МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
Західноукраїнський національний університет

ЛИПА Тетяна Петрівна

Організація захисту персональних даних пацієнта в закладі охорони здоровя

Спеціальність – 073 Менеджмент
Освітньо-професійна програма – Менеджмент закладів охорони здоров'я

ВСТУП

ВСТУП

Актуальність проблеми. Персональні дані пацієнта, і передусім інформація про стан його здоров'я належить до так званої «чутливої» інформації. Тому питання забезпечення їх конфіденційності і нерозголошення у закладі охорони здоров'я вимагають вироблення чіткого механізму їх захисту, формування баз даних та порядку організації належного їх збереження.

Цей процес передбачає дотримання законодавчих норм і впровадження технічних, організаційних та адміністративних заходів для запобігання порушенням.

Мета дослідження - узагальнити діючу практику та виробити практичні рекомендації щодо упровадження інноваційних технологій захисту персональних даних пацієнта та забезпечення конфіденційності медичної інформації.

Для досягнення мети дослідження розв'язувалися такі завдання:

- Дослідити поняття персональних даних пацієнтів в закладі охорони здоров'я та об'єктивна необхідність їхнього захисту
- узагальнити нормативно-правову базу організації захисту персональних даних пацієнтів в закладі охорони здоров'я;
- охарактеризувати механізми організаційно-функціонального забезпечення системи захисту персональних даних пацієнтів лікарні
- провести оцінку діючих процедур захисту персональних даних пацієнтів в досліджуваному КНП
- надати рекомендації щодо впровадження інноваційних технологій захисту персональних даних пацієнтів

Об'єкт дослідження - система захисту персональних даних пацієнтів в закладі охорони здоров'я.

Предмет дослідження – процес та процедури організації захисту персональних даних пацієнтів в закладі охорони здоров'я.

Методи дослідження. Для розв’язання поставлених завдань використовувалися загальнонаукові та спеціальні прийоми наукових досліджень, зокрема, методи системного, факторного, порівняльного та компаративного аналізу; методи узагальнення,графічні методи

Практична значущість результатів дослідження полягає в розроблені практичних рекомендацій щодо удосконалення процедур персоніфікованого доступу та обробки персональних даних пацієнтів та впровадження сучасних інформаційних систем для їхнього захисту.

РОЗДІЛ 1
ТЕОРЕТИКО-ПРАВОВІ ЗАСАДИ ОРГАНІЗАЦІЇ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ ПАЦІЄНТІВ В ЗАКЛАДІ ОХОРОНИ ЗДОРОВ'Я

1.1. Поняття персональних даних пацієнтів в закладі охорони здоров'я та об'єктивна необхідність їхнього захисту

Цифровізація та діджиталізація в сфері охорони здоров'я формують нові перспективи та виклики перед закладами охорони здоров'я. На сьогодні наявні значні можливості для підвищення якості медичних послуг за рахунок покращення доступу до них, ефективності обробки даних, автоматизації процесів, зниження витрат, можливості використання телемедицини. За цих умов ключовим чинником забезпечення якісного надання медичних послуг є інформація, яка охоплює сукупність даних щодо стану здоров'я пацієнтів, адміністративних процесів, медичних послуг, персоналу та ресурсного потенціалу закладу. Водночас, сьогодні, медичні заклади можуть бути об'єктами кібератак, що загрожує витоком інформації, в тому числі і розкриттям персональних даних пацієнтів. Зазначене актуалізує проблематику організації захисту персональних даних пацієнтів в закладі охорони здоров'я.

Інформація в закладі охорони здоров'я відіграє ключову роль у забезпеченні надання якісних послуг, ефективному управлінні та захисті прав пацієнтів.

Дослідження проблематики організації захисту персональних даних пацієнтів в медичному закладі потребує розуміння базових понять, які розкривають її зміст, а саме: «ініформація», «інформаційні ресурси», «персональні дані», «захист персональних даних».

Так, зазначимо, що термін «інформація» у Законі України «Про інформацію» розглядається як «будь-які відомості та/або дані, які можуть бути збережені на матеріальних носіях або відображені в електронному вигляді» [40].

На сьогодні інформація є одним із ключових ресурсів для управління організацією медичного профілю, а її обсяги та якість слугують аналітичною основою для обґрунтування управлінських рішень. У сфері охорони здоров'я інформація охоплює різноманітні потоки, зокрема медичні дані: результати оглядів лікарів, лабораторні аналізи, інформацію з експертних систем, особисті дані пацієнтів, статистику діяльності закладу та результати наукових досліджень. Фнша складова інформаційних потоків - немедична інформація, яка пов'язана з управлінням установою та виконанням її функціональних завдань (рис.1.1).

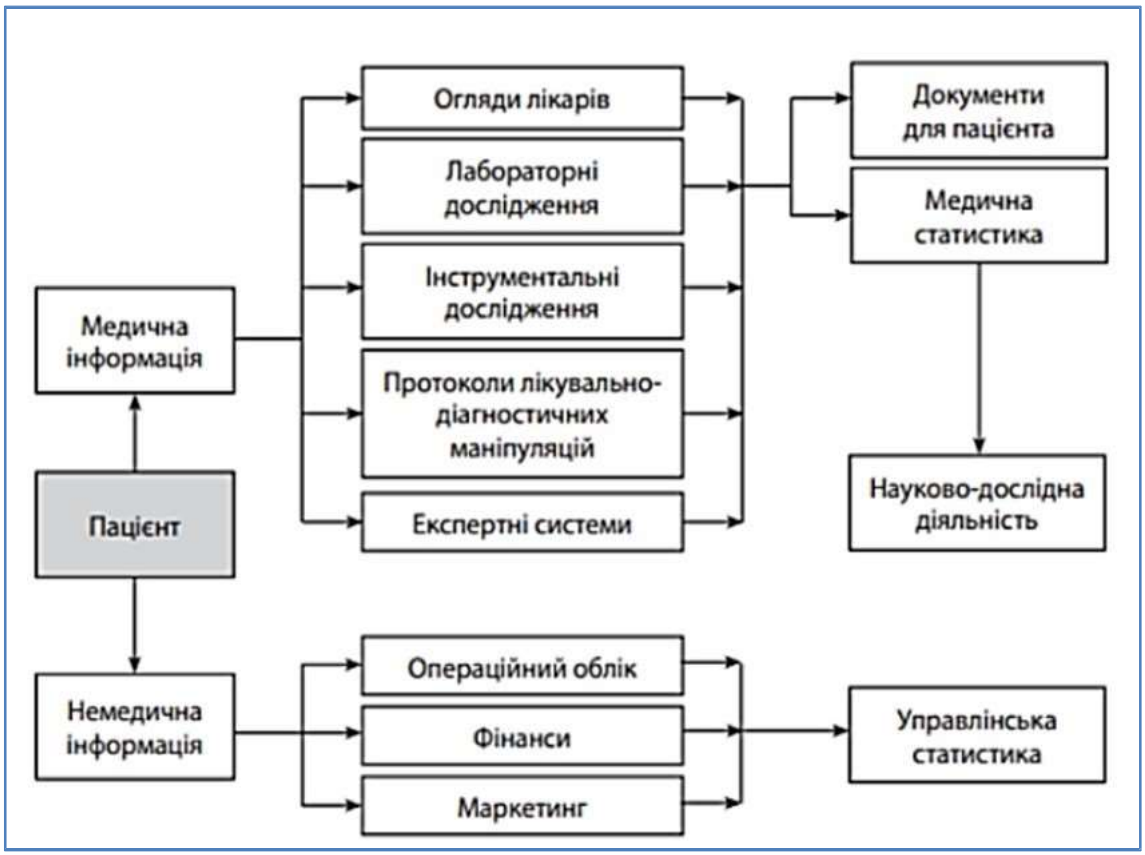

Рис. 1.1. Інформаційні потоки закладу охорони здоров'я

Примітка. Побудовано на основі [23;24].

Водночас, вказані інформаційні потоки (див.рис.1.1) можна деталізувати окремими видами інформації, які їх формують. Так, можна виокремити такі види інформації, що використовується ЗОЗ, як: медична інформація про пацієнтів, адміністративна інформація, фінансова інформація, інформація про медичний персонал, інформація про ресурсний потенціал закладу. Характерні особливості різних видів інформації наведено в табл.1.1.

Таблиця 1.1

Основні види інформації закладу охорони здоров'я

№ з/п	Вид інформації	Змістовна характеристика
1	Медична інформація про пацієнтів	дані про стан здоров'я, діагнози, результати аналізів, призначення лікарів, історії хвороб, алергії, проведені процедури та хірургічні втручання. Вона допомагає лікарям приймати обґрунтовані рішення та відслідковувати динаміку лікування
2	Адміністративна інформація	дані про запис пацієнтів на прийом, розклад роботи лікарів, наявність місць у стаціонарі та інша організаційна інформація, яка забезпечує злагоджену роботу закладу
3	Фінансова інформація	дані про оплату медичних послуг, страхові виплати, кошториси витрат та бюджет медичного закладу
4	Інформація про медичний персонал	дані про кваліфікацію, спеціалізацію, сертифікацію, графік роботи лікарів та іншого персоналу
5	Інформація про ресурси закладу	дані про медичне обладнання, наявність ліків, матеріалів і приміщень, що забезпечують ефективну роботу медичного закладу

Відповідно до норм чинного законодавства інформація залежно від доступності поділяється на загальнодоступну та інформацію з обмеженим доступом. Законом України «Про захист персональних даних» вводиться в обіг термін «персональні дані», зміст якого трактується як «відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована» [зу]. Всі питання, які пов'язані із персональними даними, їхньою обробкою та зберіганням регламентуються нормами вказаного законодавчого акту, який «регулює відносини, пов'язані з обробкою персональних даних, що здійснюється органами державної влади, органами місцевого самоврядування, іншими муніципальними органами, юридичними особами та фізичними особами з використанням автоматизованих засобів обробки, включаючи інформаційні та телекомунікаційні мережі, або не збираючи дані з цих засобів». [4]

Зміст проблематики захисту персональних даних розкривається крізь призму основних категорій, представлених в табл.1.2.

Так, вивчаюси тання захисту персональних даних важливо акцентувати увагу на тому, що фізична особа, персональні дані якої підлягають обробці є

суб’єктом персональних даних. А заклад охорони здоров’я виступатиме у ролі розпорядника чи одержувача цих даних, що несе відповідальність за їхнє зберігання.

