**Міністерство освіти і науки України**
**Національний технічний університет**
**«Дніпровська політехніка»**

**Інститут електроенергетики**
**Факультет інформаційних технологій**
**Кафедра безпеки інформації та телекомунікацій**

# ПОЯСНЮВАЛЬНА ЗАПИСКА
## кваліфікаційної роботи ступеня магістра

**студента** *Донченка Іллі Вікторовича*

**академічної групи** *125м-19-1*

**спеціальності** ***125 Кібербезпека***

**спеціалізації**[1]

**за освітньо-професійною програмою** ***Кібербезпека***

**на тему** *Методика реєстрації дій над інформацією, яка потребує захисту в медичних інформаційних системах*

| Керівники | Прізвище, ініціали | Оцінка за шкалою | | Підпис |
|---|---|---|---|---|
| | | рейтинговою | інституційною | |
| кваліфікаційної роботи | професор Корнієнко В. І. | | | |
| розділів: | | | | |
| спеціальний | ст. викладач Кручінін О. В. | | | |
| економічний | к.е.н, доцент Пілова Д. П. | | | |

| | | | | |
|---|---|---|---|---|
| **Рецензент** | Федоренко Д. А. | | | |

| | | | | |
|---|---|---|---|---|
| **Нормоконтролер** | ст. викладач Тимофєєв Д. С. | | | |

**Дніпро**
**2020**

**ЗАТВЕРДЖЕНО:**
завідувач кафедри
безпеки інформації та телекомунікацій
_____ д.т.н., проф. Корнієнко В.І.

«_____»_____20___року

# ЗАВДАННЯ
## на кваліфікаційну роботу ступеня магістра

**студенту** **Донченку Іллі Вікторовичу** **академічної групи** **125м-19-1**
(прізвище та ініціали) (шифр)

**спеціальності** ***125 Кібербезпека***

**спеціалізації**

**за освітньо-професійною програмою** ***Кібербезпека***

**на тему** ***Методика реєстрації дій над інформацією, що потребує захисту в медичних інформаційних системах***

Затверджену наказом ректора НТУ «Дніпровська політехніка» від 22.10.20 № 888-с

| **Розділ** | **Зміст** | **Термін виконання** |
|---|---|---|
| Стан питання. постановка задачі | Виконати аналіз нормативної та законодавчої баз щодо ведення медичної документації. Проаналізувати стан захисту інформації в МІС. | 26.10.2020 - 30.10.2020 |
| Спеціальна частина | Сформулювати та формалізувати вимоги щодо розробки методики реєстрації дій користувача. Обґрунтувати методи та засоби реалізації методики. | 02.11.2020 - 13.11.2020 |
| Економічна частина | Довести економічну ефективність впровадження запропонованого рішення | 16.11.2020 - 27.11.2020 |

Завдання видано _____ Кручінін О.В.
(підпис керівника) (прізвище, ініціали)

Дата видачі завдання: 01.09.20

Дата подання до екзаменаційної комісії: 09.12.20

Прийнято до виконання _____ Донченко І. В.
(підпис студента) (прізвище, ініціали)

# РЕФЕРАТ

Пояснювальна записка: 91 с., 18 рис., 4 табл., 5 додатків, 21 джерел

Об’єкт досліджень: комплекс засобів захисту медичних інформаційних систем.

Мета роботи: забезпечення контролю за діями користувачів в медичних інформаційних системах.

У першому розділі виконувався аналіз стану захищеності інформації в галузі охорони здоров’я України, відповідності ведення електронних медичних документів нормам існуючого законодавства та існуючої Електронної системи охорони здоров’я ЕСОЗ («eHealth»)

У другій частині були розглянуті послуги безпеки, що забезпечені в системі захисту функціонуючій медичній інформаційній системі, досліджені можливі вразливості та запропонована методи та засоби реалізації послуг.

В економічній частині проведений розрахунок капітальних витрат при розробці журналу, а також доведена доцільність цього рішення с точки зору економічної ефективності.

Практичне значення роботи полягає у запропоновані розробки журналу реєстрації, який може бути використаний для подальшого вдосконалення.

Наукова новизна полягає в застосуванні протоколу колективного підпису, для аутентифікації автора в медичних інформаційних системах

РЕЄСТРАЦІЯ ДІЇ НАД ІНФОРМАЦІЄЮ, ЕЛЕКТРОНА МЕДИЧНА ІНФОРМАЦІЙНА СИСТЕМА, ПРОТОКОЛЮВАННЯ, ПОСЛУГИ БЕЗПЕКИ В МЕДИЧНІЙ ІНФОРМАЦІЙНІЙ СИСТЕМІ

# THE ABSTRACT

Explanatory note: 91 pp., 18 fig., 4 tab., 5 appendices, 21 sources

Object of research: a set of means of protection of medical information systems.

The purpose of the thesis: ensuring control over the actions of users in medical information systems.

The first section analyzes the state of information security in the field of health care in Ukraine, the compliance of electronic medical records with existing legislation and the existing Electronic Health System EHEalth ("eHealth").

In the second part, the security services provided in the protection system of the functioning medical information system were considered, possible vulnerabilities were investigated and a model of the log of user actions was proposed.

In the economic part, the calculation of capital costs in the development of the journal, as well as proved the feasibility of this solution in terms of economic efficiency.

The practical significance of the work lies in the proposed development of a logbook that can be used for further improvement.

The scientific novelty lies in the use of the collective signature protocol for author authentication in medical information systems.

REGISTRATION OF ACTION ON INFORMATION, ELECTRONIC MEDICAL INFORMATION SYSTEM, PROTOCOLING, SECURITY SERVICES IN MEDICAL INFORMATION

# РЕФЕРАТ

Пояснительная записка: 91 с., 18 рис., 4 табл., 5 приложений, 21 источников

Объект исследований: комплекс средств защиты медицинских информационных систем.

Цель работы: обеспечение контроля за действиями пользователей в медицинских информационных системах.

В первом разделе выполнялся анализ защищенности информации в области здравоохранения Украины, соответствия ведения электронных медицинских документов нормам существующего законодательства и существующей Электронной системы здравоохранения ЕСОЗ ( «eHealth»)

Во второй части были рассмотрены услуги безопасности, обеспечены в системе защиты функционирующей медицинской информационной системе, исследованы возможные уязвимости и предложена методы и средства реализации услуг.

В экономической части произведен расчет капитальных затрат при разработке журнала, а также доказана целесообразность этого решения с точки зрения экономической эффективности.

Практическое значение работы состоит в предложенные разработки журнала регистрации, который может быть использован для дальнейшего совершенствования.

Научная новизна заключается в применении протокола коллективного подписи для аутентификации автора в медицинских информационных системах

РЕГИСТРАЦИЯ ДЕЙСТВИЯ НАД ИНФОРМАЦИЕЙ, ЭЛЕКТРОННАЯ МЕДИЦИНСКАЯ ИНФОРМАЦИОННАЯ СИСТЕМА, ПРОТОКОЛИРОВАНИЕ, УСЛУГИ БЕЗОПАСНОСТИ В МЕДИЦИНСКОЙ ИНФОРМАЦИОННОЙ СИСТЕМЕ

## СПИСОК УМОВНИХ СКОРОЧЕНЬ

**API** – Application Programming Interface;

**HIS** – Hospital Information System;

**RSA** – Rivest, Shamir, Adleman;

**USB** – Universal Serial Bus;

**АРМ** –Автоматизоване робоче місце;

**АС** – Автоматизированная система**;**

**АЦСК** – Акредитований центром сертифікації ключ;

**БД** – База даних;

**ДП** – Державне підприємство;

**ДССЗЗІ** – Державна служба спеціального зв'язку та захисту інформації;

**ЕД** – Електронні дані;

**ЕКП** – Електронна картка пацієнта;

**ЕМЗ** – Електронні медичні записи;

**ЕСОЗ** – Електронна система охорони здоров'я;

**ЗУ** – Закон України;

**ІВК** – Інфраструктури відкритого ключа;

**КЕП** – Кваліфікований електронний підпис;

**КЕЦП** – Колективний електронний цифровий підпис;

**ККУ** – Кримінальний Кодекс України;

**КЦД** – Конфиденциальность, Целостность, Доступность;

**МІС** – Медична інформаційна система;

**МОЗ** – Міністерство охорони здоров'я;

**НСЗУ** – Національна Служба Здоров'я України;

**СВК** – Сртифікат відкритого ключа;

**США** – Сполучені Штати Америки;

**ЦБД** – Центральна база даних;

ЗМІСТ

# ВСТУП

У 2018 р аналітичний центр компанії InfoWatch зареєстрував 429 витоків з різних установ медичної сфери з усього світу: лікарні, поліклініки, військові госпіталі, лабораторії, аптеки, медичне страхування і т.д. Це майже на 16% більше, ніж в 2017 р Число скомпрометованих записів персональних даних в порівнянні з 2017 р зросла майже вдвічі і склало 27 млн. Понад 80% записів ПДН утекло в результаті зовнішнього впливу. Кожен третій витік в минулому році відбувся в результаті хакерських атак. Але основними винуватцями витоків в даній галузі залишаються співробітники. На їх частку припадає 53,7% зареєстрованих інцидентів. Співвідношення умисних і випадкових витоків в медицині склало 47,5% і 52,5%. При цьому серед витоків, скоєних з вини співробітників, частка умисних інцидентів становить трохи більше 20%. В основному дані обмеженого доступу компрометуються в результаті помилок, недогляду, недбалості. Більше 45% витоків в 2018 р трапилися через мережевий канал. Далі в рейтингу розташовуються електронна пошта (21,1%) і паперові документи (20,2%) [1].

# 1. СТАН ПИТАННЯ. ПОСТАНОВКА ЗАДАЧІ

## 1.1. Аналіз нормативної та законодавчої бази захисту інформації в сфері охорони здоров'я

Розвиток теорії інформаційних правовідносин ґрунтується на принциповому розмежуванні типів останніх. Інформаційні правовідносини безпосередньо пов'язані з формуванням, створенням, перетворенням та використанням інформації, зберіганням інформації, передачею і розповсюдженням інформації та ін.» [2]

### 1.1.1. Класифікація інформації в сфері охорони здоров'я

В системі охорони здоров'я використовуються наступні види інформації, що поділяються відповідно її призначення

По-перше, це інформація, пов'язана з процесом організації надання медичної допомоги:

Публічно-правова:

- інформація, пов'язана з проходженням акредитації закладу охорони здоров'я;
- інформація, необхідна для отримання ліцензії на провадження господарської діяльності з медичної практики;
- інформація, пов'язана з провадженням ліцензійної діяльності
- інформація, пов'язана із (внутрішнім та зовнішнім) контролем якості медичної допомоги та медичного обслуговування;
- інформація щодо наявних у закладі охорони здоров'я лікарських засобів, витратних матеріалів, медичних виробів та харчових продуктів для спеціального дієтичного споживання;

Приватноправова складова інформації:

- інформація про кваліфікацію медичного працівника, наявність у нього відповідного сертифікату;

– інформація, яка міститься в електронній системі охорони здоров'я (приміром, реєстр пацієнтів, живих донорів);

По-друге, це інформація, пов'язана з наданням медичної допомоги:

– медична інформація (медичні відомості/дані);
– інформація немедичного характеру, тісно пов'язана із медичними відомостями/даними;
– інформація, пов'язана приватним і сімейним життям[3];

### 1.1.2. Основні положення нормативної та законодавчої бази щодо захисту інформації в сфері охорони здоров'я

Збереження лікарської таємниці регулюються наступними законодавчими актами України:

– конституція України (далі — Конституція);
– цивільний кодекс України (ЦК);
– кримінальний кодекс України (КК);
– закон України «Основи законодавства України про охорону здоров'я» від 19.11.1992 № 2801-XII (далі — Основи);
– закон України «Про інформацію» від 02.10.1992 № 2657-XII (далі — Закон про інформацію).
– закон України «Про захист персональних даних» від 01.06.2010 № 2297-VI (далі — Закон про персональні дані).
– стаття 32 Конституції визначає, що ніхто не може зазнавати втручання в його особисте і сімейне життя.

