхів вирішення захисту інформації в інформаційно-телекомунікаційних системах. *Грааль науки*. №1. С.249-254.

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. Довгань О.Д. Інформаційна безпека: стан, проблеми, тенденції. Інформаційні ресурси, інтелектуальна власність, комунікації в освітньо-науковій та інноваційній сферах: матеріали круглого столу Філософсько-правові та прикладні аспекти, м. Вінниця 12 травня 2017 р., Вінницький державний педагогічний університет ім. М. Коцюбинського / упоряд.: О.Д. Довгань, М.В. Беланюк, С.А. Лапшин, О.Г. Радзієвська, О.І. Яременко [та ін.]. Київ: Видавничий дім "АртЕк", 2017. С. 31-39.

11. Дудатьєв А. В. Комплексна інформаційна безпека соціотехнічних систем: моделі впливу та захисту : монографія. Вінниця : ВНТУ, 2017. 128 с.

12. Захаренко К. Основні суб'єкти та інститути інформаційної безпеки. *Науковий вісник. Серія «Філософія»*. Харків: ХНПУ. 2017. Вип.48 (частина І). С. 212–219.

13. Захист персональних даних /*Національне агентство України з питань державної служби.* URL: https://pdp.nacs.gov.ua/courses/zakhyst-personalnykh-danykh

14. Захист персональних даних : Закон України від 1 червня 2010 року № 2297-VI. URL: http://zpd.gov.ua/dszpd/uk/publish/article/49788;jsessionid=22FD426E29AFF7519E261246F1D0C1D6.

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. 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, 200.332. 95 с.

18. Коваленко С. В.Технологія аудиту кібербезпеки корпоративної інформаційної системи за методикою ISO/IES: 27001. *Сучасний захист інформації*. 2021. №3. DOI: 10.31673/2409-7292.2021.032935

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

20. 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.

21. Кукшин Д. В. Методи оцінювання стану захищеності підприємств від загроз кібербезпеці. *Сучасний захист інформації*. 2021. № 3 DOI: 10.31673/2409-7292.2021.035565

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

23. КУРС. GDPR В УКРАЇНІ: практика застосування. URL: https://academy.ligazakon.net/event/293

24. Лапінська Є. І. Зарубіжний досвід захисту інформації у сфері підприємництва та його використання в Україні. *Держава та регіони*. 2019 р. № 3 (65). URL: http://www.law.stateandregions.zp.ua/archive/3_2019/30.pdf

25. Легка О. В. Актуальні питання захисту персональних даних: вітчизняний та міжнародний досвід. URL: http://legalposition.umsf.in.ua/archive/2021/2/15.pdf

26. 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.

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

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

29. Мельник С.І. Інформаційна безпека як складова економічної безпеки підприємства. URL: http://www.rusnauka.com/6JPNIJ2013/Economics/9J130048.doc.htm

30. Нашинець-Наумова А.Ю. Інформаційна безпека: питання правового регулювання : монографія. Київ : Гельветика, 2017. 168 с.

31. НД ТЗІ 1.1-005-07 «Захист інформації на об'єктах інформаційної діяльності. Створення комплексу технічного захисту інформації. Основні положення». URL: https://tzi.com.ua/nd-tz-1.1-005-07.html

32. Новый экономический словарь / [А.Н. Азрилиян]. М. : Институт новой экономики, 2006. 1088 с.

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

34. Онлайн-курс «Захист персональних даних». URL: https://euprostir.org.ua/resources/159421

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

36. 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

37. Перелік засобів технічного захисту інформації', дозволених для забезпечення технічного захисту державних інформаційних рисунків та інформанії, вимога щодо захисту якої встановлена законом. URL: http//www.dstszi.gov.ua/dstszi/control/uk/publish/artide?ar1_id=234237&cat_id=39Ш

38. Персональні дані. URL: https://osvita.diia.gov.ua/courses/personaldata

39. Посібник з європейського права у сфері захисту персональних даних. К.: К.І.С., 2015. 216 с.

40. Про державні фінансові гарантії медичного обслуговування населення: Закон України від 19 жовтня 2017 року № 2168-VIII. *Офіційний вісник України.* 2018. № 4

41. Про затвердження Положення про електронний реєстр пацієнтів постанова Кабінету Міністрів України від 06.06.2012 № 546 // Офіційний вісник України від 27.06.2012 р. – № 47. – стор. 23, стаття 1832, код акту 62180/2012

42. Про затвердження Порядку ведення електронного реєстру пацієнтів Вінницької, Дніпропетровської, Донецької областей та м. Києва МОЗ України; Наказ, Порядок від 30.08.2012 № 666 // Офіційний вісник України : офіційне видання від 01.10.2012 2012 р., № 72, стор. 310, стаття 2923, код акту 63451/2012

43. Про інформацію : Закон України від 2 жовтня 1992 року № 2657-XII. URL: http://zakon5.rada.gov.ua/laws/show.