Таблиця 1.2

Основні дефініції, що розкривають зміст «персональних даних»

Основні дефініції, що розкривають зміст «персональних даних»

№ з/п	Дефініція	Зміст дефініції
1	**Суб'єкт персональних даних**	фізична особа, персональні дані якої обробляються.
2	**Володілець персональних даних**	фізична або юридична особа, яка визначає мету обробки персональних даних, встановлює склад цих даних та процедури їх обробки, якщо інше не визначено законом.
3	**Розпорядник персональних даних**	фізична чи юридична особа, якій володільцем персональних даних або законом надано право обробляти ці дані від імені володільця.
4	**Третя особа**	будь-яка особа, за винятком суб'єкта персональних даних, володільця чи розпорядника персональних даних та Уповноваженого Верховної Ради України з прав людини, якій володільцем чи розпорядником персональних даних здійснюється передача персональних даних.
5	**Одержувач**	фізична чи юридична особа, якій надаються персональні дані, у тому числі третя особа.
6	**Електронна система охорони здоров'я (ЕСОЗ)**	інформаційно-телекомунікаційна система, 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.
7	**Відповідальність**	передбачені законами негативні наслідки особистого, майнового чи організаційного характеру, яких зазнає особа за вчинення певного порушення.

Захист персональних даних пацієнтів у закладі охорони здоров'я є важливим аспектом забезпечення приватності та довіри пацієнтів.

Зазначимо, що персональні дані пацієнтів можна класифікувати за різними ознаками. Так, наприклад, персональні дані залежно від виду поділяють на:

- «загальні персональні дані (до них відносяться прізвища, ім’я та по батькові особи, місце прописки чи проживання, наявність ай-пі адреси,

реєстраційного номеру облікової картки платників податків, фотознімку, електронного цифрового підпису, відкритого рахунку та інші дані, що ідентифікують особу» [12].

- «вразливі персональні дані (до них відносяться стан здоров'я особи, наявність хвороби, притягнення особи до адміністративної чи кримінальної відповідальності, наявність расового, етнічного та національного походження, біологічні та біометричні дані особи)» [14].

У ході класифікації персональних даних «слід приділити особливу увагу також біометричним (антропометричним) даним, даним про фізіологічні особливості людини, на основі яких можна його ідентифікувати (зріст, вага, колір волосся, група крові, голос, почерк, відбитки пальців, результати аналізу ДНК, цифровий образ особи, сітківка ока тощо). Саме біометрична ідентифікація може дати абсолютно точну картину ідентифікації громадянина за допомогою унікальних біологічних параметрів» [15].

Залежно від наявності біологічних ознак суб'єкта персональних даних, останні поділяють на:

- ідентифікуючі персональні дані, що містять генетичну інформацію (вроджені персональні дані і набуті);
- ідентифікуючі персональні дані котрі містять біометричну інформацію;
- ідентифікуючі персональні дані, що місять антропологічну інформацію.

Всю інформацію, яка міститьперсональні дані можна згрупувати на:

- по-перше, персональні дані, що місять конфіденційну інформацію;
- по-друге, персональні дані, що місять таємну інформацію;
- по-третє, персональні дані, що містять службову інформацію.

Персональні дані, які включають конфіденційну, таємну та службову інформацію, є свідченням їхньої багатоаспектності та можливості використання як в медичній, так і в інших сферах, де використовується інформація з обмеженим доступом.

У медицині до персональних даних працієнта відносять «будь-які відомості чи сукупність відомостей про пацієнта, за якими він

ідентифікується чи може бути конкретно ідентифікованим» [18]. З огляду на вказане такі дані належать до інформації з обмеженим доступом.

Організація захисту персональних даних пацієнтів у закладі охорони здоров’я, в першу чергу, базується на загальних принципах охорони здоров’я (рис.1.2), в основі яких лежить принцип дотримання лікарської таємниці.

Рис.1.2. Принципи охорони здоров’я

Водночас, можна виокремити і специфічні принципи організації захисту персональних даних пацієнтів, а саме:

- по-перше, розробка політик і процедур захисту даних, тобто закладу охорони здоров’я доцільно розробити власну політику захисту конфіденційної інформації пацієнтів із чітким визначенням типів інформації, що підлягає захисту (ім’я, діагноз, історія лікування тощо) та чіткою регламентацією процесів збирання, зберігання, передачі та знищення даних;

- по-друге, використання технологій для захисту інформації, зокрема шифрування даних для забезпечення їхньої безпеки під час передачі або зберігання. В рамках цього важливим є впровадження систем обмеженого доступу до даних, таких як паролі чи біометричний контроль, а також регулярні оновлення програмного забезпечення, щоб уникнути кіберзагроз;
- по-третє, обмеження доступу до даних, оскільки дані пацієнтів мають бути доступними лише тим співробітникам, які потребують їх для виконання професійних обов’язків, а також дотримання принципу "мінімально необхідної інформації", коли працівники медзакладу отримують доступ лише до тих даних, які необхідні для їхньої роботи;
- по-четверте, постійне навчання співробітників щодо протоколів повідомлення про можливі витоки даних та методів боротьби з кіберзагрозами;
- по-п’яте,інформування пацієнтівпро їхні права, в першу чергу на доступ до своїх медичних записів, право вимагати виправлення помилок у документації та право знати, як і кому передаються їхні дані.

З метою захисту персональних даних закладу охорони здоров’я важливо розробити процедури реагування на витоки даних, мати чіткий план дій у випадку витоку конфіденційної інформації, кіберзлому або іншого інциденту у сфері інформаційної безпеки.

Захист персональних даних у сфері охорони здоров’я сприяє побудові довіри між пацієнтами та медичними закладами. Обробка персональних даних відбувається на основі використання сучасних інформаційних технологій, за допомогою яких інформація перетворюється на один із домінуючих детермінант розвитку організації. Відповідно формується інформаційний простір та інформаційне середовище медзакладу.

1.2. Нормативно-правові засади організації захисту персональних даних пацієнтів в закладі охорони здоров'я

Організація захисту персональних даних пацієнтів в закладі охорони здоров'я потребує належного законодавчого забезпечення.

Законодавство з питань захисту персональних даних включає Конституцію України, Закон України «Про захист персональних даних», інші закони та підзаконні нормативно-правові акти та міжнародні договори України, ратифіковані Україною.

Основним нормативно-правовим актим щодо цих питань є Закон України «Про захист персональних даних». Цей закон покликаний «гаратуванти захист прав і свобод людини і громадянина під час обробки його особистих даних, включаючи захист прав на недоторканність приватного життя, особистих інтересів та сімейної таємниці» [16].

Так, статтею вище вказаного закону визначено правила «обробки персональних даних у загальнодоступних джерелах персональних даних, а саме: 1. Джерела зі зберігання персональних даних можуть бути загальнодоступними. В такі примірники додають ПІБ рік, місто місця народження, домашню адресу, абонентський номер, професійні відомості та інше2. На вимогу суб'єкта або за рішенням суду персональні дані повинні негайно видалятися. Закон «Про захист персональних даних» обумовлює його використання в різних сферах суспільного життя» [15].

Водночас, у чинному законі прописано наступний алгоритм щодо захисту персональних даниих:

«1. Володільці, розпорядники персональних даних та треті особи зобов'язані забезпечити захист цих даних від випадкових втрати або знищення, від незаконної обробки, утому числі незаконного знищення чи доступу до персональних даних.

2. В органах державної влади, органах місцевого самоврядування, а також у володільцях чи розпорядниках персональних даних, що здійснюють обробку персональних даних, яка підлягає повідомленню відповідно до цього

Закону, створюється (визначається) структурний підрозділ або відповідальна особа, що організовує роботу, пов’язану із захистом персональних даних при їх обробці.

Інформація про зазначений структурний підрозділ або відповідальну особу повідомляється Уповноваженому Верховної Ради України з прав людини, який забезпечує її оприлюднення.

3. Структурний підрозділ або відповідальна особа, що організовує роботу, пов’язану із захистом персональних даних при їх обробці:

1) інформує та консультує володільця або розпорядника персональних даних з питань додержання законодавства про захист персональних даних;

2) взаємодіє з Уповноваженим Верховної Ради України з прав людини та визначеними ним посадовими особами його секретаріату з питань запобігання та усунення порушень законодавства про захист персональних даних.

4. Фізичні особи - підприємці, у тому числі лікарі, які мають відповідну ліцензію, адвокати, нотаріуси особисто забезпечують захист персональних даних, якими вони володіють, згідно з вимогами закону» [15].

Порядок визначення «механізмів обробки персональних даних та комплекс заходів щодо їх захисту від випадкових втрати або знищення, від незаконної обробки, у тому числі незаконного знищення чи доступу до персональних даних, під час здійснення Мінфіном перевірки достовірності інформації та документів, що внесені до електронної системи охорони здоров’я (крім інформації про стан здоров’я людини), на підставі яких формуються звіти, що є підставою для оплати наданих медичних послуг, лікарських засобів та медичних виробів за програмою медичних гарантій, або які містять персональні дані пацієнтів, медичних працівників, яким (якими) надано відповідні медичні послуги, лікарські засоби та медичні вироби» [21] регламентується відповідним Наказам Мінфіну від 01.05.2024 № 219.

Водночас, З впровадженням електронної системи охорони здоров’я (ЕСОЗ) проблема захисту персональних даних пацієнтів посилюєьбся. Перехід медичних даних у цифровий формат та недостатнє розуміння

принципів обробки персональних значно підвищують ризик розголошення конфіденційної інформації. Витік даних про стан здоров'я пацієнтів чи подробиці їх лікування може спричинити серйозні наслідки як для самого пацієнта, так і для співробітника, з вини якого стався інцидент, а також для медичного закладу загалом. Тому забезпечення надійного захисту персональних даних пацієнтів є ключовим завданням під час роботи з ЕСОЗ.При цьому, Збір та обробка персональних даних пацієнта у системі «Електронне здоров'я» регулюється Законом України «Про захист персональних даних», Законом України «Про державні фінансові гарантії медичного обслуговування населення», Постановою КМУ «Деякі питання електронної системи охорони здоров'я» №411 від 25.04.2018.

Також у 2020р. схвалено Концепцію розвитку електронної охорони здоров'я, відповідно до якої «електронна система охорони здоров'я eHealth – інформаційно-телекомунікаційна система, що забезпечує автоматизацію ведення обліку медичних послуг та управління медичною інформацією в електронному вигляді та надає можливість кожному пацієнту швидко отримати свою медичну інформацію, а лікарям – правильно ставити діагноз, враховуючи цілісну картину здоров'я пацієнта, виписувати електронні рецепти» [3]. В межах роботи цієї системи відбувається акумулювання величезної кількості персональних даних громадян.

Процедура роботи з персональними даними пацієнтів починається з підписання декларації про вибір лікаря первинної медичної допомоги відповідно до норм наказу Міністерства охорони здоров'я №503 від 19.03.2018 р. «Про затвердження Порядку вибору лікаря, який надає первинну медичну допомогу, та форми декларації про вибір лікаря, який надає первинну медичну допомогу» [4]. Важливо зауважити, що підписана декларація про вибір лікаря є документом, згадно з яким медичний персонал отримує доступ до персональних даних пацієнтів, оскільки до персональних даних належить вся інформація, яка підлягає внесенню в декларацію (прізвище, ім'я, по батькові, дата народження, РНОКПП, дані документа, що посвідчує особу, адреса проживання, засоби зв'язку).