Законодавством України захищається право кожної фізичної особи на таємницю про стан свого здоров'я, факт звернення по медичну допомогу, діагноз, а також про відомості, одержані під час медичного обстеження, забороняється вимагати та подавати за місцем роботи або навчання інформацію про діагноз і методи лікування фізичної особи (ст. 286 ЦК).

Окрім цього в системі охорони здоров'я України існує інформація з обмеженим доступом, до якої належить конфіденційна, таємна та службова інформація.

Конфіденційною є інформація про фізичну особу, а також інформація, доступ до якої обмежено фізичною або юридичною особою, крім суб'єктів владних повноважень. Конфіденційну інформацію можна поширювати за бажанням (згодою) відповідної особи у визначеному нею порядку відповідно до передбачених нею умов, а також в інших випадках, визначених законом (ст. 21 Закону про інформацію).

Поза тим, законодавство містить поняття лікарської таємниці, під якою розуміють відомості, отримані під час виконання професійних обов'язків посадовими особами та медичними працівниками закладів охорони здоров'я.

Зокрема, це інформація:

- про факт звернення по медичну допомогу;
- про діагноз;
- про хворобу;
- про медичне обстеження, огляд та їх результати;
- про інтимну й сімейну сторони життя громадянина;
- про будь-які інші відомості, одержані під час медичного обстеження (ч. 1 ст. 40 Основ і ст. 286 ЦК).

Показовим є Рішення Конституційного Суду України у справі щодо офіційного тлумачення статей 3, 23, 31, 47, 48 Закону України «Про інформацію» та статті 12 Закону України «Про прокуратуру» (справа К. Г. Устименка) від 30.10.1997 № 5-зп (далі — Рішення КСУ). Згідно із цим Рішенням, до конфіденційної, тобто інформації з обмеженим доступом, за своїм правовим режимом належить така медична інформація:

- свідчення про стан здоров'я людини;
- історія хвороби;
- відомості про мету запропонованих досліджень і лікувальних заходів;

– прогноз можливого розвитку захворювання, зокрема й про наявність ризику для життя та здоров’я людини.

Оскільки інформація про пацієнта є конфіденційною, медичним працівникам заборонено розголошувати її третім особам. Надавати такі відомості можна виключно у випадках, передбачених законами України, наприклад ч. 2 ст. 26 Закону України «Про захист населення від інфекційних хвороб» від 06.04.2000 № 1645-III.

## 1.2. Аналіз стану безпеки інформації в Електронній системи охорони здоров’я України

У серпні 2014 року Міністерство охорони здоров’я ініціювало розробку Національнї стратегії реформування системи охорони здоров’я в Україні. За допомогою нових стратегічних підходів до підвищення якості та доступності допомоги та зменшення фінансових ризиків для людей потрібно було надати нового поштовху реформі галузі [4].

На основі Концепції реформи фінансування системи охорони здоров'я Верховна Рада 19 жовтня 2017 року прийняла Закон «Про державні фінансові гарантії медичного обслуговування населення», який набрав чинності 30 січня 2018 року. За один із ключових елементів реформи фінансування системи охорони здоров'я відповідає новий орган — Національна служба здоров'я України. Національна служба здоров’я України (НСЗУ) — центральний орган виконавчої влади, що реалізовуватиме державну політику у сфері державних фінансових гарантії медичного обслуговування населення. НСЗУ — це національний страховик, який укладає договори із закладами охорони здоров’я та закуповує у них послуги з медичного обслуговування населення. Для того, аби почати співпрацювати за договором з НСЗУ, медичний заклад повинен приєднатися до Електронної системи охорони здоров’я та забезпечити подання даних до електронної системи охорони здоров'я на постійній основі.

Норми комплексної системи захисту інформації - лише частина політики безпеки eHealth. Архітектура системи пройшла міжнародну експертизу і

побудована таким чином, щоб виключити варіант найменшої маніпуляції. eHealth - одна з небагатьох систем в Україні, в якій реалізовані найсучасніші засоби захисту, серед яких: використання користувачами кваліфікованих електронних підписів (КЕП), відокремлене зберігання медичних та персональних даних, алгоритми, що забезпечують цілісність даних та інші.

Центральна база даних eHealth знаходиться в захищеному датацентрі в м. Києві, який також має комплексну систему захисту інформації з підтвердженою відповідністю.

В основу архітектури системи покладений принцип орієнтованості на пацієнта. Тобто дані накопичуються навколо єдиного облікового запису пацієнта. Згодом пацієнт зможе самостійно керувати доступом до таких даних.

За замовчуванням, доступ до медичних даних пацієнта матиме лікар первинної ланки, з яким пацієнт підписав декларацію. Лікарі-спеціалісти матимуть змогу отримати доступ до окремих епізодів медичної допомоги лише за направленням його лікаря первинної ланки. В подальшому в системі буде реалізований функціонал, що дозволятиме пацієнту самостійно керувати доступами до власних даних через електронні кабінети пацієнтів, які можуть бути реалізовані в тому числі у мобільних пристроях.

Медичні дані, що зберігатимуться в електронній системі охорони здоров'я, є більш захищеними, у порівнянні з існуючими картками пацієнтів на паперових носіях в закладах охорони здоров'я.

Раніше була проведена величезна робота з побудови систем захисту даних. Важливими її етапами були експертні дослідження та отримання експертних висновків про відповідність програмного забезпечення центральної бази даних, засобів криптографічного захисту, розробка та затвердження разом з ДССЗЗІ вимог до електронних медичних інформаційних систем.

Попереду ще багато роботи у напрямку захисту інформації, адже норми комплексної системи захисту інформації - це лише частина політики безпеки, яка активно розвивається та оновлюється відповідно до появи нових можливих загроз у сфері кібербезпеки [5].

### 1.2.1. Призначення Електронної системи охорони здоров'я

Електронна система охорони здоров'я (eHealth, ЕСОЗ) забезпечує обмін медичною інформацією та реалізацію програми медичних гарантій населення. ЕСОЗ — інформаційно-телекомунікаційна система, яка забезпечує автоматизацію ведення обліку медичних послуг та управління медичною інформацією шляхом створення, розміщення, оприлюднення та обміну інформацією даними і документами в електронному вигляді. Розробка системи та підтримка системи відбувається спеціально створеним державним підприємством «Електроне Здоров'я» («eZdorovya), яке керує процесом створення та впровадження електронних медичних систем. Фінансування відбувається як зі сторони держави, так і міжнародними організаціями. Завдання ЕСОЗ – забезпечити можливості використання пацієнтами електронних сервісів для реалізації їх прав за програмою державних гарантій медичного обслуговування населення, автоматизація ведення обліку медичних послуг і управління медичною інформацією, запровадження електронного документообігу у сфері медичного обслуговування населення за програмою медичних гарантій.

Інформатизація охорони здоров'я відбувається швидкими темпами. Протягом останніх 15 років для підтримки розвитку медичної інформатики Євросоюзом було виділено 500 млн євро. Нині ця індустрія виходить на третє місце за фінансуванням у системі охорони здоров'я (загальний обіг – 11 млрд євро). У країнах Західної та Північної Європи електронна картка пацієнта (ЕКП) вже на 50–90% замінила паперовий варіант документації, а в США — на 70%. Економія часу, який витрачає медичний персонал на ведення документації в електронному вигляді, становить 63,4% [6]

Провідні світові аналітики очікують, що зростаючий попит на цифровизацию національних систем охорони здоров'я поряд з технологічними досягненнями в області інформаційних технологій для охорони здоров'я стане ключовим фактором, який сприяє зростанню ринку. Крім того, урядові ініціативи, що стимулюють перехід на електронне охорону здоров'я, швидше за все, посилять

попит на електронні системи ведення медичної документації. Очікується, що до 2025 року обсяг глобального ринку МІС зросте до 33-38 млрд. доларів США. МІС пропонують ряд переваг для медичних працівників і пацієнтів, що в кінцевому підсумку збільшує продуктивність системи охорони здоров'я і задоволеність пацієнтів. Очікується, що подальший розвиток інформаційних технологій, таких як інтелектуальний аналіз даних, систем підтримки прийняття лікарських рішень і штучного інтелекту, будуть стимулювати попит на МІС.

### 1.2.2. Узагальнена структурна схема Електронної системи охорони здоров'я

До складу ЕСОЗ входять Центральна База Даних та електронні медичні інформаційні системи, між якими забезпечено автоматичний обмін інформацією, даними та документами через відкритий програмний інтерфейс (API). Схема ЕСОЗ з позначенням місця кожного елементу системи та їх взаємозв'язки наведена на рис. 1.1.

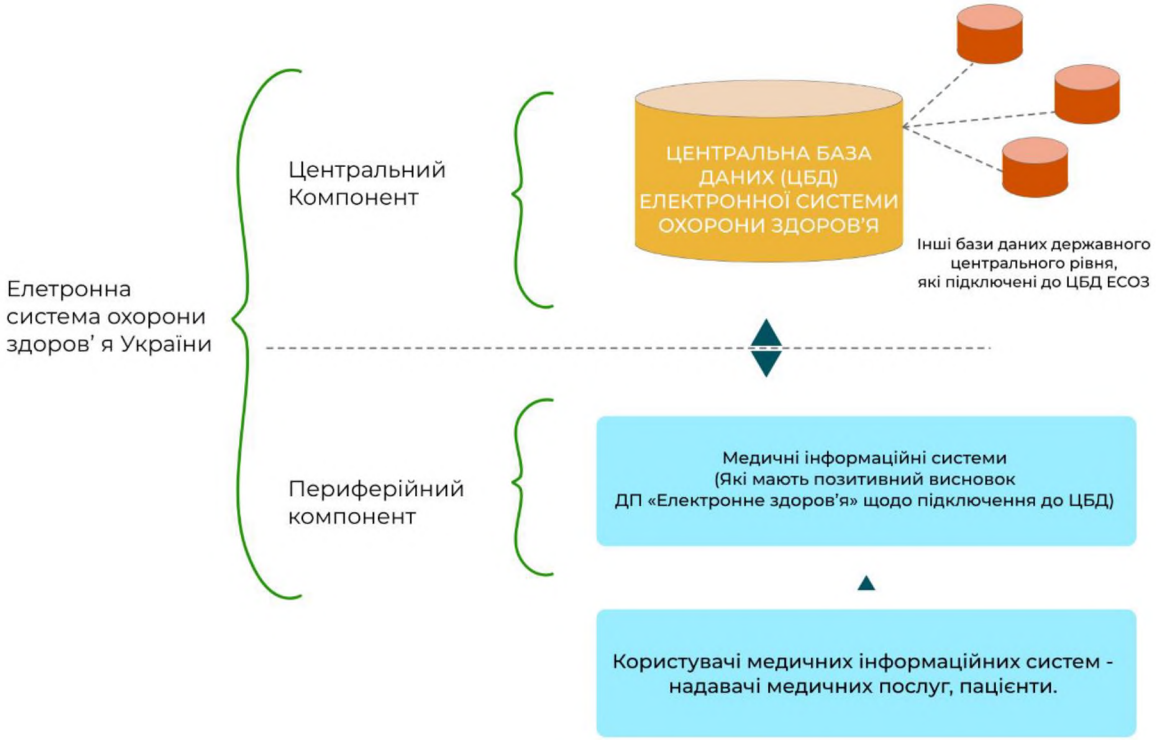


Рисунок 1.1 – Структурна схема взаємозв'язків елементів ЕСОЗ


Рисунок 1.2 – Управлінська ієрархія електронної системи охорони здоров'я

Система ЕСОЗ складається з:

– центральної бази даних — ЦБД (адміністратор ДП "Електронне здоров'я") – програмно-апаратний комплекс, який забезпечує можливість створення, перегляду, обміну інформацією та документами між реєстрами та електронними медичними інформаційними системами, а також модулями Національної служби здоров'я;
– електронних медичних інформаційних систем — МІС (системи, які дають змогу автоматизувати роботу медзакладів з ЦБД).