44. Програма економічних реформ на 2012-2014 роки «Заможне суспільство, конкурентоспроможна економіка, ефективна держава» : затверджена Указом Президента України від 12.03.2012 № 187 [Електронний ресурс]. – Режим доступу : http://zakon1.rada.gov.ua/laws/show/n0004100-10

45. Северина С. В. Інформаційна безпека та методи захисту інформації. Вісник Запорізького національного університету. *Економічні науки.* 2016. №1. С.155-161.

46. Сенюта І. Я. Захист персональних даних у сфері охорони здоров'я: алгоритм змін. *Науковий вісник Херсонського державного університету. Серія «Юридичні науки»*. Випуск 6-1/2014. 2014. С. 216–221.

47. Статут КП «Хмельницьке обласне бюро судово-медичної експертизи»: затверджений рішенням Хмельницької обласної ради від 11.12.2019 р. №37. Хмельницький, 2019, 13 с.

48. Степанова О.М. Інформаційна безпека в умовах розвитку інформаційної системи / О.М. Степанова, Л.М. Дегтярьова URL: http://dspace.snu.edu.ua:8080/jковськаspui/bitstream/123456789/685/1/11.pdf.

49. Терешко Х.Я. Види інформації як об'єкта цивільних правовідносин у сфері медичного обслуговування. *Медичне право*. 2019. № 1 (23). С. 65–73.

50. Фінансовий план підприємництва на 2019 р. КП «Хмельницьке обласне бюро судово-медичної експертизи». Хмельницький, 2019, 2 с.

51. Фінансовий план підприємництва на 2020 р. КП «Хмельницьке обласне бюро судово-медичної експертизи». Хмельницький, 2020, 2 с.

52. Хто і як контролює сферу захисту персональних даних. Юридична газета. URL: https://yur-gazeta.com/publications/practice/informaciyne-pravo-telekomunikaciyi/skandal-cifra-diya.html

53. Шандига-Глушко О.І., Арзянцева Д.А. Напрями підвищення ефективності управління інформаційною безпекою закладу охорони здоров'я. *Збірник матеріалів Всеукраїнської науково-практичної Інтернет-конференції молодих учених та студентів «Міждисциплінарні дослідження науки XXI століття»* (1 грудня, 2021 р., м.Київ). URL: https://conf.krok.edu.ua/ISR/ISR-2021/paper/view/933

54. Шепета О. В. Основні вимоги до створення служби захисту інформації на підприємстві. *Прикарпатський юридичний вісник*. 2020. № 3(32). URL: http://pyuv.onua.edu.ua/index.php/pyuv/article/view/607

55. Юніна М.П. Деякі питання захисту персональних даних у сфері охорони здоров'я під час пандемії covid-19. URL: http://www.lsej.org.ua/2_2021/27.pdf

56. Юридична GDPR Сертифікація. URL: https://legal-support.top/gdpr-certification/

57. Як медикам працювати з персональними даними пацієнтів. Міністерство охорони здоров'я України: веб-сайт. URL: https://moz.gov.ua/article/for-medical-staff/jak-medikam-pracjuvati-z-personalnimi-danimi-pacientiv

58. General Data Protection Regulation від компанії ITEA – 14400 грн. URL: https://itea.ua/corporate-education/methodology/itil-2011/general-data-protection-regulation/

59. ISO/IEC 27005:200.335. Інформаційні технології. Методи захисту. Управління ризиками інформаційної безпеки [Текст]. Київ: ДП "УкрНДНЦ", 200.335. 60 с.

Виконала: студентка
2 курсу магістратури
спеціальності
073 Менеджмент
заочної форми навчання
«____» грудня 2021 р.

_____ Підпис

О.І. Шандига-Глушко
Ініціали, прізвище

Науковий керівник
к.е.н., доцентка,
доцентка кафедри

_____ Підпис

Д.А. Арзянцева
Ініціали, прізвище

Робота допущена до захисту:
завідувачка кафедри
к.е.н., доцентка
«____» грудня 2021 р.