Концепція розвитку електронної охорони здоров'я передбачає забезпечення пацієнтів доступом до їхніх персональних даних та використання інших можливостей електронної системи охорони здоров'я через електронний кабінет пацієнта. За даними МОЗ України, медичні дані в електронній системі охорони здоров'я мають вищий рівень захисту порівняно з паперовими картками пацієнтів, що зберігаються в медичних закладах. Система eHealth використовує сучасні технології безпеки, серед яких кваліфіковані електронні підписи, розподілене зберігання медичної та особистої інформації, а також алгоритми, що гарантують цілісність даних. Окрім цього, система отримала атестат відповідності КСЗІ, який підтверджує відповідність державним вимогам у сфері захисту інформації.

Українське законодавство встановлює адміністративну та кримінальну відповідальність за порушення правил обробки персональних даних пацієнтів. Відповідальність за контроль у цій сфері покладено на Уповноваженого Верховної Ради України з прав людини, в секретаріаті якого працює Департамент захисту персональних даних. Водночас експерти часто підкреслюють необхідність створення незалежного органу, який би забезпечував ефективний контроль за дотриманням прав на захист персональних даних і доступ до публічної інформації.

Приведення українського законодавства у відповідність до європейських стандартів у сфері захисту персональних даних через впровадження Регламенту Європейського Парламенту та Ради 2016/679 (Загального регламенту про захист даних, GDPR)[7] є одним із основних завдань України. Це передбачено пунктом 11 Плану заходів щодо виконання Угоди про асоціацію, затвердженого постановою Кабінету Міністрів України від 25 жовтня 2017 року №1106, однак реалізація цього завдання поки що залишається незавершеною.

Українські медичні заклади та підприємства, які надають послуги громадянам ЄС або здійснюють моніторинг поведінки осіб, що перебувають у ЄС, автоматично підпадають під дію положень GDPR. Медичний туризм є однією з привабливих сфер для іноземців в Україні завдяки доступним цінам

(іноді вдвічі нижчим, ніж у країнах ЄС) та високій якості медичних послуг. Найбільш популярними напрямками є стоматологія, офтальмологія, репродуктивна медицина, неврологія, кардіологія, клітинна терапія та реабілітація.

GDPR передбачає можливість накладення санкцій контролюючими органами країн ЄС за межами їх територій, включно з Україною. Це обумовлює обов'язковість дотримання вимог Регламенту.

Регламент передбачає суттєві зміни в процесах збору, обробки, зберігання та передачі медичних даних. Пацієнти мають надавати інформовану згоду на використання своїх даних, а також мають право відкликати її або вимагати видалення інформації за певних умов. Наприклад, громадянин ЄС може звернутися до медичного закладу з вимогою видалити свої медичні записи, і заклад зобов'язаний виконати цей запит.

GDPR визначає три ключові категорії персональних даних, важливих для медичної сфери:

- Дані про здоров'я – відомості про фізичний або психічний стан людини, включаючи інформацію про отриману медичну допомогу.
- Генетичні дані – характеристики, які можуть розкрити фізіологічні або медичні деталі, включаючи результати лабораторних аналізів.
- Біометричні дані – фізичні або поведінкові характеристики (наприклад, відбитки пальців, зображення обличчя), що дозволяють ідентифікувати особу.

Регламент встановлює жорсткі вимоги до інформованої згоди пацієнта. Згода повинна містити чітке визначення типу даних, мети їх збору, а також пояснювати потенційні ризики. Вона повинна бути надана в зрозумілій та доступній формі з можливістю підтвердження або відмови.

Отже, для українських медичних установ дотримання вимог GDPR є важливим викликом, що потребує адаптації їх діяльності до європейських стандартів.

Згідно з GDPR, відповідальність за обробку персональних даних покладається на дві сторони: контролера та процесора. Контролером є

фізична чи юридична особа або орган державної влади, які визначають цілі й методи обробки даних. Процесор — це суб'єкт, який здійснює обробку даних на підставі вказівок контролера. Наприклад, лікарня, яка збирає інформацію про пацієнтів, виступає в ролі контролера, тоді як розробник програмного забезпечення, де зберігаються дані, або медичний персонал, що вводить дані в систему, виконують функції процесорів (обробників).

Контролер і процесор несуть спільну відповідальність за дотримання норм GDPR. Уразі порушення, такого як витік, несанкціонований доступ чи крадіжка даних, вони зобов'язані протягом 72 годин повідомити про це відповідні контролюючі органи, а в окремих випадках — і суб'єктів даних.

Отже, українські медичні заклади неминуче мають адаптувати свою діяльність до вимог GDPR для забезпечення відповідності міжнародним стандартам захисту даних.

Важливо зазначити, що на рівні ЗОЗ можуть розроблятися Положення про обробку та захист персональних даних пацієнтів, **які** визначають комплекс заходіворганізаційного та технічного характерів для забезпечення захисту персональних даних пацієнтів від несанкціонованого доступу, витоку інформації, неправомірного використання або втрати під час обробки. Такі положення розробляються відповідно до чинних нормативно-правових актів з питань захисту персональних даних та вони є обов'язковим для виконання працівниками медзкладу, які мають доступ до персональних даних пацієнтів та обробляють персональні дані.

РОЗДІЛ 2

АНАЛІЗ ПРАКТИКИ ОРГАНІЗАЦІЇ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ ПАЦІЄНТІВ В КНП «ЗОЛОТНИКІВСЬКА РАЙОННА ЛІКАРНЯ»

2.1. Організаційно-функціональне забезпечення системи захисту персональних даних пацієнтів лікарні

Вивчення чинної практики організації роботи із захисту персональних даних пацієнтів нами проводився на матеріалах КНП «Золотниківська районна лікарня» Золотниківської сільської ради (далі –КНП«ЗРЛ»). Дане медичне підприємство надає медпослуги вторинної медичної допомоги населенню Золотниківської територіальної громади та громадам на території Тернопільського району, «іншим громадянам інших населених пунктів, згідно з укладеними договорами на медичне обслуговування» [41]. У нинішньому правовому статусі КНП було створене в лютому 2022р. рішенням Золотниківської СР. На даному етапі КНП діє у відповідності до затвердженого Статуту. Його засновником є Золотниківська СР.

КНП є юридичною особою і користується майном, що є власністю ТГ, за правом оперативного управління. Це право реалізується через можливість використовувати отримане в користування майно для забезпечення власних потреб в необхідних коштах, але з певними обмеженнями. Такі обмеження прописані в Статуті, як заборона продажу майна або ж нецільового використання.

До джерел, що формують його активи, належать «комун.майно, що було передане закладу при його формуванні; кошти місцевого та державного бюджетів; банківські кредити; кошти благодійних внесків іпожертвувань, а також кошти, що надходять на забезпечення реалізації програм і проєктів розвитку закладу, інших незаборонених коштів тощо.

Основною метою діяльності КНП«ЗРЛ» «є забезпечення спеціалізованої, висококваліфікованої медичної допомоги населення шляхом надання йому медичних послуг в порядку та обсязі, встановлених чинним

законодавством України» [41]. Також вживаються заходи з профілактики захворювань та підтримання гроадськогоздоровя. Основною діяльністю закладу, згідно наданої ліцензії, є «Діяльність лікарняних закладів -86.10» та інші види діяльності «86.21 Загальна медична практика. 86.90 Інша діяльність у сфері охорони здоров'я».

Коротка характеристика КНП «ЗРЛ» наведена в табл. 1.1.

Таблиця 1.1

Коротка характеристика КНП «Золотниківська районна лікарня »

Повне найменування юридичної особи	КОМУНАЛЬНЕ НЕКОМЕРЦІЙНЕ ПІДПРИЄМСТВО ЗОЛОТНИКІВСЬКА РАЙОННА РАДА Золотниківської сільської ради
Код ЄДРПОУ/ статус	02001067 /Юридична особа
Скорочена назва	КНП "Золотниківська РЛ", КНП «ЗРЛ»
Дата реєстрації	05.03.1999. (25 років) Реорганізоване. Зареєстровано 23.02.2022р.
Розмір статутного капіталу	1000 грн
Організаційно-правова форма	КОМУНАЛЬНЕ ПІДПРИЄМСТВО
Власник	Золотниківська сільська рада
Види діяльності	Основна: 86.10 Діяльність лікарняних закладів
	Інші: 86.21 Загальна медична практика 86.90 Інша діяльність у сфері охорони здоров
Кількість працівників, осіб	68 (2024р.)
Чистий прибуток	3165тис. грн.

Засадничими статутними вимогами провадження операційно діяльності лікарні, є : «діяльність у відповідності до затвердженого фінансового плану; надання платних медичних послуг за тарифами, затвердженими засновником, залучення необхідних фінансових, матеріально-технічних та трудових ресурсів; формування та затвердження організаційної структури управління та чисельності працівників, складання штатного розпису; здійснення закупівлі товарів і послуг через встановлені законодавством процедури» [43]. До базових прав, які забезпечують правову основу діяльності КНП, належать: отримання інформації та матеріалів, які необхідні для того, щоб виконувати покладені на заклад завдання; можливість «самостійно

планувати, організовувати і здійснювати статутну діяльність, визначати основні напрямки свого розвитку відповідно до своїх завдань і цілей, утому числі спрямовувати отримані від господарської діяльності кошти на утримання підприємства та його матеріально-технічного забезпечення» [43]; забезпечення укладання господар ських договорів з усіма зацікавленими сторонами для надання якісних МП; здійснення співробітництва з зарубіжними партнерами у питаннях покращання якості медобслуговування населення за спеціалізованими напрямами надання МД; самостійне; самостійне визначення напрямів використання отриманих коштів, але у порядку, передбаченому законодавством України; здійснювати співпрацю з іншими ЗОЗ та організаціями, здійснювати консультативний супровід пацієнтів тощо.

Предметом діяльності КНП «ЗРЛ», відповідно до його статуту, є:

здійснення медичної практики з надання вторинної МД;

створення спільно із засновникомКНП сприятливих умов «для забезпечення доступної та якісної медичної допомоги населенню, організації належного управління внутрішніми лікувально-діагностичним процесом та ефективного використання майна та інших ресурсів підприємства» [43];

надання консультацій з питань профілактики, діагностування і лікування захворювання, ведення здорового способу життя;

дотримання у медичній практиці принципів доказової медицини, а також, медичних стандартів якості МД;

обрахунок потреби у лікарських засобах, мед.обладнанні, медичних виробах, транспортних засобів для того, щоб забезпечити доступність , своєчасність та якість МД;

«надання елементів паліативної допомоги пацієнтам на останніх стадіях перебігу невиліковних захворювань, яка визначає комплекс заходів, спрямованих на полегшення фізичних та емоційних страждань пацієнтів, моральну підтримку членів сімей» [43].