Рівень управління системою охорони здоров'я та універсального доступу до медичних даних пацієнта (ЦБД ЕСОЗ):

– ключові реєстри (реєстр пацієнтів, реєстр декларацій про вибір лікаря, реєстр суб'єктів господарювання, реєстр медичних спеціалістів, реєстр

медичних працівників, реєстр договорів про медичне обслуговування населення);

– електронні медичні записи (рецепти, направлення, медичні довідки, листки непрацездатності).

Рівень медичних інформаційних систем надавачів медичних послуг (периферійний компонент ЕСОЗ):

– автоматизація запису на прийом (електронна черга);
– електронні медичні записи та документи локального зберігання;
– управління лікарськими запасами та виробами медичного призначення;
– автоматизовані локальні системи управління ресурсами;
– облік платних послуг;
– лабораторія;
– кадровий облік.


Рисунок 1.3 –Структура ЕСОЗ

На рис. 1.4 можна побачити, що база даних ЕСОЗ стрімко розвивається, якщо у вересні 2019 року вона містила 13 тис. створених електронних медичних

записів (ЕМЗ), то у листопаді 2020 р. створено 17,6 млн ЕМЗ з накопичувальним підсумком 106 млн на 09 грудня 2020 р. [7]

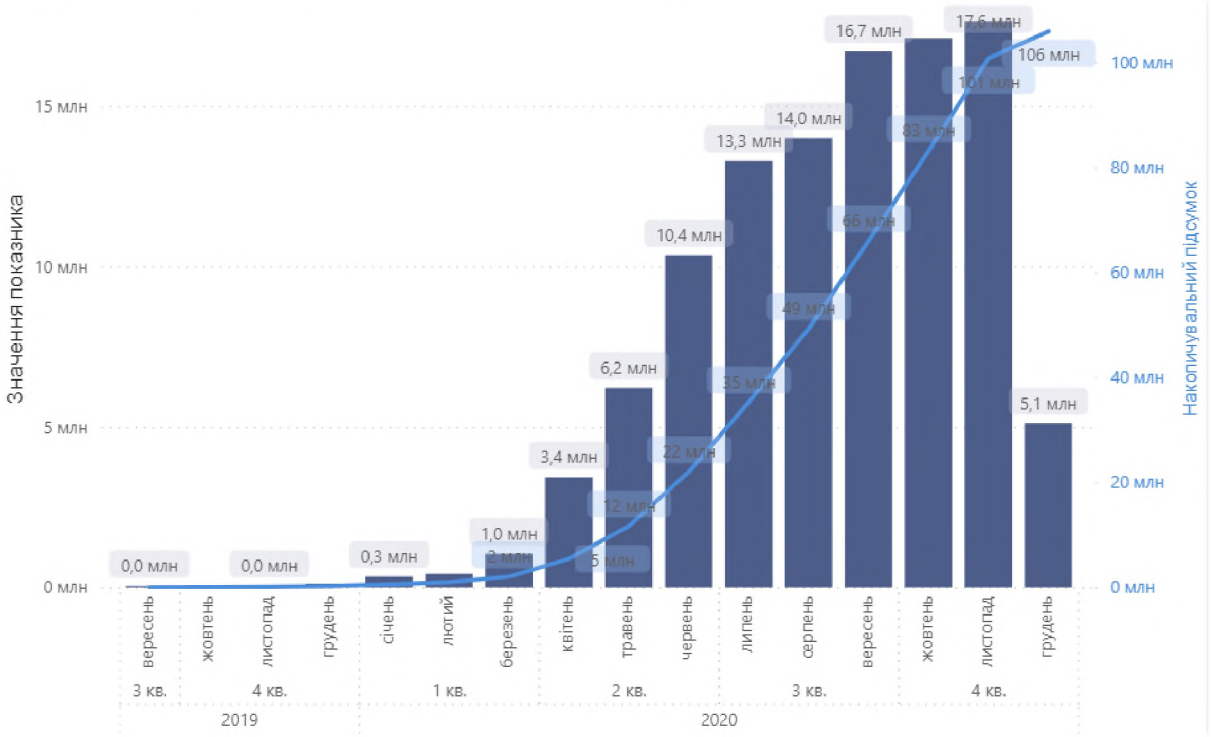


Рисунок 1.4 –Динаміка створених електронних медичних записів

МІС — це комплексний програмний продукт, місією якого є автоматизація всіх основних процесів, пов'язаних із роботою медичних установ всіх рівнів спеціалізації. МІС дозволяють швидко й ефективно налагодити електронний документообіг, гнучко вибудовувати роботу з пацієнтами, вести оперативний облік роботи адміністративного персоналу, контролювати всі організаційні і фінансові питання. За кордоном прийнято використовувати термін HIS (Hospital Information System) - госпітальна інформаційна система для комплексного управління всіма процесами медобслуговування, у тому числі юридичному аспекті. На рис. 1.5 зображена структурна схема ЕСОЗ.

Функціонування (ЕСОЗ) України регламентовано наступними законодавчими актами:

– закон України “Про державні фінансові гарантії медичного обслуговування населення”;
– постанова Кабінету Міністрів України №411 “Деякі питання електронної системи охорони здоров’я” від 25 квітня 2018 року;

– наказ МОЗ №503 “Про затвердження Порядку вибору лікаря, який надає первинну медичну допомогу, та форми декларації про вибір лікаря, який надає первинну медичну допомогу” від 19 березня 2018 року;
– наказ МОЗ №586 “Про затвердження Порядку направлення пацієнтів до закладів охорони здоров’я та фізичних осіб - підприємців, які в установленому законом порядку одержали ліцензію на провадження господарської діяльності з медичної практики та надають медичну допомогу відповідного виду” від 28 лютого 2020 року;
– наказ МОЗ №587 “Деякі питання ведення Реєстру медичних записів, записів про направлення та рецептів в електронній системі охорони здоров'я” від 28 лютого 2020 року.

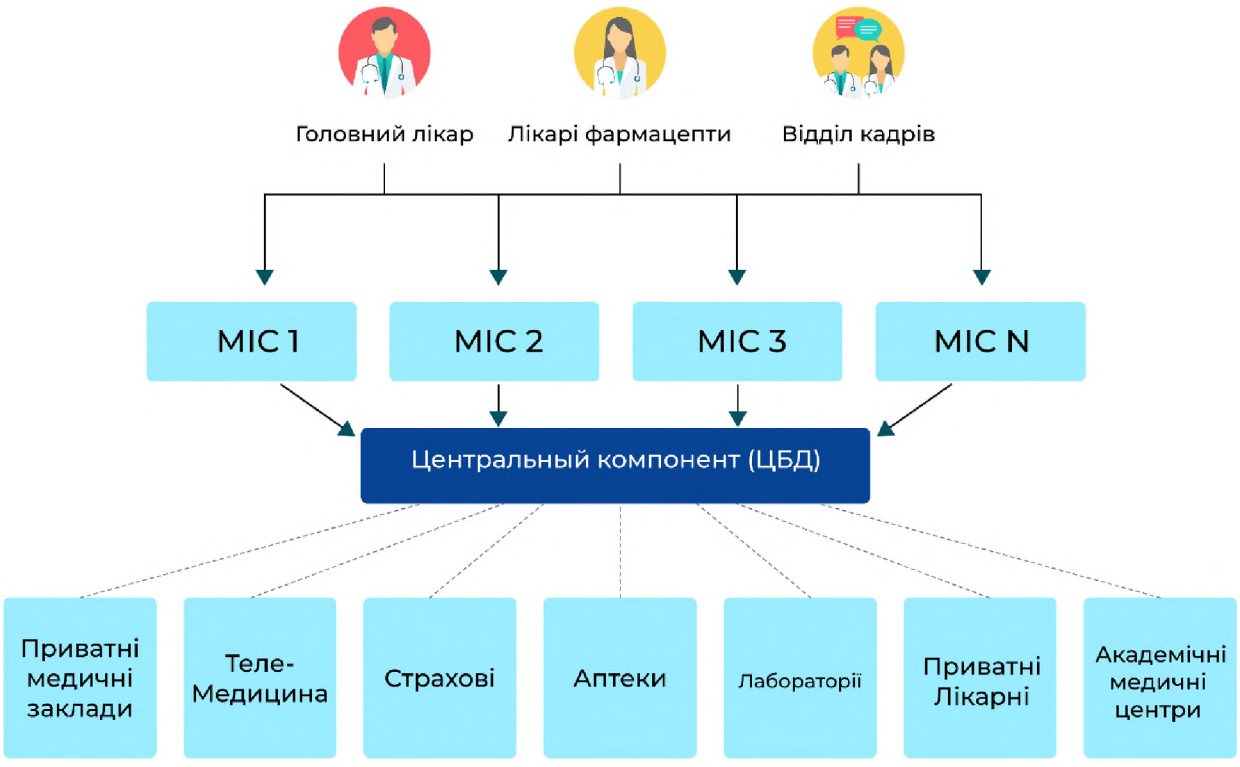


Рисунок 1.5 – Структурна схема ЕСОЗ

### 1.2.3. Класифікація Електронної системі охорони здоров'я

МІС є розподілений багатомашинний багатокористувачевий комплекс, який одночасно обробляє інформацію різних ступенів обмеження доступу, тому, згідно НД ТЗІ 2.5-005 -99, її тому слід відносити до класу 3 Стандартні функціональні профілі захищеності в КС, що входять до складу автоматизованих систем, які призначені для керування технологічними процесами. Основними загрозами для інформації оброблюваної в АС керування технологічними процесами є загрози порушення доступності АС і технології обробки інформації. В зв'язку з цим до КЗЗ ОС, що входять до складу таких АС, в першу чергу пред'являються вимоги до забезпечення доступності і адміністративного керування доступом щодо інформації з боку об'єктів процесів. В зазначених АС рекомендується використовувати операційні системи, КЗЗ яких реалізують профілі КЦД. х.

### 1.2.4. Аналіз вразливостей та механізмів захисту інформації в Електронній системі охорони здоров'я

НСЗУ регулярно здійснює заходи з верифікації даних, які містяться в електронній системі охорони здоров'я. Верифікація – це комплекс заходів з порівняння, встановлення відповідності та підтвердження відомостей, що містяться у центральній базі даних, з відомостями, що отримані від органів державної влади, з державних електронних інформаційних ресурсів, іншими даними.

На сьогодні НСЗУ використовує такі заходи з верифікації:

- деактивація даних про користувачів, які померли;
- робота з даними в системі відповідно до запитів її користувачів;
- опрацювання даних у системі відповідно до даних моніторингових досліджень.

Крім того, одним з механізмів верифікації даних, для забезпечення їх консистентності в системі, є заходи з дедублікації таких даних.

За результатами здійснення з моніторингу НСЗУ може прийняти рішення про вчинення відповідних заходів з верифікації даних у системі.

Перелік заходів з верифікації даних у системі не є вичерпним. На цей час триває процес з розроблення функціоналу для деактивації даних, створених у системі, під час його тестування, з помилками, з метою запобігання шахрайству (антифрод) тощо.