_____ Підпис

Н.П. Захаркевич
Ініціали, прізвище

ДОДАТКИ

Додаток А

Критерії оцінювання рівня захищеності інформації в закладі охорони здоров’я

Параметр	Показники параметру	Значення показника параметра
Оцінка організаційно-методичного та технічного забезпечення внутрішнього контролю		
Вид носія інформації (Документації).	Документи відсутні в будь-якому вигляді.	0
	Використовується тільки електронний формат.Централізований електронний архів документів відсутній.	3
	Використовується тільки паперовий формат документів	3
	Використовуються паперові та електронні версіїдокументів.Централізований архів документів відсутній.	4
	Використовуються паперові та електронні версії документів з використанням централізованого архіву документів.	5
Ступінь безпеки (захищеності) інформаційного потоку	Конфіденційна інформація зберігається безбудь-якого захисту. Регламент доступу не розроблено. Відсутні засоби захисту конфіденційної інформації, що озвучується	0
	Конфіденційна інформація зберігається без будь-якого захисту. Регламент доступу розроблено. Наявні засоби захисту інформації з обмеженим доступом, що озвучується, однак ступінь захисту не достатній. Відсутній регламент використання	1
	Конфіденційна інформація зберігається без використання спеціалізованого ПЗ. Регламент доступу розроблено. Використовуються засоби захисту конфіденційної інформації, що озвучується. Ступінь захисту не достатній. Регламент наявний	2
	Конфіденційна інформація зберігається без використання спеціалізованого ПЗ. Регламент доступу розроблено. Використовуються засоби захисту конфіденційної інформації, що озвучується, однак ступінь захисту не достатній	3
	Конфіденційна інформація зберігається без використання спеціалізованого ПЗ. Регламент доступу не розроблено. Наявні засоби захисту конфіденційної інформації, що озвучується, однак використовуються не в усіх випадках, передбачених регламентом	4
	Конфіденційна інформація зберігається з використанням спеціалізованого ПЗ. Регламент доступу не розроблено.Використовуються засоби захисту конфіденційної інформації, що озвучується	5
Ступінь відповідності комплексної системи захисту інформаційної системи (КСЗІ)	наявні комп’ютерні програми (їх оновлення), в яких є недокументовані функції	0
	використовуються хоча б 1 комп’ютерна програма (їх оновлення), в якій є недокументовані функції	2
	використовуються комп’ютерні програми (їх оновлення), в яких немає недокументованих функцій, однак це не	3

вимогам нормативних документів системи технічного захисту інформації	підтверджено результатами державної експертизи у сфері захисту інформації. Наявні випадки циркуляції інформаційні потоки з обмеженим доступом циркулюють із використанням неслужбових ПО	
	використовуються комп'ютерні програми (їх оновлення), в яких немає недокументованих функцій, однак це не підтверджено результатами державної експертизи у сфері захисту інформації	4
	використовуються комп'ютерні програми (їх оновлення), в яких немає недокументованих функцій, що підтверджується результатами державної експертизи у сфері захисту інформації (наявний Атестат відповідності)	5
Ступінь розвитку організаційного забезпечення	Контроль за збереженням медичної інформації не здійснюється	0
	Контроль за збереженням медичної інформації здійснюється тими самими суб'єктами, що відповідальні за інформаційну безпеку	1
	Рішення про організацію внутрішнього контролю за збереженням медичної інформації відсутнє. Здійснюється окремі процедури у сфері контролю за збереженням медичної інформації, однак відповідні регламенти відсутні.	2
	Прийнято рішення про організацію внутрішнього контролю за збереженням медичної інформації. Регламент внутрішнього контролю та інші документи розроблено, але не введено в дію.	3
	Впроваджена система внутрішнього контролю за збереженням медичної інформації. Регламент внутрішнього контролю та інші документи розроблено введено в дію. Однак контроль здійснюється тими самими суб'єктами, що відповідальні за інформаційну безпеку	4
	Впроваджена незалежна система внутрішнього контролю за збереженням медичної інформації	5
Оцінка дієвості внутрішнього контролю за збереженням медичної інформації		
Наявність скарг, пов'язаних з недотриманням вимог захисту персональних даних	Наявні протягом звітного періоду та знайшли своє підтвердження	0
	Відсутні протягом звітного періоду або не знайшли своє підтвердження	5
Наявність звернень до Уповноваженого ВРУ з прав людини щодо випадків недотримання вимог захисту персональних даних	Наявні протягом звітного періоду та знайшли своє підтвердження	0
Юрисдикційні звернення (позови до судів) щодо випадків недотримання вимог захисту персональних даних	Наявні протягом звітного періоду та знайшли своє підтвердження	0
	Відсутні протягом звітного періоду або не знайшли своє підтвердження	5

Притягнення до відповідальності працівників	Наявні протягом звітного періоду та підтверджені відповідними матеріалами	0
	Відсутні через відсутність складу правопорушення або обставин, що виключають відповідальність або змінено (скасовано) за рішенням суду	5

Примітка. Запропоновано автором.