На КНП в рамках забезпечення ефективної дальності з виконання операційних завдань покладаються наведені на рис. 2.1. обов’язки.

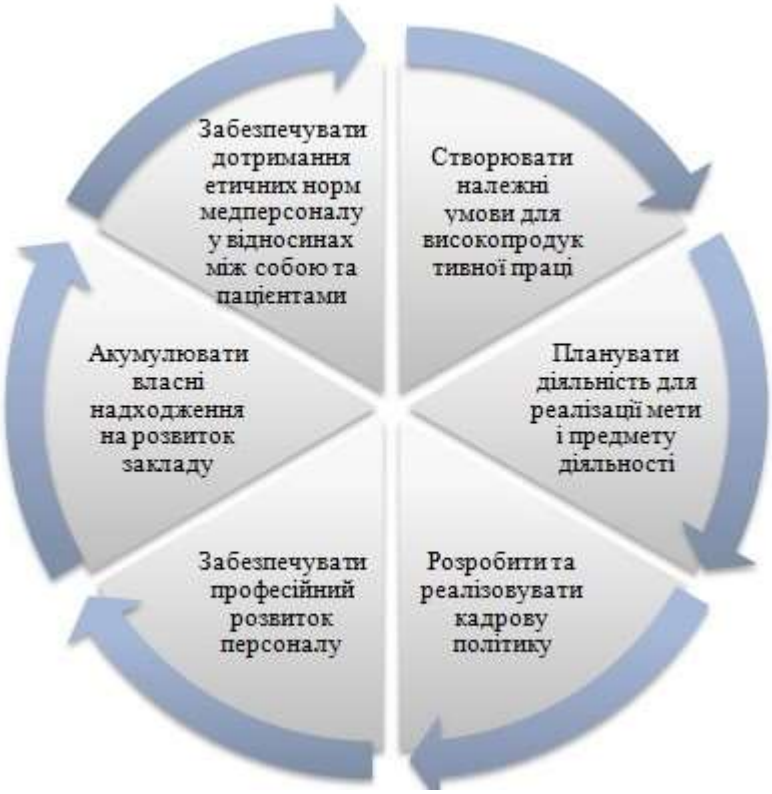

Рис. 2.1. Обов’язки управлінської діяльності КНП «ЗРЛ»

Операційна діяльність медичного закладу спрямовується на надання медичної допомоги населенню громади і району у необхідному обсязі , в установленому порядку та належної якості. Такі послуги надаються в структурних підрозділах лікарні, до яких входять:

відділи: терапевтичний, фізіотерапевтичний;

жіноча консультація;

лабораторії: клініко-діагностична;

кабінети: хірургічний, психологічний, офтальмологічний, отоларингологічний; інфекційних захворювань.

Варто зазначити, що в 2023р. в лікарні було відкрито відділення паліативної допомоги населенню. Його потужність складає 20 ліжок. Як зазначається в наведеній інформації, у стаціонарі паліативної допомоги «забезпечується повний комплекс побутового і медичного догляду, надається симптоматичне медикаментозне лікування, складання плану спостереження пацієнта, що потребує паліативної допомоги, проводиться підбір індивідуальної схеми протибольової терапії та здійснюється кваліфікований

догляд, також пацієнти консультуються фахівцями суміжних відділень лікарні. Відділення забезпечене функціональним ліжками, проти пролежневими матрацами, кріслами-візками, каталками та ін.» [40]. Надання такої допомоги здійснюється за програмою медичних гарантій і під яку НСЗУ виділило фінансування.

За статистичною звітністю лікарні, в 2023р. були надані послуги:

з операційного втручання (проведено 93 операції);

терапевтичної допомого (надано 667 пацієнтам);

паліативної допомого (отримали 115 пацієнтів);

профілактичних оглядів 166 мешканцям громади, обстежено на профогляд з метою захворювання на туберкульоз – 849 сільських жителів.

ультразвукових досліджень (було проведені для 2707 громадян).

Чисельність пролікованих пацієнтів та стан використання ліжкового фонду в КНП «ЗРЛ» наведено в табл.2.2.

Таблиця 2.2

Використання ліжкового фонду в КНП «ЗРЛ» в 2023р.

Профіль ліжок	Кількість ліжок, фактично розгорнутих та згорнутих на ремонт		У звітному році (кількість)				Проведено хворими ліжко-днів
	на кінець звітного року	середньо-річних	надійшло хворих, усього	у тому числі дітей віком 0-17 р.	випи сано хворих	Помер ло	
А	1	2	3	4	5	6	7
Усього у тому числі:	50,00	50,00	**1394**	612	1385	3	12184.00
Терапевтичні	15,00	15,00	**667**	-	672	2	5398.00
Педіат.ком.вт.ч:	15,00	15,00	**612**	612	609	-	4634.00
Інші д/дорослих	20,00	20,00	**115**	-	104	1	2152.00
Паліативної допомоги для дорослих	20,00	20,00	**115,00**	-	104	1	2152.00

Наведено за [42]

Аналіз системи управління в КНП засвідчив, що вона на сьогодні має спрощену структуру і представлена керівництвом лікарні (директором та медичним директором), головним бухгалтером, інспектором з кадрів, спеціалістом із публічних закупівель, керівниками структурних підрозділів.

Загальне керівництво КНП провадить Золотниківська СР, як засновник закладу, а оперативне управління забезпечується директором закладу , який, згідно Статуту, призначається і звільняється з неї за рішенням засновника.

Основний функціонал керівництва лікарні полягає в організації роботи лікарні щодо надання медичної допомоги населенню та забезпечення

належного медичного обслуговування пацієнтів. Функціональні завдання керівника, визначені Статутом лікарні, проілюстровано на рис. 2.2.

ФУНКЦІОНАЛ ДИРЕКТОРА КНП «ЗРЛ»

Організовує роботу щодо надання населенню медичної допомоги.

Організовує та моні торить виконання операційних планів.

Несе відповідальність за формування та виконання фінансового плану і плану розвитку Підприємства, результати його господарської діяльності, виконання показників ефективності діяльності Підприємства, якість послуг, що надаються, використання наданого на праві оперативного управління майна спільної власності територіальних громад

Забезпечує контроль за веденням та зберіганням медичної та іншої документації.

Приймає рішення про прийняття на роботу, звільнення з роботи працівників Підприємства, укладає трудові договори з працівниками. Забезпечує раціональний добір кадрів, дотримання працівниками правил внутрішнього трудового розпорядку. Створює умови підвищення фахового і кваліфікаційного рівня працівників згідно із затвердженим в установленому порядку штатним розписом.

Вживає заходи щодо своєчасної та в повному обсязі виплати заробітної плати, а також передбачених законодавством податків, зборів та інших обов'язкових платежів.

Затверджує положення про структурні підрозділи Підприємства, інші положення та порядки, що мають системний характер, зокрема:

- положення про преміювання працівників за підсумками роботи Підприємства;
- порядок надходження і використання коштів, отриманих як благодійні внески, гранти та дарунки;
- порядок приймання, зберігання, відпуску та обліку лікарських засобів та медичних виробів.

Керівник Підприємства та головний бухгалтер **несуть персональну відповідальність за додержання порядку ведення і достовірність обліку та статистичної звітності у встановленому законодавством порядку**

Рис. 2.2. Функціонал директора КНП«ЗРЛ»

Як свідчать наведені на рис. 2.2. функціональні повноваження керівництва лікарнею, то в їх переліку відсутні завдання, пов'язані із захистом персональних даних пацієнтів, а збереження конфіденціальної

інформації про пацієнтів реалізується в межах дотримання етичних норм у впровадженні медичної практики. Єдиним напрямом функціональної діяльності КНП, де застосовуються контрольні і обмежувальні заходи щодо інформації про пацієнтів, є забезпечення контролю за належним веденням ізберіганням медичної таїншої документації, в яких ці дані представлені через облік пацієнтів, які перебували в лікарні.

Надання медичної допомоги в лікарні забезпечує 68 медпрацівників, з яких лікарів – 18,0 осіб (або 26, 5% до загальної чисельності працюючих), середнього медичного персоналу - 22,0 особи (або 32,4% у заг.чиссельності), молодшого медперсоналу – 11 осіб (або 16,2% заг.чисельності), адміністративний персонал – 5 осіб (або 7,4%) та інші – 11 осіб (16,2%).

Розподіл медичного персоналу лікарні в розрізі посад та за рівнем кваліфікації станом на початок 2024р.наведено в табл.2. 3.

Таблиця 2.3

Чисельність медичного персоналу КНП «Золотницької районної лікарні» та їх розподіл за посадами

Найменування посад	Кількість посад у цілому в закладі		у тому числі в поліклініці (амбулаторії), диспансері, консультації		Кількість штатних працівників на зайнятих посадах, осіб
	штатних	зайнятих	штатних	зайнятих	
А	1	2	3	4	5
Лікарі, усього	18.50	13.0	9.50	5.50	10.00
у т.ч. керівники закладів та їх заступники	1.00	1.00	-	-	1.00
Середній медперсонал	22,5	21,0	4,0	3,5	18,0
Молодший медперсонал	11,0	11,0	2,0	2,0	10,0
Адміністративно-господарський персонал	13,0	13,0			13,0
Інший з немедичною освітою	3,0	3,0			3,0
ВСЬОГО	68	61	15,5	11	55

Аналіз наведених в табл.2.3. даних свідчить, що лікарня на даний час є укомплектованою на 89,7 % (тобто 10,3% посад на разі є вакантними), в т.ч. за лікарями недоукомплектованими є 28,2% посад, за старшим медперсоналом – 7,%, за молодшим медперсоналом – всі посади зайняті.

Структура посад в лікарні проілюстрована на рис. 2.3.