Зазначені заходи перебувають у процесі становлення та постійного удосконалення. Також покращуються моделі й інструменти, які використовуються для здійснення верифікації, тощо.

Також для здійснення заходів з верифікації триває робота щодо інтеграції системи з іншими державними реєстрами, що дасть можливість отримати дані з таких реєстрів.

Національна служба здоров'я України приділяє велику увагу точності та актуальності всіх даних в системі. Адже саме на їх основі ми здійснюємо оплати закладам за договором. І повинні бути впевненими в їхній достовірності [8].

Для роботи медичних закладів в ЕСОЗ їм необхідно до неї підключитися через приватну МІС, яку заклад обирає самостійно. Медзаклади можуть віддавати перевагу будь-якій МІС. Ринок МІС на сьогодні є конкурентним і передбачає велику кількість учасників.

Не всі наявні МІС мають підключення до ЕСОЗ. Системи, які успішно пройшли тестування та підключені до центральної бази даних ЕСОЗ, зазначені на сайті ЕСОЗ [9].

МІС складається з модулів та опцій до цих модулів. Кожен модуль має індивідуальну функціональність, адаптовану до діяльності конкретного медичного закладу. Забезпечення безпеки та конфіденційності даних є однією з головних вимог до існуючих МІС. Технічні вимоги до МІС затверджені наказом Національної служби здоров'я України від 30.09.2019 № 385. Розмежування доступу до інформації забезпечується шляхом ідентифікації користувачів. Допущені користувачі мають різні повноваження на доступ до інформаційних ресурсів. Але основною вразливістю захисту інформації в МІС є недоліки

механізмів розмежування доступу, що призводять до здійснення несанкціонованого доступу до захищеної інформації: несанкціоноване ознайомлення з інформацією, її розголошення та корекція, а також недостатня глибина реалізації вимог щодо автентифікації авторства документів.

Усі МІС підпорядковуються чинному законодавству, в свою чергу її розробники та власники відповідають за створення умов для безпечного збереження та обробки даних Користувачів. В свою чергу, на них покладається вирішення багатьох питань, зокрема додаткове розмежування доступу в залежності від потреб закладу, а також захист даних, що зберігаються у БД, як зазначалося вище. Додавання надмірних можливостей у межах МІС може не впливати на загальний функціонал спілкування с ЦБД, але поступове збільшення її обсягів може створювати нестабільні умови для працездатності та навіть утворювати вразливості та окремі ризики щодо реалізації загроз. Користувачі добре обізнані про те, що з себе уявляє ЦБД, де вона зберігається, ким контролюється та підтримується, якими законодавчими актами було затверджено її впровадження та порядок роботи, та які дані вона зберігає в собі. В свою чергу цю інформацію не надає розробник МІС у відкритий доступ. Користувачі можуть бути недостатньо інформовані про те, які дані зберігає МІС, якій обробці вони підлягають, кому надається доступ та хто та яким чином може отримати дані [10].

Таким чином, актуальними вразливостями МІС є загрози порушення доступності автоматизованої системи і технології обробки інформації.

## 1.3. Аналіз системи ведення медичної документації

Аналіз системи ведення медичної документації є складової клініко-експертної оцінки якості надання медичної допомоги та медичного обслуговування шляхом експертизи первинної облікової документації, клінічних питань профілактики, діагностики, медичного лікування та реабілітації, наявності відповідної кваліфікації спеціалістів за напрямом надання медичної допомоги та медичного обслуговування відповідно до вимог клінічних протоколів надання медичної допомоги, нормативно-правових актів у сфері охорони здоров'я [11].

### 1.3.1. Загальні відомості про систему медичної документації

Медична документація — система документів, встановленої (затвердженої спеціальним державним органом або самою медичною установою) форми, призначених для запису даних, підтвердження певних фактів, які виникають у процесі надання медичної послуги. В закладах охорони здоров'я України Медична документація використовується як обліково-звітна, так і первинна. В первинній медичній документації фіксують усі етапи лікувально-діагностичного процесу: стан хворого, дії медичного персоналу, використані технології і матеріали тощо. Коректне ведення медичної документації входить у посадові обов'язки медичних працівників. Згідно Номенклатури справ кожен вид медичної документації має відповідний строк зберігання.

Для виконання аналізу в роботі розглянуто ведення в МІС «Медичної картки стаціонарного хворого», тобто. внесення в базу даних відомостей про випадок госпіталізації хворого. «Медичної картки стаціонарного хворого» - форма 003/о первинної медичної документації. Форма 003/о та інструкція щодо її заповнення затверджена наказом Міністерства охорони здоров’я України від 14.02.2012 № 110. Форма № 003/о є основним медичним документом, що заповнюється на кожного хворого, який отримує медичну послугу в умовах стаціонару лікарні та ведеться в усіх закладах охорони здоров’я, які надають стаціонарну допомогу. Форма № 003/о містить всі дані щодо стану хворого протягом усього епізоду, а також дані об’єктивних, інструментальних, апаратних, лабораторних та інших методів обстежень. За допомогою зазначеної форми здійснюється контроль належної організації лікувально-діагностичного процесу та використовується для надання матеріалів за запитами (правоохоронних органів, суду тощо).

### 1.3.2. Структура та вимоги до медичної картки хворого

Умовно «Медичну картку стаціонарного хворого» можна розділити на такі частини:

- відомості ідентифікації пацієнта (паспортні дані, дані про близьких родичів, дата та час госпіталізації та виписки, тривалість перебування в умовах стаціонару, відділення госпіталізації, діагноз при госпіталізації, особливі відмітки, тощо);
- відомості про діагноз та методи його підтвердження (скарги, анамнез, локальний та загальний статуси, призначені обстеження, діагноз, призначене лікування, тощо);
- відомості про проведене обстеження, лікування, його результати (хронологія обстеження та лікування, застосовані методи, лікарські засоби та вироби медичного призначення, дози препаратів, час їх застосування, відомості про медичний персонал, що приймав участь в епізоді надання медичної послуги, тощо).

Наведемо деякі окремі вимоги у веденні паперового варіанту зазначеної медичної документації:

- у підпункті 22.2 «Медичної картки стаціонарного хворого» лікар зазначає дату запису (число, місяць, рік), свої прізвище, ім'я, по батькові, підпис та реєстраційний номер облікової картки платника податків або серію та номер паспорта (для фізичних осіб, які через свої релігійні переконання відмовляються від прийняття реєстраційного номера облікової картки платника податків та повідомили про це відповідний контролюючий орган і мають відмітку в паспорті);
- у пунктах 10-30 всі записи здійснює лікуючий лікар. Після цього у пункті 31 він зазначає свої прізвище, ім'я, по батькові, підпис і реєстраційний номер;
- у пункті 32 завідувач відділення зазначає свої прізвище, ім'я, по батькові, підпис та реєстраційний номер;
- у пункті 40 лікар приймального відділення проставляє свої прізвище, ім'я, по батькові, підпис та реєстраційний номер;

- у пункті 43 лікар здійснює записи про стан здоров'я та медичного лікування хворого або щогодини, або щодня, або щотижня залежно від стану хворого та місця його перебування Записи щоденника засвідчуються підписом лікуючого лікаря;
- у період перебування хворого в стаціонарі форма № 003/о зберігається у лікуючого лікаря;
- у пункті 57 вказується результат медичного лікування хворого. Після заповнення епікризу лікуючий лікар і завідувач відділення зазначають свої прізвища, підписи, реєстраційні номери та дату (число, місяць, рік) заповнення;
- у підпунктах 57.1, 57.2 після заповнення епікризу лікар і завідувач відділення зазначають свої прізвища, підписи, реєстраційні номери та дату (число, місяць, рік) заповнення [12].

Щомісячно, згідно стандартів експертизи ведення медичної документації конкретного закладу охорони здоров'я, медична картка стаціонарного хворого завіряється підписом особи вищого рівня експертизи (заступник генерального директора, медичний директор, представники контролюючих органів тощо).

На підставі даних форми № 003/о формуються звіти про діяльність лікаря, відділення, закладу в цілому.

На вимогу наказу Міністерства охорони здоров'я України від 14.02.2012 № 110 у разі ведення форми № 003/о в електронному форматі вона повинна включати в себе всі дані, які містяться на паперовому носії інформації. Строк зберігання форми № 003/о - 25 років.

## 1.4. Аналіз відповідності медичних інформаційних систем вимогам ведення медичної документації

За аналіз прийнято приклад ведення медичних записів у МІС Х, що підключена до центральної бази даних електронної системи охорони здоров'я

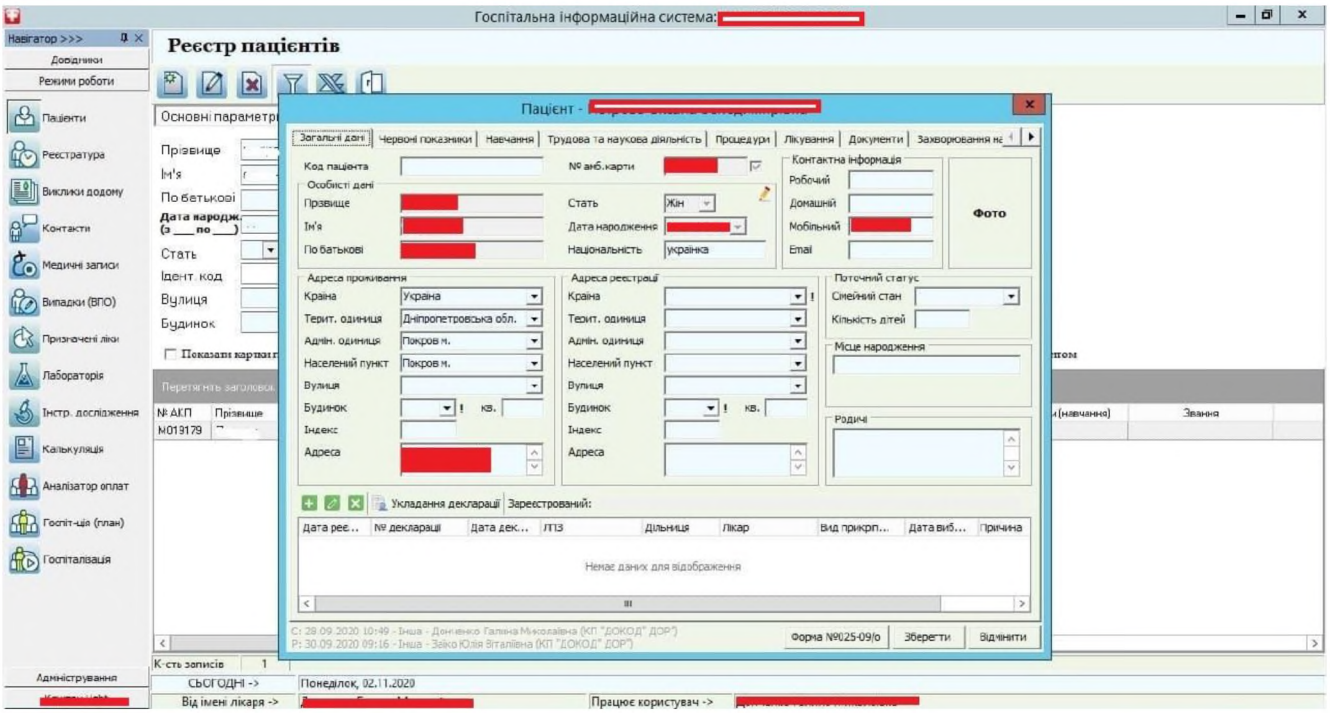


Рисунок 1.6 – Інтерфейс паспортної частини електронної картки (етап реєстратури)

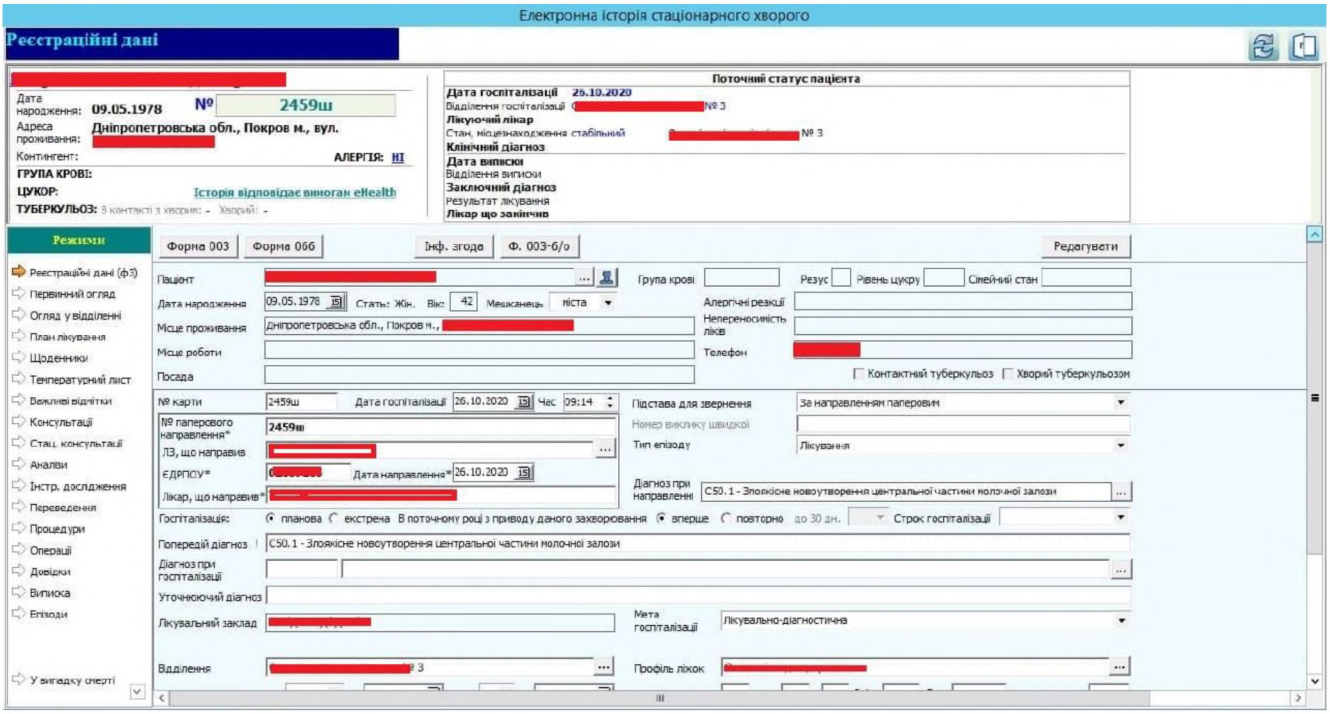


Рисунок 1.7 – Інтерфейс паспортної частини електронної картки (етап приймального відділення стаціонару)

В паспортній частині є всі елементи медичної картки, що повинні бути відображені: (дата та час госпіталізації, прізвище, ім’я, по батькові хворого, стать, дата народження, вік, назва та номер документа, що посвідчує особу, код країни,

громадянином якої є, постійне місце проживання, місце роботи, посада; для інвалідів - вид і група інвалідності, найменування та код закладу охорони здоров'я, який направляє хворого до стаціонару). Зазначено діагноз при госпіталізації, коди відділення закладу охорони, вид госпіталізації (ургентна чи планова), інформація про обстеження на ВІЛ-інфекцію, група крові хворого, резус-приналежність, дата (число, місяць, рік) проведення реакції Васермана, щодо алергічних реакцій, гіперчутливості чи непереносимості лікарського засобу (вказуються назва лікарського засобу, характер побічної дії). Передбачено фіксування первинна чи повторна госпіталізація.

Зазначені пункти заповнюються медичним працівником у приймальному відділенні закладу охорони здоров'я. В інструкції по заповненню форми № 003/о визначено, що всі записи здійснює лікуючий лікар. Після цього у пункті він зазначає свої прізвище, ім'я, по батькові, підпис і реєстраційний номер. На етапі приймального відділення є відмітка про сестру медичну, що створила госпіталізацію. Підпис лікуючого лікаря не передбачено.

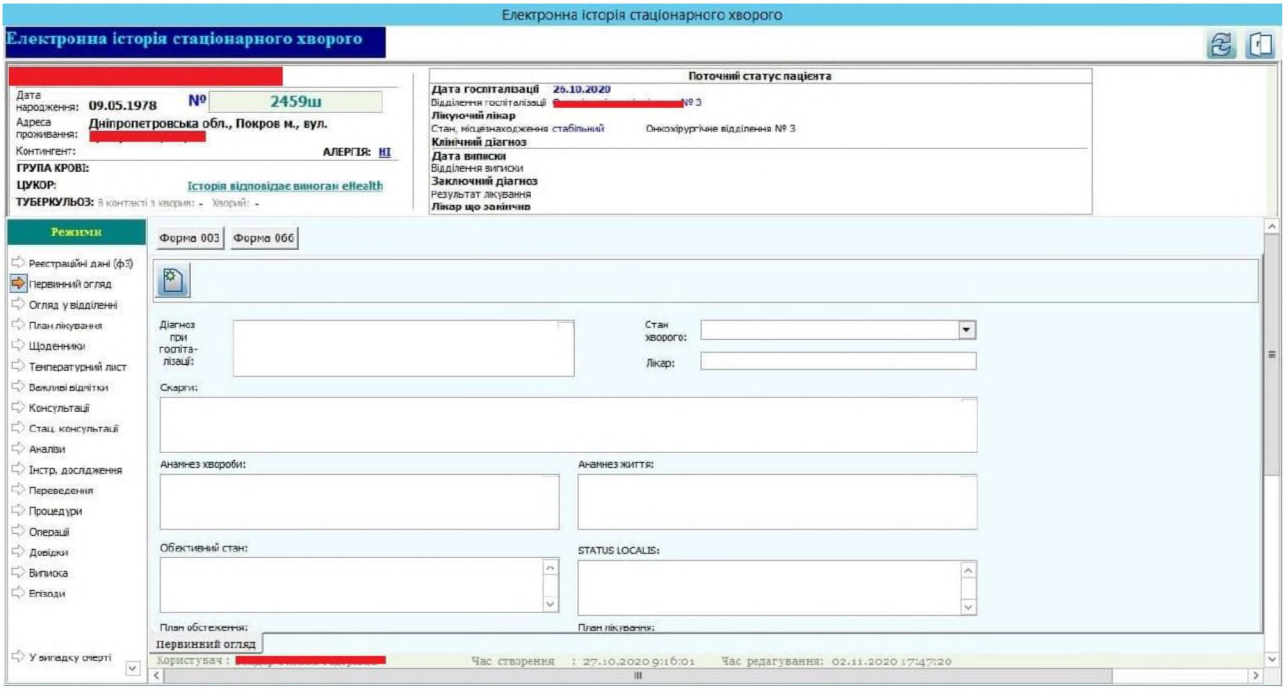


Рисунок 1.7 – Інтерфейс первинного огляду пацієнта електронної картки

Відповідно до вимог наказу Міністерства охорони здоров'я України від 14.02.2012 № 110 «У пункті 39 відмічається, чи ознайомлений хворий із режимом дня та забороною паління, зазначаються дата (число, місяць, рік) ознайомлення та

підпис хворого. У пункті 40 лікар приймального відділення проставляє свої прізвище, ім'я, по батькові, підпис та реєстраційний номер». Опції підпису лікарем даних, внесених на етапі приймального відділення, не передбачено.

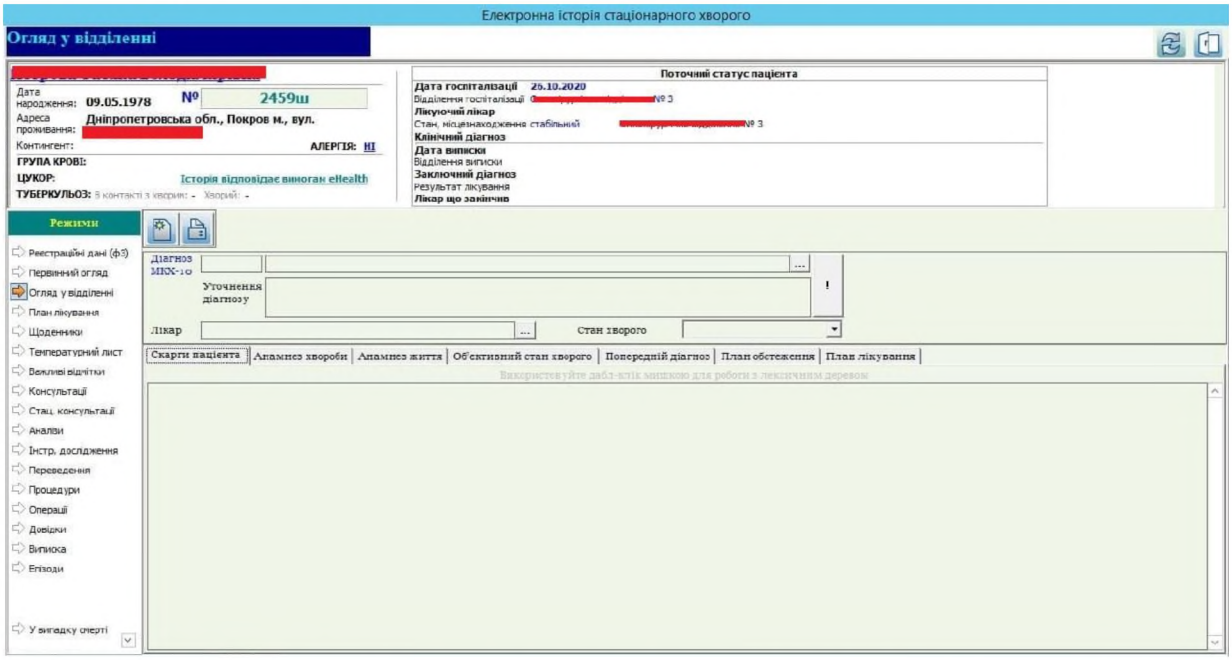


Рисунок 1.8 – Інтерфейс первинного огляду у відділенні електронної картки

Вимоги у оформленні документації дотримано: етап містить фіксацію скарг пацієнта, анамнез хвороби, анамнез життя, об'єктивний стан хворого, попередній діагноз, план обстеження та план медичного лікування.