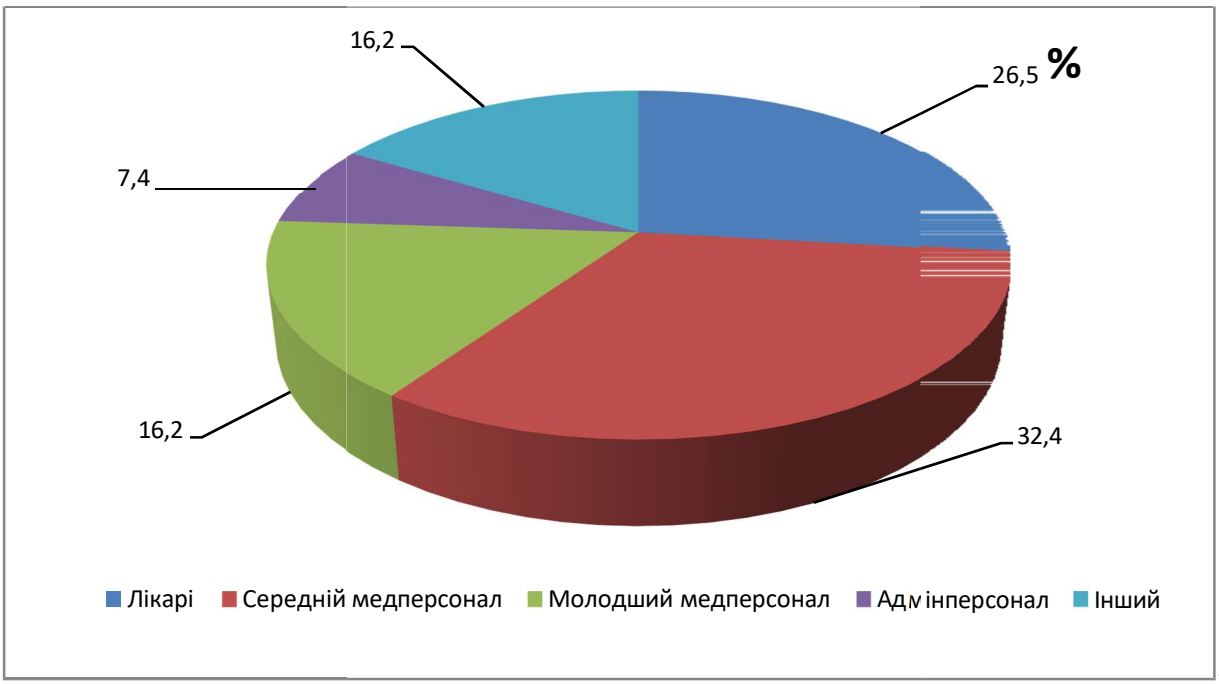

Рис. 2.3 Структура посад в КНП «ЗРЛ» в 2023р.

За якісним складом лікарський персонал характеризується такими даними: по лікарському персоналу 1 лікар має вищу кваліфікаційну категорію (або 10,0% до загальної чисельності лікарів в закладі) і один - другу. Решта (80,0%) лікарського персоналу на даний час є без категорії. По середньому медперсоналу лікарні 6 медичних сестер має вищу категорію (або 33,3% до заг. їх чисельності), 4-о медичних сестер має 1 категорію (або 22,25) та 1 особа – другу категорію (або 5,6%). Більше 38% середнього медперсоналу без категорії.

Важливе значення в забезпеченні діяльності медзакладу належить фінансовій складовій, яка залежить від обсягу наданих медичних послуг споживачам, а також спроможності закладу забезпечити якісне медичне обслуговування громадян. За останні три роки фінансові результати роботи КНП характеризуються даними,наведеними в табл. 2.4.

Таблиця 2.4

Фінансові результати діяльності КНП «ЗРЛ»

	2023	2022	2021	2020
Дохід	18 337,9	12 293,4	8 884,0	4 732,8
Чистий прибуток	3 165,1	304,8	1 171,7	-1 638,4
Активи	7 273,8	3 290,8	3 282,1	2 120,4
Зобов'язання	0	0	0	0
Кількість працівників осіб	68	62	59	

Аналіз динаміки показників, наведених в таблиці , дозволяє зробити такі узагальнюючі висновки:

1. Динаміка доходів свідчить про стабільне зростання доходів. Найбільш суттєве збільшення відбулося в 2023р.(на 49,2% порівняно з 2022 роком). Основними факторами, які обумовили таке зростання було збільшення обсягу фінансування НЗСУ за пакетом надання паліативної допомоги та збільшення попиту на платні послуги.

2. Чистий прибуток демонстрував позитивну динаміку з 2021р. У 2020 році лікарня мала збиток (-1 638,4 тис. грн), але вже у 2021 році досягла прибутку (1 171,7 тис. грн). У 2023 році прибуток зріс до 3 165,1 тис. грн. Різке зростання прибутку в 2023 році знову ж таки пов’язане з наданням більшого обсягу паліативної допомоги за урізноманітненим переліком послуг .

3. Активи лікарні в 2023р. суттєво збільшилися через залучення додаткових інвестицій у відкриття відділення паліативної допомоги**.**

Отже, можна зробити висновок, що КНП демонструє стабільний рівень доходів, активів і прибутків , що сприяє покращенню її фінансового стану. Відсутність зобов'язань є позитивною ознакою, оскільки знижує фінансові ризики.

Розрахункові показник ефективності діяльності лікарні наведені в табл. 2.5. Аналіз показників свідчить про їх позитивні динаміки, особливо в 2023 році.

Таблиця 2.5

Ключові показники ефективності КНП«Золотницька районна лікарня»

Рік	Рентабельність діяльності (%)	Рентабельність активів %)	Дохід на одного працівника (тис. грн)	Прибуток на одного працівника (тис. грн)
2023 рік	17.26	43.51	295,77	51.05
2022 рік	2.48	9.26	208,36	5.17
2021 рік	13.19	35,70	150,58	19.86

Позитивна динаміка розвитку КНП «ЗРЛ» закріплена у розробленій та затвердженій Програмі розвитку закладу в 202р. та внесених суттєвих змінах у 2024р. Золотниківською СР [41]. Актуальність розроблення програми обумовлена необхідністю вирішення проблем: «поліпшення якості надання медичної допомоги населенню Золотниківської ТГ ; поліпшення матеріально-технічної бази» [41]. Як зазначається у преамбулі до програми,
«основною проблемою, на яку буде спрямована Програма – проблема фінансового характеру – нестача коштів на оплату поточних та капітальних видатків. Дефіцит фінансового ресурсу унеможливлює подальшу роботу підприємства, в тому числі: проведення закупівлі матеріалів, медикаментів, покращення матеріально - технічної бази та оплату комунальних» [41].

Отже, «метою Програми є модернізація вторинної медичної допомоги для покращення якості надання медичної допомоги КНП «ЗРЛ»ЗСР шляхом покращення його ресурсного забезпечення, зміцнення матеріально-технічної бази, поліпшення превентивної медичної допомоги мешканцям територіальної громади, зниження рівня смертності та поліпшення показників здоров'я населення, закупівлю медикаментів, медичних виробів та засобів, проведення поточних та капітальних ремонтів лікарні» [41].

Реалізація мети розвитку лікарні, буде вирішуватися засобами і підходами, наведеними на рис. 2.3. Як видно із наведених напрямів роботи , основна увага надається покращанню інформаційного забезпечення роботи

лікарні, оновленню матеріально-технічної бази та медичного обладнання для можливості розширити перелік послуг, які можуть надаватися лікарнею.

Рис. 2.3. Напрями розв'язання проблем розвитку КНП «ЗРЛ»

Реалізація програми розвитку КНП дозволить забезпечити надання якісної вторинної МД населенню; покращити МТБ КНП«ЗРЛ»ЗСР; покращити доступність МД до жителів Золотниківської ТГ.

Оскільки на даний час медичний заклад не може забезпечити можливість належного захисту персональних даних пацієнтів із-за відсутності спеціального інформаційного ресурсу, проблемності його належного утримування з-за відсутності фінансування, то реалізації програмних засад дозволить в якійсь мірі ці питання розв'язати.

2.2. Оцінка діючих процедур захисту персональних даних пацієнтів в досліджуваному КНП

Аналіз процедур захисту персональних даних пацієнтів в КНП засвідчив про певну проблематику в надійності гарантованого збереження персональних даних з огляду на те, що в закладі є відсутніми сучасні

інформаційні системи для організації такої роботи, відсутність кваліфікованого спеціаліста (програміста) з інформаційного забезпечення роботи МІС у штатному розпису, а також не призначена відповідальна особа за таку ділянку роботи та не розроблені відповідні положення та інструкції з організації захисту персональних даних пацієнтів лікарні.

Для вироблення дієвих підходів до організації захисту персональних даних пацієнтів в КНП розглянемо загальну проблематику такої роботи та можливості уникнути ситуацій, які тягнуть за собою окрім зниження репутації закладу, і юридичну відповідальність.

Загалом, як зазначалося в розділі 1 процедури захисту персональних даних пацієнтів (далі – ЗПД) є ключовими для забезпечення конфіденційності та дотримання прав людини в системі охорони здоров'я. Цей процес передбачає дотримання законодавчих норм і впровадження технічних, організаційних та адміністративних заходів для запобігання порушенням.

В юридичному аспекті вивчаються норми чинного законодавства, зокрема Закон України «Про захист персональних даних», а також міжнародні стандарти, як-от GDPR. Це дозволяє виробити внутрішню політику захисту, як от відповідного регламенту конфіденційності, інструкції для працівників, договір про нерозголошення (NDA), укладання угоди з пацієнтом, оскільки передача чи обробка даних можлива лише за його письмовою згодою.

В організаційному аспекті щодо ЗПД пацієнта в закладі призначається відповідальної особи,яка є спеціалістом, що контролює дотримання правил обробки даних, здійснює навчання працівників як правильно працювати з даними і уникати витоків, сегментувати доступ до даних, що передбачає необхідність надання такої інформації і доступу до неї лише тим, кому це необхідно для виконання професійних обов'язків.

Технічний аспект ЗПД пацієнта передбачає використання технічних можливостей закладу, а саме можливості шифрування даних як при передачі, так і при зберіганні, захисту систем від хакерських атак шляхом

встановлення антивірусів, міжмережевих екранів, регулярного оновлення програмного забезпечення; забезпечення резервного копіювання даних.

Фізичний захист передбачає захист серверних приміщень, архівів із паперовими даними (сейфи, замки) та контроль доступу до робочих станцій і пристроїв (ключі, паролі, біометрія).

Типовими проблемами ЗПД пацієнтів , що спостерігаються у багатьох ЗОЗ є (рис. 2.5) :

недостатність ресурсів;

вразливість ІТ-систем;

неправомірний доступ;

недоліки законодавства:

культурні фактори.

Рис. 2.4. Типові проблеми захисту персональних даних пацієнтів

За ЗПД пацієнтів у лікарні, як правило, відповідає уповноважена особа або підрозділ, який займається питаннями захисту інформації. Це може бути окремий працівник (наприклад, Уповноважений з питань захисту персональних даних) або служба, що спеціалізується на інформаційній безпеці.

Загалом, ЗПД пацієнтів мають сукупно вирішувати директор КНП, уповноважений з питань ЗПС, І-Т відділ (або спеціаліст з ІТ, керівники структурних підрозділів). Їх обов'язки наведені в табл.2.6.

Таблиця 2.6

Функціональні обов'язки відповідальних осіб за захист персональних даних пацієнтів

Відповідальна особа	Функціональна відповідальність
Директор КНП, Медичний директор	➢ Відповідає за загальну організацію процесу захисту персональних даних. ➢ Затверджує внутрішні політики та процедури щодо обробки даних. ➢ Забезпечує створення належних умов для безпечної роботи з інформацією. ➢ Призначає уповноважену особу або підрозділ для контролю цього процесу.
Уповноважена особа з питань захисту персональних даних	➢ Координує діяльність щодо захисту даних у лікарні. ➢ Розробляє внутрішні регламенти, інструкції, політики та рекомендації для персоналу. ➢ Контролює дотримання законодавства про захист даних. ➢ Виступає зв'язковою ланкою між пацієнтами, персоналом і державними органами. ➢ Проводить регулярні перевірки систем захисту. ➢ Здійснює навчання співробітників щодо роботи з персональними даними
ІТ-відділ (технічна підтримка):	➢ Забезпечує технічну реалізацію заходів захисту (паролі, шифрування, резервне копіювання). ➢ Реагує на кіберінциденти або порушення безпеки
Керівники структурних підрозділів лікарні	➢ Контролюють дотримання правил роботи з персональними даними у своїх відділах. ➢ Звітують перед головним лікарем або уповноваженою особою про порушення.

За порушення вимог ЗПД пацієнта і порушення конфіденційності лікарської інформації передбачаються заходи дисциплінарної, адміністративної, матеріальної, кримінальної та репутаційної відповідальності. Основними факторами, що впливають на ступінь відповідальності за допущення витоку інформації є:

характер дій особи, що допустила витік інформації, а саме чи було порушення результатом недбалості або свідомого рішення;

наслідки порушення, що випливає з обсягу і важливості розголошеної інформації, нанесена шкода пацієнту.

ступінь дотримання встановлених процедур: якщо уповноважена особа діяла відповідно до затверджених регламентів, її відповідальність може бути обмеженою.

Як засвідчила практика недотримання вимог ЗПД пацієнтів, найчастіше вони виникають у таких нестандартних ситуаціях, наведених в табл. 2.7.

Таблиця 2.7

Ситуації, в яких порушуються вимоги захисту персональних даних пацієнтів

Подія	Ситуація, причина її виникнення та наслідки
Розголошення інформації медичним персоналом:	**Ситуація**: Медсестра поділилася інформацією про пацієнта з іншими працівниками або знайомими, що не мали права доступу до цих даних. **Причина**: Недостатнє навчання персоналу або банальна людська недбалість **Наслідки**: Порушення приватності пацієнта, подання скарги до керівництва або суду
Випадковий витік даних через електронну пошту	**Ситуація**: Лікар відправив дані про пацієнта помилково на іншу адресу електронної пошти. **Причина**: Відсутність перевірки адресата перед надсиланням або помилка через поспіх. **Наслідки**: Витік конфіденційної інформації, репутаційні ризики для лікарні
Використання незахищених IT-систем	**Ситуація**: Внаслідок кібератаки були викрадені медичні записи пацієнтів, включно з інформацією про їхні діагнози. **Причина**: Відсутність належного захисту систем, використання застарілого програмного забезпечення. **Наслідки**: Збитки для лікарні, штрафи за недотримання правил захисту даних, шкода репутації.
Обговорення стану пацієнта в громадських місцях	**Ситуація**: Лікарі чи медсестри обговорювали стан пацієнта у присутності сторонніх осіб (наприклад, у коридорі чи кафе). **Причина**: Недотримання етичних стандартів та конфіденційності. **Наслідки**: Порушення приватності, скарги від пацієнтів
Помилка у видачі медичних документів	**Ситуація**: Інформація про пацієнта була передана іншій особі через неправильну обробку запитів на документи. **Причина**: Недбалість адміністративного персоналу. **Наслідки**: Розголошення конфіденційних даних, скарги та репутаційні втрати.
Публікація медичних даних у ЗМІ або соцмережах	**Ситуація**: Інформація про пацієнта стала відомою громадськості через витік даних або розголошення лікарем у публічному просторі. **Причина**: Недотримання законодавства або етичних стандартів. **Наслідки**: Судові позови, значні штрафи, втрата довіри до медичного закладу

Частота такі порушення залежить від рівня організації та цифровізації сфери охорони здоров’я загалом. Як стверджують фахівці, [40] у країнах із низьким рівнем автоматизації (де переважають паперові записи) виникають одні типи порушень, тоді як у цифрових системах ризики пов'язані

переважно з ІТ-безпекою. Приміром, за даними звітів у ЄС (GDPR), медичні заклади входять до групи найбільш вразливих організацій через велику кількість чутливих даних. В Україні випадки витоків менш задокументовані, проте основними проблемами є низький рівень ІТ-захисту та необізнаність персоналу.

Для того щоб ефективно запобігати порушенням вимог ЗПД пацієнтів у медичному закладі доцільним вважаємо:

проводити регулярні навчання персоналу з питань забезпечення конфіденційності медичної інформації про захворювання пацієнта;

використовувати сучасні технології захисту (шифрування, брандмауери);

впроваджувати чіткі регламенти роботи з персональними даними;

здійснювати моніторинг і аудит ІТ-систем;

інформувати пацієнтів про їхні права та правила обробки їхніх даних.

шукати фінансові можливості для цифровізації та захист інформації.

РОЗДІЛ 3
ІННОВАЦІЙНІ ТЕХНОЛОГІЇ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ ПАЦІЄНТІВ В ЗАКЛАДІ ОХОРОНИ ЗДОРОВ'Я

3.1. Блок-чейн технології як інструмент забезпечення безпеки персональних даних пацієнта

Блокчейн (від англ. blockchain, що означає «ланцюг блоків») – це децентралізована та розподілена цифрова технологія зберігання та передачі інформації, яка організована у вигляді послідовно з'єднаних блоків даних. Кожен блок містить записи транзакцій, час їх створення та криптографічний підпис (хеш), який пов'язує його з попереднім блоком, утворюючи безперервний і незмінний ланцюг.

1. Технологія блокчейн має низку переваги, яка робить її винятково важливою для всіх сфер національної економіки, зокрема:

2. Децентралізація. Інформація зберігається в розподіленій мережі вузлів, що виключає необхідність у централізованих серверах. Це зменшує залежність від одного центру управління і підвищує стійкість системи.

3. Безпека даних. Дані у блокчейні зашифровані та захищені криптографією. Це унеможливлює несанкціонований доступ, зміну або видалення інформації без згоди учасників мережі.

4. Незмінність записів. Після запису даних у блок їх неможливо змінити чи видалити, що забезпечує цілісність і надійність інформації. Це особливо важливо для юридично значущих даних.

5. Прозорість та довіра. Учасники мережі мають доступ до загального реєстру транзакцій, що робить систему прозорою і підвищує рівень довіри між сторонами.

6. Висока доступність. Завдяки розподіленій природі, система залишається доступною навіть у разі виходу з ладу частини вузлів мережі.

7. Ефективність та автоматизація. Використання смарт-контрактів дозволяє автоматизувати бізнес-процеси, зменшуючи час на обробку транзакцій і мінімізуючи витрати.

8. Відстежуваність транзакцій. Кожна транзакція у блокчейні має часову мітку, що дозволяє відстежувати всю історію змін.

9. Стійкість до хакерських атак. Завдяки децентралізації, система менш вразлива до кібератак. Для компрометації блокчейну необхідно отримати контроль над більшістю вузлів мережі, що є технічно складним.

10. Зменшення посередників. Блокчейн дозволяє проводити прямі транзакції між сторонами без участі посередників, що зменшує витрати та час.

11. Інноваційність та гнучкість. Технологія може бути адаптована до різних галузей, таких як фінанси, охорона здоров'я, логістика, державне управління, енергетика тощо.

Використання блокчейну дозволяє створити надійні, прозорі та ефективні системи, які відповідають сучасним вимогам до безпеки та продуктивності, роблячи його універсальним інструментом для вирішення широкого спектра задач.

Блокчейн технології сьогодні використовуються в різних сферах національної економіки: в сфері фінансів – для криптовалют, цифрових платежів і смарт-контрактів; в сфері охорона здоров'я – для захисту персональних даних пацієнтів, обміну медичною інформацією; в сфері логістики – для відстеження товарів у ланцюгах постачання; в сфері управління – для проведення електронних голосувань, зберігання офіційних документів; в сфері телекомунікації –для забезпечення безпечного обміну даними.

Сфера охорони здоров'я є одним із пріоритетних напрямків використання блокчейну. Блокчейн-технології виступають сучасним та ефективним інструментом забезпечення безпеки персональних даних пацієнтів у медичних закладах. Їх унікальні особливості, такі як децентралізація, прозорість, незмінність даних і захист від несанкціонованого доступу, дозволяють створити надійну платформу для обробки, зберігання та передачі чутливої медичної інформації.

Основні напрямки їх використання включають:

1. Децентралізоване зберігання даних. Блокчейн дозволяє уникнути залежності від централізованих серверів, що зменшує ризик масштабних витоків даних. Кожна транзакція із записом даних фіксується у захищеному реєстрі, доступ до якого строго регламентований.

2. Контроль доступу до даних.Пацієнти можуть самостійно контролювати, хто і коли отримує доступ до їхніх медичних даних. Блокчейн надає можливість налаштовувати індивідуальні рівні доступу для лікарів, страхових компаній чи інших третіх сторін.

3. Автентифікація користувачів і пристроїв. Використання блокчейну для управління цифровими ідентифікаціями дозволяє надійно ідентифікувати пацієнтів, лікарів та медичний персонал, а також медичні пристрої, забезпечуючи безпеку обміну інформацією.

4. Захищений обмін даними.Завдяки шифруванню та смарт-контрактам, блокчейн забезпечує безпечний обмін медичними даними між різними установами та системами, уникаючи ризику несанкціонованого доступу.

5. Смарт-контракти для автоматизації процесів. Блокчейн дозволяє автоматизувати виконання умов, наприклад, доступ до даних можливий тільки після отримання згоди пацієнта. Це знижує ймовірність людських помилок і забезпечує прозорість процесів.

6. Верифікація даних та історія змін. Блокчейн створює незмінний журнал записів, який фіксує всі дії з даними, включаючи внесення змін, доступ або передачу. Це спрощує аудит і підвищує довіру до системи.

7. Захист від кібератак. Децентралізація блокує можливість компрометації всієї системи через одну точку зламу, що робить блокчейн високоефективним механізмом захисту від кібератак.

8. Підтримка телемедицини та мобільних додатків. Блокчейн може забезпечити безпечний доступ до персональних даних пацієнтів у мобільних додатках і платформах телемедицини, надаючи захист від несанкціонованого доступу.

9. Використання цифрових підписів. Цифрові підписи, інтегровані з

блокчейном, гарантують, що будь-який запис у реєстрі є автентичним і належить визначеному користувачу.

10. Відстеження доступу та прозорість. Пацієнти отримують можливість бачити, хто, коли і з якою метою отримував доступ до їхніх даних, що підвищує довіру до системи.

Ці напрямки роблять блокчейн технології важливим інструментом для забезпечення конфіденційності, безпеки та ефективного управління персональними даними у медичних закладах. Розглянемо деякі із них більш детально.