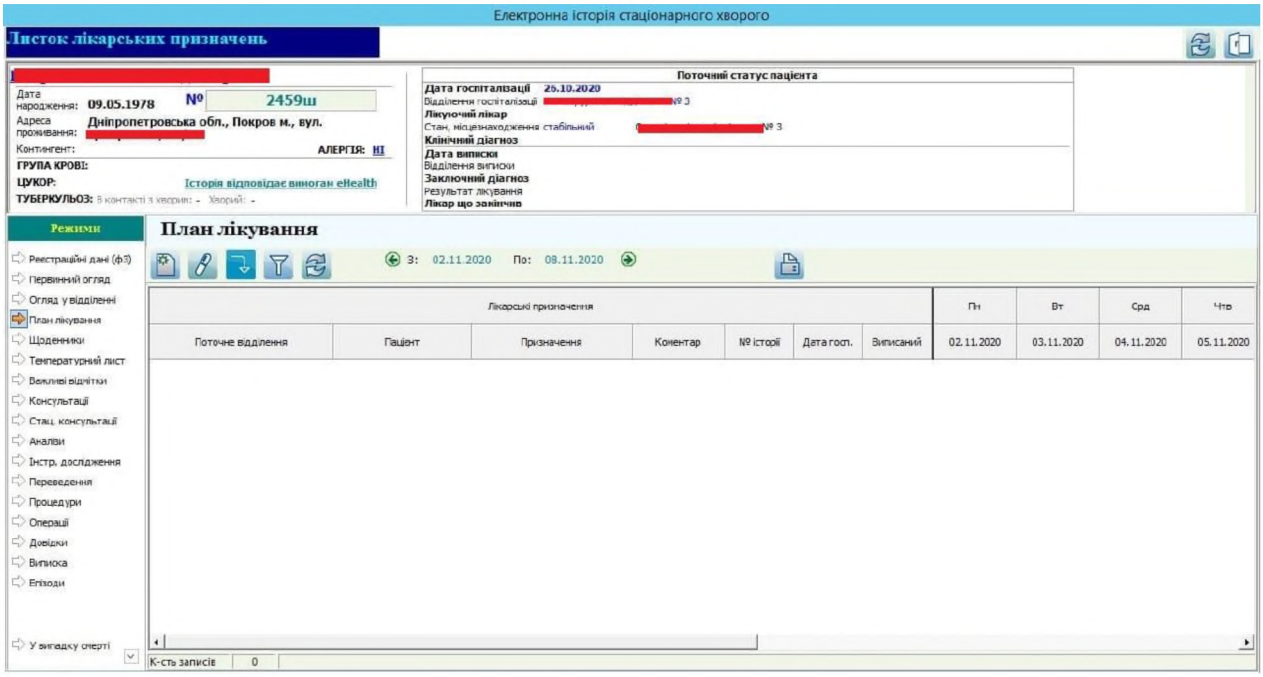


Рисунок 1.9 – Інтерфейс плану лікування електронної картки

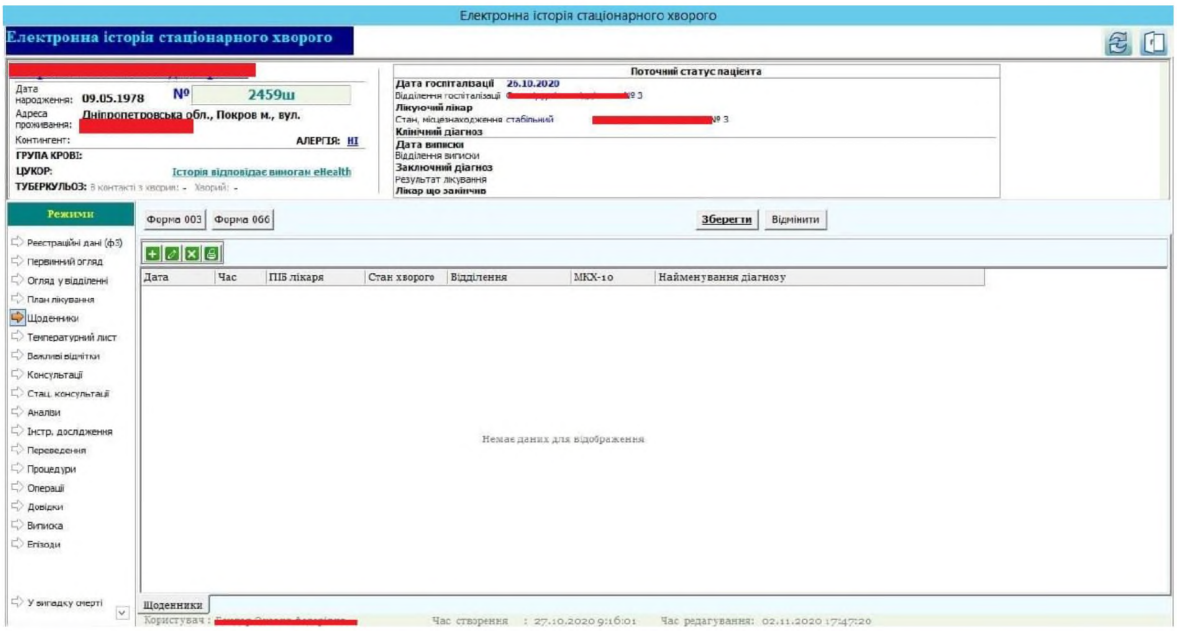


Рисунок .1.10 – Інтерфейс щоденника електронної картки

Відповідно до вимог вищезазначеного наказу лікар здійснює записи про стан здоров'я та медичного лікування хворого у повному обсязі та відображати зміни стану хворого (погіршення, поліпшення, повне одужання) та увесь процес медичного лікування впродовж перебування в стаціонарі. Записи щоденника повинні засвідчуватись підписом лікуючого лікаря. Зазначена опція не передбачена в представленій електронній картці пацієнта. Також не дотримується зберігання щоденників (обмеження доступу до записів) у лікуючого лікаря у період перебування хворого в стаціонарі.

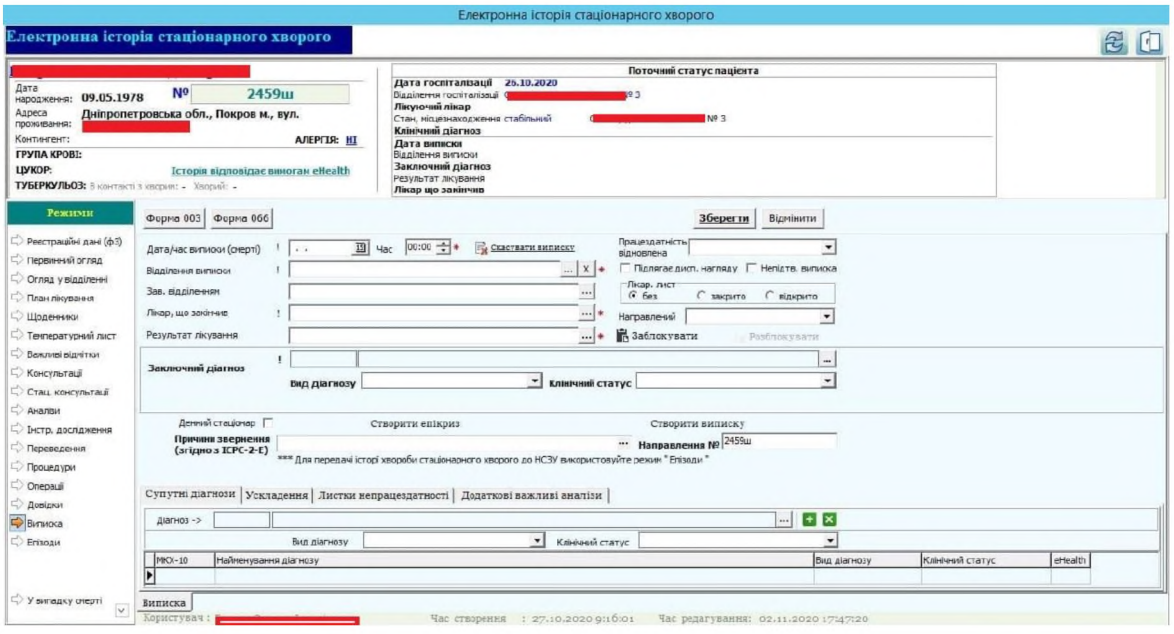

Рисунок 1.11 – Інтерфейс виписка зі стаціонару електронної картки

Етап виписки зі стаціонару передбачає внесення даних з медичної картки в обсязі, що передбачена вимогами наказу Міністерства охорони здоров'я України від 14.02.2012 № 110. Але відсутнє дотримання основної вимоги п. 34 Інструкції, затвердженої цим наказом, а саме: «Після заповнення епікризу лікуючий лікар і завідувач відділення зазначають свої прізвища, підписи, реєстраційні номери та дату (число, місяць, рік) заповнення».

Відповідність електронних записів медичної карти стаціонарного хворого існуючим нормативам веденням медичної документації викладена в додатку Б.

## 1.5. Висновки

Впровадження електронної медицини – це етап розвитку системи охорони здоров'я, що відбувся. Бурхливе впровадження ІТ розробок в систему охорони здоров'я обумовлено підвищенням якості обслуговування пацієнтів, підвищення ефективності роботи медперсоналу, підвищення рентабельності закладів охорони здоров'я. Питання безпеки інформації в медичних інформаційних системах є на сьогоднішній день актуальним й пріоритетним напрямком в розвитку ІТ-медицини. Розробка програмного забезпечення, яке супроводжує електронну медицину, знаходиться в постійному оновленні, яке може вміщувати в себе, як в підході, так і в реалізації продукту, деякі недоліки, в тому числі й інформаційній безпеці. Основними недоліками існуючої системи є те, що не в повній мірі відображають вимоги законодавства щодо ведення медичної документації. В результаті чого існує підґрунтя для виникнення зловживання в використанні медичних інформаційних систем. Основна задача – недопущення та попередження зловживань шляхом протоколювання дій користувачів в медичній інформаційній системі для забезпечення можливості проведення службових розслідувань. Розробка протоколювання дій є на сьогодні однією з актуальних, тому існує необхідність в розробці та подальшому впровадженні методики реєстрації дій над інформацією, що. потребує захисту в медичних інформаційних системах.

# 2. СПЕЦІАЛЬНА ЧАСТИНА

## 2.1. Основні вимоги до методики реєстрації дій над інформацією, яка потребує захисту в медичних інформаційних системах

Збереження лікарської таємниці – пріоритетний напрямок в розвитку електронних систем в охороні здоров'я. Саме персональні дані пацієнтів є основною метою кіберзлочинників. Експерти в галузі кібербезпеки постійно працюють над розробкою базової методології технічних засобів захисту інформації. Ця методологія розробляється на підставі існуючих законодавчих та нормативних актів , що регулюють способи доступу, обробки, зберігання та передачі даних.

У відповідності до існуючого законодавства, кожний заклад системи охорони здоров'я, власник МІС, повинен забезпечити необхідні організаційні та технічні заходи для захисту персональних даних від неправомірних дій. Для попередження ненавмисних та випадкових погроз необхідні спеціальні засоби ідентифікації користувача, що забезпечують доступ до системи лише у разі повної упевненості в наявності у користувача прав користування та обсягу доступу до інформації.

Основну частину збитку системі завдають дії легальних користувачів, по відношенню до яких операційні регулятори не можуть дати вирішального ефекту. Головні вороги - некомпетентність і неакуратність при виконанні службових обов'язків, і тільки програмно-технічні заходи здатні їм протистояти.

Основний перелік вимог до методики щодо забезпечення реєстрації дій над інформацією, що потребує захисту:

- методика повинна сприяти виникненню мінімальних змін та не впливати на функціонуючу медичну інформаційну систему. Дозволяється покращання її роботи, розширення функціоналу, але не порушувати систему;
- сприяти веденню електронної медичної документації у відповідності до вимог існуючих норматив та законодавчих актів;

- застосована методика не повинна вимагати високої кваліфікації користувачів;
- впровадження додаткової методики не повинно спричинити зайвих фінансових витрат: придбання додаткового обладнання, введення нових посад у штатний розклад медичного закладу, вимагати часу на навчання користувачів.

## 2.2. Формалізація вимог до системи реєстрації дій над інформацією, яка потребує захисту в медичних інформаційних системах (послуги безпеки)

Відповідно до нормативного документу системи технічного захисту інформації «Класифікація автоматизованих систем і стандартні функціональні профілі захищеності оброблюваної інформації від несанкціонованого доступу» медичні інформаційні системи слід віднести до автоматизованих систем класу «3»: МІС є розподіленим багатомашинним багатокористувацьким комплексом, який обробляє інформацію різних ступенів обмеження доступу, тобто належить до автоматизованих систем (АС), які призначені для автоматизації діяльності закладів охорони здоров'я. Крім того, існує необхідність передачі інформації через незахищене середовище або, в загальному випадку, наявність вузлів, що реалізують різну політику безпеки.