Використання блокчейн-технологій для забезпечення децентралізованого зберігання персональних даних пацієнтів дозволяє забезпечити:

1. Децентралізовану структуру зберігання: блокчейн забезпечує зберігання даних у розподіленій мережі вузлів. Замість того, щоб використовувати єдиний сервер або центральну базу даних, інформація розподіляється серед учасників мережі. Кожен вузол зберігає копію реєстру, що робить систему стійкою до відмов і атак.Записи про пацієнтів розподіляються у блоках, кожен з яких пов’язаний із попереднім за допомогою криптографії.Навіть якщо один або кілька вузлів вийдуть з ладу, дані залишаються доступними в інших частинах мережі.

2. Захист від несанкціонованого доступу. Криптографічні механізми блокчейну гарантують, що лише авторизовані особи можуть отримати доступ до персональних даних пацієнтів. Пацієнти або медичні заклади отримують криптографічні ключі, які дозволяють доступ до даних. Без ключів прочитати інформацію неможливо.Пацієнти можуть надати або відкликати доступ до своїх даних медичним установам, страховим компаніям або іншим учасникам системи.

3. Незмінність записів. Будь-яка інформація, внесена в блокчейн, стає незмінною. Це особливо важливо для ведення медичних записів, оскільки гарантує їхню точність і відповідність нормативним вимогам.Усі зміни даних або доступ до них фіксуються, що дозволяє відстежувати, хто і коли

звертався до інформації.Неможливість змінити або видалити записи запобігає шахрайству і маніпуляціям.

4. Прозорість і контроль для пацієнтів. Децентралізована система дозволяє пацієнтам отримувати повний контроль над своїми персональними даними.Пацієнт вирішує, які саме дані будуть доступні для лікарів, страхових компаній або дослідницьких установ. Пацієнти можуть бачити, хто і коли отримав доступ до їхніх записів, що підвищує рівень довіри до системи.

5. Підвищення стійкості до атак. Оскільки дані зберігаються у розподіленій мережі, блокчейн є надзвичайно стійким до кібератак, зокрема до DDoS-атак і злому баз даних.Для компрометації системи необхідно одночасно змінити дані на більшості вузлів, що є технічно складним.Відсутність єдиного сервера унеможливлює його цільовий злом.

6. Можливість інтеграції зі смарт-контрактами. Смарт-контракти дозволяють автоматизувати управління даними пацієнтів. Наприклад: автоматичний доступ (дані передаються лікарю або страховику автоматично після отримання згоди пацієнта) та автоматичне оновлення (нові записи додаються до реєстру автоматично під час діагностики чи лікування).

7. Зниження адміністративних витрат. Децентралізована система блокує необхідність у посередниках для обробки даних, що скорочує адміністративні витрати.Немає потреби у великих серверах для централізованого зберігання.Децентралізація зменшує час на обробку запитів.

Блокчейн для децентралізованого зберігання персональних даних пацієнтів забезпечує високий рівень безпеки, прозорості, контролю та надійності. Використання цієї технології створює нові можливості для підвищення якості медичних послуг, довіри до закладів охорони здоров’я та зниження ризиків витоку даних.

Використання блокчейн-технологій для здійснення контролю доступу до персональних даних пацієнтівдозволяє забезпечити:

1. Реалізацію розподіленої моделі управління доступом. Блокчейн

створює розподілену систему, у якій права доступу до персональних даних пацієнтів не залежать від єдиного централізованого сервера. Кожен запит на доступ записується в блокчейн, забезпечуючи прозорість і безпеку процесу.Дані про доступ не зберігаються на одному сервері, що знижує ризики витоку.Усі запити на доступ та дії з даними записуються у блокчейн і доступні для аудиту.

2. Використання смарт-контрактів. Смарт-контракти автоматизують управління доступом до персональних даних. Це дозволяє забезпечити контроль відповідно до встановлених правил і процедур.Смарт-контракт перевіряє, чи має запитувач відповідні права на доступ до конкретних даних.Наприклад, лікар може отримати доступ до даних лише за наявності згоди пацієнта або після виконання певних умов.

3. Криптографічний захист. Дані, збережені в блокчейні, захищені за допомогою криптографічних механізмів, що дозволяють забезпечити доступ до них лише авторизованим особам.Пацієнти та медичні установи отримують унікальні ключі, що дозволяють шифрувати і дешифрувати дані.Тільки авторизовані користувачі можуть отримати доступ до даних через багатофакторну аутентифікацію.

4. Пацієнт-орієнтований контроль. Блокчейн дозволяє пацієнтам мати повний контроль над своїми даними. Вони можуть самостійно вирішувати, хто отримає доступ, які саме дані будуть доступні, і на який термін.Пацієнти можуть налаштувати рівні доступу для різних груп користувачів, наприклад, лікарів, страхових компаній або дослідницьких установ.Пацієнт може в будь-який момент відкликати наданий раніше доступ до своїх даних.

5. Невід’ємність записів. Кожен запит на доступ до персональних даних фіксується у блокчейні, забезпечуючи надійний журнал активності.Кожна взаємодія з даними (запит, передача, оновлення) записується з фіксацією часу, ідентифікатора користувача та мети доступу.Усі записи є незмінними і можуть бути використані для аудиту.

6. Прозорість і довіру. Блокчейн-технології забезпечують прозорість усіх процесів, пов’язаних з доступом до персональних даних, що підвищує

довіру пацієнтів до системи охорони здоров’я.Пацієнти можуть бачити, хто і коли отримав доступ до їхніх даних.Система дозволяє зберігати інформацію про доступ конфіденційно, водночас забезпечуючи її перевірку.

7. Інтеграція з іншими системами. Блокчейн може бути інтегрований із системами електронного документообігу та медичними інформаційними системами для ефективнішого управління доступом до даних.Інтеграція з іншими системами дозволяє зберігати цілісність даних і забезпечити зручність роботи для користувачів.Дані можуть бути надані негайно після отримання відповідного запиту.

8. Захист від несанкціонованого доступу. Блокчейн-технології роблять систему управління доступом стійкою до зовнішніх і внутрішніх загроз.Відсутність централізованої бази даних знижує ризик масових зламів.Адміністратори можуть виявляти підозрілу активність та реагувати на неї в режимі реального часу.

9. Підвищення ефективності управління. Використання блокчейну спрощує процес управління доступом і знижує адміністративне навантаження.Завдяки смарт-контрактам процеси надання та відкликання доступу можуть виконуватись автоматично.Система забезпечує простоту в управлінні правами доступу, скорочуючи потребу у посередниках.

Використання блокчейн-технологій для контролю доступу до персональних даних пацієнтів гарантує високий рівень безпеки, прозорості та ефективності. Це дозволяє медичним закладам забезпечувати захист даних, дотримуватись нормативних вимог і підвищувати довіру пацієнтів до послуг.

Блокчейн-технології є одним із найнадійніших інструментів захисту персональних даних від кібератак завдяки своїй децентралізованій, незмінній і криптографічно захищеній природі. Це дозволяє мінімізувати ризики несанкціонованого доступу, маніпуляцій або втрати даних.Використання блокчейн-технології для захисту від кібератак забезпечує:

1. Децентралізоване зберігання даних. Замість централізованих серверів, які є основними мішенями для кібератак, блокчейн забезпечує зберігання інформації у розподіленій мережі вузлів.Дані розподіляються між

багатьма вузлами мережі, що унеможливлює компрометацію всієї системи через злам одного сервера.Децентралізація знижує ризик успішного проведення атак, спрямованих на перевантаження одного вузла.

2. Незмінність даних. Кожен запис у блокчейні захищений криптографічними алгоритмами і пов'язаний з попереднім записом, що робить його незмінним.Будь-яка спроба змінити інформацію потребуватиме модифікації всіх наступних блоків у ланцюжку, що є практично неможливим через високу обчислювальну складність.Система дозволяє проводити аудит даних без ризику їхньої підробки або втрати.

3. Криптографічний захист. Блокчейн використовує складні криптографічні алгоритми для шифрування персональних даних пацієнтів.Інформація шифрується перед додаванням до блокчейну, що унеможливлює її перегляд навіть у разі доступу до блоків.Доступ до даних можливий лише за допомогою унікального приватного ключа, який належить авторизованим користувачам.

4. Аутентифікацію і доступ. Система надає можливість багатофакторної аутентифікації та суворого контролю доступу до даних.Смарт-контракти забезпечують автоматичну перевірку прав доступу до інформації.Кожна спроба доступу записується у блокчейн, забезпечуючи прозорість і можливість аудиту.

5. Захист від несанкціонованого копіювання. Дані, збережені у блокчейні, не можуть бути скопійовані або дубльовані без відображення цієї дії у мережі.Кожен блок має унікальний криптографічний хеш, що запобігає створенню фальшивих записів.Кожна дія або зміна запису вимагає підтвердження консенсусу в мережі.

6. Протидію кібератакам. Блокчейн надає високий рівень захисту від поширених типів атак, таких як фішинг, зломи баз даних або маніпуляції з даними.Завдяки багатофакторній аутентифікації зменшується ризик крадіжки облікових даних.Розподілене зберігання і шифрування унеможливлюють отримання даних навіть у разі часткового доступу до системи.Зміна даних без відома всіх учасників мережі неможлива через необхідність консенсусу.

7. Надійне відновлення після атак. У разі пошкодження вузлів мережі дані залишаються доступними через інші вузли блокчейну.Кожен вузол має копію блокчейну, що забезпечує відновлення навіть у разі компрометації частини мережі.Розподіл даних між вузлами підвищує стійкість системи.

8. Безпечний обмін даними. Блокчейн забезпечує захищений обмін інформацією між медичними закладами, страховими компаніями та іншими учасниками екосистеми.Усі передані дані шифруються.Тільки авторизовані сторони можуть отримати доступ до інформації, відповідно до умов, визначених смарт-контрактами.

Використання блокчейн-технологій для забезпечення стійкості до кібератак на персональні дані пацієнтів дозволяє створити надійну і прозору систему захисту. Вона забезпечує децентралізоване зберігання даних, криптографічний захист, незмінність записів і захищений обмін інформацією. Це знижує ризики кібератак, підвищує довіру пацієнтів до системи охорони здоров'я та сприяє ефективному управлінню даними.

Отже, використання блокчейн технологій забезпечує високий рівень безпеки персональних даних пацієнтів завдяки своїй децентралізованій структурі. Інформація зберігається у розподіленій мережі, що унеможливлює злам усієї системи через атаку на один сервер. Усі дані в блокчейні шифруються, і доступ до них можна отримати лише за допомогою унікальних ключів. Кожна дія з даними записується і захищається від змін, що дозволяє запобігти несанкціонованим маніпуляціям. Завдяки цьому забезпечується прозорий і безпечний обмін інформацією між медичними установами та іншими учасниками системи. Блокчейн також забезпечує стійкість до кібератак, оскільки видалення або зміна даних без загального схвалення мережі неможлива.

3.2. Хмарні сервіси як інноваційна технологія зберігання, обробки та управління персональними даними пацієнтів

Хмарні технології – це система доступу до обчислювальних ресурсів

(серверів, сховищ даних, додатків) через інтернет, яка дозволяє користувачам зберігати, обробляти та керувати даними у віддалених центрах обробки інформації, без потреби в локальному зберіганні чи потужному обладнанні.

Хмарні технології надають ефективні рішення для забезпечення безпеки персональних даних пацієнтів у медичних закладах. Вони дозволяють зберігати та обробляти великі обсяги даних у захищеному віртуальному середовищі, доступ до якого регулюється відповідними рівнями дозволів.

Дані пацієнтів, такі як медичні картки, результати аналізів або історії хвороб, зберігаються на серверах хмарних провайдерів із використанням сучасних методів шифрування. Шифрування забезпечує конфіденційність інформації як під час передачі між користувачами та хмарою, так і у стані зберігання. Це зменшує ризик перехоплення або несанкціонованого доступу до даних.

Хмарні платформи також забезпечують автоматичне створення резервних копій даних, що мінімізує ризик втрати інформації через технічні збої, людські помилки чи кібератаки. У випадку загрози, дані можуть бути швидко відновлені із резервного сховища.

Контроль доступу є ще однією важливою функцією хмарних технологій. Адміністратори медичних закладів можуть чітко визначати права доступу до різних рівнів інформації, наприклад, обмежуючи доступ лікарів до конкретних карток пацієнтів. Це дозволяє гарантувати, що тільки уповноважені особи можуть отримувати доступ до конфіденційної інформації.

Крім того, хмарні сервіси забезпечують моніторинг і запис усіх дій із даними, створюючи аудит-треки. Це допомагає виявляти та запобігати підозрілим діям, підвищуючи прозорість та відповідність регуляторним вимогам, таким як GDPR або HIPAA.

Завдяки цим можливостям хмарні технології є ефективним інструментом захисту персональних даних пацієнтів, забезпечуючи їхню конфіденційність, доступність та цілісність, що є критично важливим у сфері

охорони здоров’я.

Основними напрямками використання хмарних технологій для захисту персональних даних пацієнтів є такі:

1. Децентралізоване зберігання даних: хмарні платформи дозволяють зберігати дані пацієнтів у захищеному віртуальному середовищі, яке мінімізує ризик втрати або крадіжки інформації. Це забезпечується за допомогою резервного копіювання та розподіленого зберігання на кількох серверах.

2. Шифрування даних: використання хмарних сервісів включає застосування сучасних алгоритмів шифрування для забезпечення конфіденційності персональних даних як у процесі їх передачі, так і під час зберігання.

3. Контроль доступу: хмарні технології забезпечують можливість налаштування рівнів доступу до інформації, дозволяючи медичним закладам надавати доступ лише уповноваженим особам і контролювати, хто і коли взаємодіє з даними.

4. Аудит і моніторинг: хмарні сервіси створюють журнал дій (аудит-треки), що дозволяє відслідковувати будь-які зміни або доступ до персональних даних, забезпечуючи прозорість і можливість виявлення порушень.

5. Захист від кібератак: хмарні провайдери впроваджують багаторівневі механізми захисту, такі як міжмережеві екрани, системи виявлення загроз і оновлення програмного забезпечення для запобігання вторгненням та витокам даних.

6. Резервне копіювання та відновлення: хмарні технології забезпечують регулярне створення резервних копій даних і можливість їх оперативного відновлення у разі втрати через технічні збої, помилки або кібератаки.

7. Дотримання регуляторних вимог: хмарні платформи сприяють відповідності нормативним актам (GDPR, HIPAA тощо) шляхом забезпечення необхідного рівня захисту персональних даних і прозорості їх

обробки.

Ці напрямки забезпечують надійний захист персональних даних пацієнтів, підвищуючи рівень довіри до медичних закладів і сприяючи розвитку цифрових технологій у сфері охорони здоров'я.

Використання хмарних технологій для децентралізованого зберігання персональних даних пацієнтів полягає у створенні інфраструктури, яка дозволяє зберігати дані у віртуальному середовищі, розподіленому між кількома серверами. Цей підхід забезпечує підвищений рівень безпеки, доступності та ефективності обробки інформації. Основні аспекти такого використання включають:

1. Розподілене зберігання: дані пацієнтів розподіляються на кілька серверів або центрів обробки даних, що знаходяться в різних географічних точках. Це знижує ризик втрати інформації через технічні збої, стихійні лиха або кібератаки.

2. Географічну реплікацію: хмарні сервіси використовують географічну реплікацію даних, яка дозволяє створювати дублікати інформації в різних регіонах. Це забезпечує стійкість системи до відмов і зменшує ризик одночасної втрати всіх копій.

3. Масштабованість: хмарні платформи можуть легко адаптуватися до збільшення обсягу даних, що є важливим у міру зростання кількості пацієнтів або введення нових типів даних, таких як результати обстежень чи історії хвороб.

Загалом, децентралізоване зберігання в хмарі персональних даних пацієнтів забезпечує надійний, економічно ефективний і безпечний спосіб управління ними, сприяючи підвищенню рівня довіри до медичних закладів.

Використання хмарних технологій для шифрування персональних даних пацієнтів забезпечує високий рівень захисту інформації завдяки впровадженню передових методів шифрування, інтегрованих у хмарну інфраструктуру. Цей підхід дозволяє захищати чутливу медичну інформацію від несанкціонованого доступу як під час зберігання, так і при передачі. Основні аспекти такого використання включають:

1. Шифрування під час зберігання (data-at-rest encryption): усі персональні дані пацієнтів, що зберігаються в хмарі, шифруються за допомогою сучасних криптографічних алгоритмів, таких як AES (Advanced Encryption Standard). Це гарантує, що навіть у разі несанкціонованого доступу до фізичних носіїв даних, інформація залишиться недоступною для зловмисників.

2. Шифрування під час передачі (data-in-transit encryption): дані пацієнтів, які передаються між клієнтським пристроєм і хмарною платформою, шифруються за допомогою протоколів безпеки, таких як TLS (Transport Layer Security). Це запобігає можливості їх перехоплення під час передачі через мережу.

3. Ключове управління (Key Management): хмарні провайдери надають сервіси для зберігання, управління та використання криптографічних ключів. Деякі рішення дозволяють медичним закладам самостійно управляти ключами, що додає додатковий рівень контролю над безпекою даних.

4. Гібридне шифрування: використання одночасно симетричних та асиметричних методів шифрування. Симетричне шифрування використовується для забезпечення швидкості, а асиметричне – для передачі ключів і підвищення безпеки.

5. Розширене шифрування (end-to-end encryption): у деяких хмарних платформах забезпечується наскрізне шифрування, коли дані шифруються на пристрої користувача перед передачею до хмари і розшифровуються лише на пристрої, уповноваженому для доступу.

6. Шифрування специфічних типів даних: хмарні технології дозволяють шифрувати окремі поля бази даних (наприклад, імена, дати народження, медичні історії), що забезпечує більшу гнучкість і безпеку при роботі з великими обсягами інформації.

Загалом, шифрування в хмарних технологіях створює багаторівневий захист персональних даних пацієнтів, що дозволяє медичним закладам дотримуватися нормативних вимог і захищати конфіденційну інформацію від зловмисників.

Хмарні технології забезпечують ефективний захист від кібератак на персональні дані пацієнтів завдяки комплексному підходу до безпеки, який включає передові методи захисту, моніторинг і управління ризиками. Основні аспекти їх використання для цього включають:

1. Інтеграцію передових засобів кіберзахисту: хмарні провайдери впроваджують сучасні інструменти безпеки, такі як системи виявлення та запобігання вторгненням (IDS/IPS), фаєрволи веб-додатків (WAF), захист від розподілених атак типу «відмова в обслуговуванні» (DDoS), що знижують ризик кібератак на персональні дані.

2. Шифрування даних: дані пацієнтів, які зберігаються в хмарі або передаються через мережу, шифруються за допомогою сильних алгоритмів шифрування, таких як AES-256. Це унеможливлює доступ до даних навіть у разі їх перехоплення.

3. Мультирівневу автентифікацію: для доступу до систем і даних використовуються методи багатофакторної автентифікації (MFA), що значно ускладнює зловмисникам можливість проникнення.

4. Моніторинг та аналіз безпеки в реальному часі: хмарні платформи використовують автоматизовані інструменти для аналізу аномальної активності, що може свідчити про потенційну атаку. Системи машинного навчання допомагають виявляти загрози на ранніх стадіях.

5. Безперервне оновлення та патчинг: хмарні провайдери забезпечують регулярне оновлення програмного забезпечення, включаючи виправлення вразливостей, що знижує ризик експлуатації вразливих місць хакерами.

6. Контроль доступу: хмарні технології дозволяють встановлювати гнучкі політики доступу на основі ролей і привілеїв, зменшуючи ризик витоку даних через внутрішні загрози.

7. Резервне копіювання та відновлення даних: хмарні рішення включають автоматичне створення резервних копій і механізми швидкого відновлення даних після атак, таких як програмне забезпечення-вимагач.

8. Сегментацію даних і мереж: розділення зберігання та обробки

даних пацієнтів на різні середовища та сегменти унеможливлює доступ до всіх даних у разі атаки.

9. Дотримання стандартів безпеки: хмарні провайдери відповідають міжнародним стандартам безпеки (наприклад, ISO 27001, HIPAA), що гарантує дотримання найкращих практик у сфері захисту даних.

10. Інтеграцію з інструментами управління інцидентами: у разі атаки хмарні системи дозволяють оперативно реагувати та ізолювати загрози, зменшуючи можливий збиток.

Використання хмарних технологій для захисту від кібератак на персональні дані пацієнтів створює безпечне середовище, яке дозволяє медичним закладам зосередитися на основній діяльності, мінімізуючи ризики витоку чи компрометації конфіденційної інформації.

Отже, хмарні технології забезпечують надійний захист персональних даних пацієнтів завдяки своїй гнучкості та безпечності. Дані зберігаються в захищених центрах обробки інформації, які використовують передові методи шифрування для запобігання доступу сторонніх осіб. Завдяки багаторівневій автентифікації та постійному моніторингу загроз, система здатна виявляти й усувати потенційні кібератаки в реальному часі. Хмарні провайдери регулярно оновлюють свої системи, що дозволяє закладам охорони здоров’я бути захищеними від нових загроз. Крім того, завдяки автоматичному резервному копіюванню дані можна швидко відновити у разі збоїв чи атак. Хмарні технології дозволяють зручно організувати доступ до інформації, зберігаючи при цьому її конфіденційність і цілісність.