Загрози безпеки для медичної інформаційної системи поділяються на наступні основні типи:

- несанкціонований доступ (перегляд інформації співробітником, який не має дозволу користуватися нею, шляхом перевищення посадових повноважень. Несанкціонований доступ призводить до витоку інформації. Залежно від того, які дані і де вони зберігаються, витоку можуть організовуватися різними способами, а саме через атаки на сайти, злом програм, перехоплення даних по мережі, використання несанкціонованих програм;
- витік інформації як випадковий, так й навмисний (Випадкові витоки відбуваються через помилки обладнання, програмного забезпечення та

персоналу. Умисні, в свою чергу, організовуються навмисно з метою отримати доступ до даних, завдати шкоди);

- втрата даних (Одна з основних загроз в інформаційній безпеці. Порушення цілісності інформації може бути викликано несправністю обладнання або навмисними діями людей, будь то співробітники або зловмисники).

З приводу комплексу засобів захисту необхідно розглянути НД ТЗІ 2.5-005 - 99 та НД ТЗІ 2.5-004-99. В даних нормативних документах наведені рекомендовані для використання профілі щодо автоматизованих систем.

Стандартний функціональний профіль захищеності для автоматизованих систем класу 3.КЦД.1 = { КД-2, КО-1, КВ-1, ЦД-1, ЦО-1, ЦВ-1, ДР-1, ДВ-1, НР-2, НИ-2, НК-1, НО-2, НЦ-2, НТ-2, НВ-1 } слід застосовувати разом із додаванням послуги НА-1, яка забезпечить політику автентифікації відправника, визначення множини властивостей і атрибутів об'єкта, що передається, користувача-відправника і інтерфейсного процесу, а також процедури, які дозволяли б однозначно встановити, що даний об'єкт був відправлений (створений) певним користувачем.

Розглянемо наступні основні послуги безпеки:

- ідентифікацію та автентифікацію користувачів (ідентифікація та атентифікація дозволисть КСЗ визначити і перевірити користувача, що намагається одержати доступ до ІС (НИ-2);
- протоколювання (реєстрація подій) (реєстрація дозволяє контролювати небезпечні для ІС дії. Рівні даної послуги ранжуються залежно від повноти і вибірковості контролю, складності засобів аналізу даних журналу реєстрації і спроможності вияву потенційних порушень) (НР-2);
- автентифікація відправника (ця послуга дозволяє забезпечити захист від відмови від авторства, однозначно встановити належність певного об'єкта певному користувачу, тобто той факт, що об'єкт був створений або відправлений даним користувачем) (НА-1).

Комплекс засобів захисту повинен бути здатним здійснювати реєстрацію подій, що мають безпосереднє відношення до безпеки. Також повинен забезпечуватись захист журналу реєстрації від несанкціонованого доступу, модифікації або руйнування.

Основні організаційні та технічні засоби по забезпеченню захисту персональних даних містять:

- ідентифікацію та автентифікацію суб'єктів доступу та об'єктів доступу;
- управління доступом суб'єктів доступу до об'єктів доступу;
- захист технічних носіїв інформації, на яких зберігаються чи обробляються персональні дані;
- реєстрація подій безпеки;
- контроль захищеності персональних даних;
- захист технічних засобів;
- виявлення фактів загроз безпеки та реагування на них.

В МІС управління доступом забезпечується основі розподілу ролей з розподілом прав в роботі в системі. Рольова модифікація найбільш адекватно забезпечує вимоги захисту медичної інформації.

В інформаційній системі медичного закладу об'єктами захисту є:

- інформація в баз даних;
- ресурси файлового сервера закладу охорони здоров'я;
- резервні копії баз даних і архівні копії ресурсів файлового сервера;
- керуюча інформація операційної системи, АРМ адміністратора МІС і адміністратора інформаційної безпеки;
- технологічний процес збору, обробки, зберігання та передачі інформації в МІС;
- апаратно-програмний комплекс, що забезпечує роботу МІС.

Для досягнення найбільшого ефекту при організації захисту інформації в МІС необхідно дотримуватись наступними правилами:

Першим і найбільш важливим є правило, що забезпечення інформаційної безпеки не може бути разовим заходом, а потребує постійного вдосконалення і розвитку системи інформаційної безпеки.

Друге правило, що комплексне використання всіх ресурсів наявних засобів захисту у всіх всіх відділах та відділеннях лікувального закладу, а також на всіх етапах обробки інформації [13].

Допущені до роботі в МІС користувачі мають різні повноваження для отримання доступу до інформаційних, програмних, апаратних та інших ресурсів МІС відповідно до прийнятої політики інформаційної безпеки (правилами).

При функціонуванні МІС інформаційна безпека забезпечується спеціальними програмними засобами - підсистемою інформаційної безпеки, що виконує наступні основні функції:

- організація санкціонованого доступу до даних;
- моніторинг небезпечних подій;
- управління властивостями користувача МІС;
- ведення журналів безпеки.

Організація санкціонованого доступу до бази даних належить до загальносистемних механізмів. Решта функцій покладено для адміністратора інформаційної безпеки МІС.

МІС зобов'язана надавати лікарям та іншим користувачам необхідну їм інформацію відповідно до їх функціональних обов'язків і не повинна перешкоджати в отриманні цієї інформації. Одночасно з тим закон захищає право громадян для нерозголошення інформації про стан їх здоров'я. Для цього доступ користувачів до систем, що містить таку інформацію, повинен бути авторизованим. При цьому для кожного користувача повинен бути визначений рівень доступу, тобто обсяг функцій і інформаційних ресурсів, до яких він отримує доступ. Особлива увага повинна приділятися поділу доступу користувачів МІС до різних фрагментів даних і захисту інформації від несанкціонованого доступу, а також від втрати і спотворення даних.

Особливість медичної предметної області обумовлює в розробленої медичної інформаційної системи застосування дворівневої моделі груп доступу.

Спільне застосування двох видів груп, одна з яких враховує рівні прав доступу, а інша медичну спеціальність всіх об'єктів МІС від сервера до електронного документа в БД МІС, дозволяють одночасно забезпечити і максимальну захищеність системи, і максимально ефективну, і просту в експлуатації належність безпеки

На практиці виконання зазначених вимог має здійснюватися в МІС власною системою безпеки, що має найвищий пріоритет над будь-якими іншими процесами в МІС. Іншими словами, в МІС не повинно бути програмних або апаратних модулів, які могли б отримати путь до даних або програм МІС в обхід системи безпеки.

Робота в МІС ведеться в режимі, розрахованому для багатьох користувачів з розмежуванням прав доступу. Розмежування доступу забезпечується після автентифікації суб'єктів.

При вході в систему і видачу запитів на доступ здійснюється автентифікація користувачів МІС, яка має в своєму розпорядженні необхідними даними для ідентифікації, автентифікації, а також перешкоджає несанкціонованому доступу до ресурсів.

При вході в систему користувач вводить логін і пароль, після чого конструкція визначає роль (повноваження) даного користувача і запускає відповідний модуль. Вузол дозволяє путь тільки до тих даних, які необхідні для роботи конкретного користувача згідно матриці доступу. Щоб забезпечити безпеку даних, система повинна обмежувати путь до інформації навіть всередині однієї групи користувачів. Так, лікар повинен мати доступ до своїх історій хвороби і пред архівних історій хвороби тих пацієнтів, яких він лікував; завідувач відділенням - тільки до історій хвороби пацієнтів відповідного відділення; лікар-консультант отримує доступ історій хвороби заданих (адміністратором безпеки) відділень і тільки при наявності відповідного направлення в електронній історії хвороби.

Всі спроби входу в систему повинні фіксуватись в електронних журналах. Так можна виявити, хто та коли звертався до системи, відстежити спроби підбору пароля та інші потенційно небезпечні події.

## 2.3. Спосіб забезпечення послуги автентифікації користувача (НИ-2)

Основними процедурами реєстрації користувачів в інформаційній системі є процедура ідентифікації та автентифікації. Ідентифікація та автентифікація є основною послугою в системі захисту інформації. Свою автентичність користувач може підтвердити деякими засобами:

- пароль, табельний або ідентифікаційний номер, криптографічний ключ;
- чіпована картка;
- унікальні біометричні дані (відбитки пальців або малюнок сітчатки ока).

Найчастіше в існуючих медичних інформаційних системах використовується система паролів. Існує ряд недоліків при застосуванні зазначеного засобу автентифікації: пароль можна забути, його можна вкрасти, скопіювати, підробити, підглянути. Існують випадки, коли паролі повідомляють колегам. Проте простота та доступність – один з факторів, за яким вибирають саме цю систему автентифікації. Парольна система – найбільш вразлива до електронного перехоплення.

Існують методики для забезпечення безпеки використання парольного методу автентифікації:

- формулювання вимог для створення паролю (кількість знаків, що містять літери великі та маленькі, цифри та розділові знаки);
- визначення терміну дії паролю та їх систематичне оновлення;
- захист доступу до файлу паролів;
- обмеження кількості помилкових проб використання паролю;
- навчання користувачів етиці створення паролів;
- використання сервісів генерації паролів.

Вищенаведені методи слід застосовувати також у випадках, коли паролі застосовуються разом з іншими методами автентифікації, наприклад токенами.

Несанкціоноване отримання зловмисником доступу до ІС пов'язано, в першу чергу, з порушенням процедури автентифікації. Автентифікація - процедура встановлення належності користувачеві інформації в системі пред'явленого ним ідентифікатора. Один із способів автентифікації в інформаційній системі полягає у попередній ідентифікації на основі користувацького ідентифікатора логіна і пароля — певної конфіденційної інформації, знання якої передбачає володіння певним ресурсом в мережі. Отримавши введений користувачем логін і пароль, комп'ютер порівнює їх зі 25 значенням, яке зберігається в спеціальній захищеній базі даних і, у випадку успішної автентифікації виконує авторизацію з подальшим допуском користувача до роботи в системі. Традиційну автентифікацію за допомогою пароля називають ще однофакторною або слабкою. Оскільки за наявності певних ресурсів перехоплення або підбір пароля є справою часу. Таким чином часто виникає необхідність використовувати сильну або багатофакторну автентифікацію - на основі двох чи більше факторів. В цьому випадку для автентифікації використовується не лише інформація відома користувачеві, а й додаткові фактори. Використання багатофакторної автентифікації для підтвердження особи базується на передумові, що неавторизований користувач навряд чи зможе надати фактори необхідні для доступу. Якщо в спробі автентифікації хоча б один з компонентів відсутній або вказаний невірно, то ідентифікація користувача не встановлюється з достатнім ступенем впевненості та доступу до об’єкту (наприклад, до будівлі або даних), захищеному багатофакторною автентифікацією, залишається заблокованим [14].

Для кожного внутрішнього користувача МІС створюється обліковий запис з відповідною роллю, де кожна роль передбачає виконання визначених обов’язків із відповідними обмеженнями. Для кожного облікового запису встановлюються відповідні права доступу до файлових об’єктів, мережевих ресурсів. Система захисту ключами вирішує задачу автентифікацію користувача.

Згідно НД ТЗІ 2.5-004-99, послуга „Ідентифікація та автентифікація” дозволяє визначити і перевірити особистість користувача, що намагається одержати доступ до МІС. Також в МІС повинно бути забезпечено ведення журналу реєстрації, здатним здійснювати реєстрацію подій, що мають безпосереднє відношення до безпеки. Адміністратори і користувачі, яким надані відповідні повноваження, повинні мати в своєму розпорядженні засоби перегляду і аналізу журналу реєстрації.

### 2.3.1. Обґрунтування механізму автентифікації відправника (НА-1)

Автентифікація відправника дозволяє забезпечити захист від відмови від авторства і визначити належність певної корекції вмісту бази даних певному користувачу, тобто той факт, що запис був створений або відправлений конкретним користувачем системи. Для забезпечення зазначеної послуги використовується цифровий підпис.

### 2.3.2. Впровадження цифрового електронного підпису в ідентифікацію записів

Кваліфікований електронний підпис (КЕП, який раніше мав назву ЕЦП — електронний цифровий підпис) - удосконалений електронний підпис, який створюється з використанням засобу кваліфікованого електронного підпису і базується на кваліфікованому сертифікаті відкритого ключа. Існують два типи КЕП: КЕП фізичної особи та КЕП співробітника організації (юридичної особи). Електронна система охорони здоров’я потребує від кожного лікаря мати КЕП співробітника організації. Отримання кваліфікованого електронного підпису є обов'язковою умовою, оскільки він потрібен для підписання всіх документів в МІС.

Електронний цифровий підпис за правовим статусом прирівнюється до власноручного підпису (печатки) у разі, якщо:

– електронний цифровий підпис підтверджено з використанням посиленого сертифіката ключа за допомогою надійних засобів цифрового підпису;

– під час перевірки використовувався посилений сертифікат ключа, чинний на момент накладення електронного цифрового підпису;
– особистий ключ підписувача відповідає відкритому ключу, зазначеному у сертифікаті [15].

Умовну схему, підписання документу можна побачити на рис 2.1


Рисунок 2.1 – Алгоритм підпису документів

Як правило, власний підпис вважається юридичним гарантом авторства документа. У разі якщо підробити підпис людини на папері дуже складно, а ввести авторство підпису передовими криміналістичними способами - техно

дрібниця, то з підписом електричної справа йде по іншому. Підробити ланцюжок бітів, елементарно її скопіювавши, або ж непомітно привнести незаконні поправки в документ може досвідчений користувач. З широким розповсюдженням в системі охорони здоров'я електронних форм документів (в тому числі й конфеденційних) і засобів їх обробки найбільш актуальною стала проблема встановлення автентичності та авторства безпаперової документації. У розділі криптографічних систем з не закритим ключем було показано, власне що при всіх перевагах передових систем шифрування вони не дають можливість гарантувати автентифікацію даних. В наслідок цього способи автентифікації слід застосовувати в сукупності і криптографічними методами. Окрім вибору адекватної для певної МІС криптографічной системи, істотна проблема - управління ключами. Як би не була складна і надійна сама криптосистема, вона заснована на застосуванні ключів. У разі якщо для здійснення секретного обміну інформацією між декількома користувачами процес обміну ключами банальний, то в МІС, де чисельність користувачів досягає сотні, управління ключами - відповідальна проблема. Під головною інформацією розуміється сукупність всіх задіяних в ІС ключів. У разі якщо не забезпечено досить надійне управління головної інформацією, то оволодівши нею, злочинець отримує необмежений доступ до всієї інформації.

Управління ключами - інформаційний процес, що включає в себе основні напрямки:

– генерацію ключів;
– накопичення ключів;
– розподіл ключів.

Розглянемо, як визначені напрямки повинні здійснюватися для такого, щоб гарантувати захищеність головною інформації в ІС.

У серйозних ІС застосовуються особливі апаратні і програмні способи генерації випадкових ключів. Як правило використовують детектори ПСЧ. Втім рівень випадковості їх генерації повинна бути досить високою. Ідеальним генераторами вважаються прилади на базі "натуральних" випадкових процесів. До

прикладу випадковим математичним об'єктом вважаються десяткові символи ірраціональних кількостей, які розраховуються з підтримкою нормальних математичних методів.

Під накопиченням ключів розуміється організація їх зберігання, обліку та знищення. В зв'язку з тим, що ключ вважається найбільш привабливим для злочинців об'єктом, який відкриває йому дорогу до конфіденційної інформації, то завданням накопичення ключів слід приділяти особливу увагу. Приховані ключі жодного разу не повинні записуватися в очевидному вигляді на носії, який має можливість бути зчитаним або ж скопійований. В досить об'ємній ІС користувач має можливість працювати з величезним розміром головною інформації, і часом в тому числі і з'являється потреба організації невеликих баз даних по головній інформації. Ці бази даних відповідають за прийняття, збереження, облік і видалення застосовуваних ключів. Нарешті, будь-яка інформація про застосовувані ключи зобов'язана зберігатися в зашифрованому вигляді. Ключі, зашифровують головну інформацію іменуються майстер-ключами. Ідеально, якщо майстер-ключі кожен користувач знав на пам'ять, і не зберігав їх взагалі на якихось речових носіях. Досить необхідною умовою захищеності інформації вважається періодичне оновлення головної інформації в ІС. При цьому перепризначатися зобов'язані як звичайні ключі, наприклад і майстер-ключі. У найбільш серйозних ІС оновлення головної інформації краще створювати кожен день. Питання оновлення головної інформації пов'язаний і з наступним напрямком управління ключами - розподілом ключів.

Розподіл ключів - найсерйозніший процес в управлінні ключами. До нього пред'являються наступні вимоги:

– оперативність і точність розподілу;
– секретність ключів, що розподіляються.

Останнім часом помітний зсув в бік застосування криптосистем з не закритим ключем, в яких проблема розподілу ключів відпадає. В той же час розподіл інформації про ключі в ІС вимагає свіжих дієвих висновків. Розподіл ключів між користувачами реалізуються наступними шляхами:

1) Шляхом створення єдиного чи декількох центрів розподілу ключів;

Брак такого підходу складається в тому, в що в центрі розподілу відомо, кому і які ключі призначені і це дозволяє декламувати всі повідомлення, що циркулюють в ІС. Ймовірні зловживання суттєво впливають на захист.

2) Взаємообмін ключами між користувачами інформаційної системи;

В даному випадку проблема очевидна в тому, щоб надійно запевнити справжність суб'єктів. Для обміну ключами можливо застосувати криптосистеми з не закритим ключем, застосовуючи що ж метод RSA.

Як узагальнення сказаного про розподіл ключів робимо висновки: Завдання управління ключами зводиться до винаходу такого протоколу розподілу ключів, який забезпечував би:

- ймовірність відмови від центру розподілу ключів;
- двобічне свідчення справжності елементів сеансу;
- свідоцтво достовірності сеансу механізмом запиту-відповіді, використання для цього програмних або ж апаратних засобів;
- впровадження при обміні ключами малої кількості повідомлень.
- проблема реалізації засобів захисту інформації містить основні складові:
- розробка засобів, що реалізують криптографічні алгоритми;
- методика застосування даних засобів.

Будь-який з розглянутих криптографічних засобів можуть бути здійснені або програмною, або апаратною методикою. Імовірність програмного здійснення обумовлюється тим, власне що всі способи криптографічного перебудови формальні і мають всі шанси бути представлені у вигляді кінцевої алгоритмічної процедури. При апаратної реалізації всі процедури шифрування і дешифрування виробляються особливими електричними схемами. Найбільшого поширення набули модулі, що реалізують комбіновані способи. Основна маса іноземних серійних засобів шифрування засноване на південноамериканському ідеалі DES. Головною перевагою програмних способів реалізації захисту вважається їх адаптивність, тобто ймовірність доступної можливості зміни конфігурації

алгоритмів шифрування. Головним же дефектом програмної реалізації вважається витратною за часом в порівнянні з апаратними способами (приблизно в 10 разів).

З урахуванням того, що ЕЦП являє собою код, тобто набір електронних даних у двійковій формі, "прочитати" безпосередньо з нього дані про особу підписувача неможливо. Для цього існує і використовується механізм, в основу якого покладено сертифікат відкритого ключа (СВК), що формується для кожного конкретного ВК одним з суб'єктів інфраструктури відкритого ключа (ІВК) – центром сертифікації ключів (ЦСК)/акредитованим центром сертифікації ключів (АЦСК), або засвідчувальним центром. Відповідно до статті 1 Закону України "Про електронний цифровий підпис" ЕЦП дає змогу перевірити цілісність електронних даних, на які він накладений, та ідентифікувати особу підписувача. Оскільки ЕЦП являє собою код, то для отримання даних про особу підписувача використовується механізм сертифікату відкритого ключа (СВК). При цьому СВК (ПСВК) являє собою документ, виданий ЦСК (АЦСК, засвідчу вальним центром). Відповідно до статті 1 зазначеного Закону цей документ засвідчує чинність і належність ВК підписувачу. При цьому СВК можуть розповсюджуватися в електронній формі або у формі документа на папері та використовуватися для ідентифікації особи підписувача. Склад СВК визначено у статті 6 цього Закону. Він містить, зокрема, основні дані (реквізити) підписувача – власника ОК, а також ВК, який є парним до цього ОК, що означає, що ці ключі були з генеровані разом.

Відповідно до постанови Кабінету Міністрів України "Про затвердження Порядку застосування електронного цифрового підпису органами державної влади, органами місцевого самоврядування, підприємствами, установами та організаціями державної форми власності" справжність ЕЦП, накладеного на ЕД або інші електронні дані, та цілісність цього документа (електронних даних) перевіряється з дотриманням таких вимог: – ЕЦП повинен бути підтверджений з використанням ПСВК за допомогою надійних засобів ЕЦП; – під час перевірки повинен використовуватися ПСВК, чинний на момент накладення ЕЦП; – ОК підписувача повинен відповідати ВК, зазначеному у ПСВК; – на час перевірки

повинен бути чинним ПСВК, сформований АЦСК та ПСВК відповідного засвідчувального центру.

Відповідно до статті 6 Закону України "Про електронні документи та електронний документообіг" накладанням електронного підпису завершується створення ЕД. Це означає, зокрема, що на цей момент в ЕД повинні бути присутніми усі необхідні елементи, включаючи його номер і дату підписання. На цю обставину слід звернути увагу під час впровадження і використання ЕД і ЕДО із застосуванням ЕЦП. Практика традиційного документообігу свідчить, що дата і номер зазвичай вносяться до документа на папері вже після його підписання. Внесення дати і номера до ЕД, на який вже накладено ЕЦП, порушить цілісність цього ЕД (набору даних) і при перевірці справжності ЕЦП буде отриманий негативний результат. Позначка часу Постановою Кабінету Міністрів України "Про затвердження Порядку засвідчення наявності електронного документа (електронних даних) на певний момент часу" визначено умови та вимоги до процедури засвідчення і створені правові засади для надання ЦСК відповідних послуг ЕЦП (точніше – послуг у сфері використання ЕЦП). У цьому Порядку визначено такі терміни: послуга фіксування часу – процедура засвідчення наявності ЕД (електронних даних) на певний момент часу шляхом додання до нього або логічного поєднання з ним позначки часу; позначка часу – сукупність електронних даних, створена за допомогою технічних засобів та засвідчена ЕЦП центру сертифікації ключів, яка підтверджує наявність ЕД (електронних даних) на певний момент часу. Затвердженням зазначеного Порядку врегульовано функціонування ЦСК – довірених суб'єктів в ІВК, які повинні цілодобово надавати послуги зі створення позначок часу і мати при цьому точне й надійне джерело часу. У процесі фіксування часу позначка часу (англ. – Time Stamping) додається або логічно поєднується з електронними даними таким чином, щоб була виключена можливість вносити до них зміни, а також зберігати позначки часу після надання послуги фіксування часу. Наявність позначки часу дає змогу перевірити достовірність часу наявності ЕД (електронних даних). При цьому можна використовувати СВК, який на момент перевірки ЕЦП, накладеного на ЕД,

вже анульований або відкликаний. В іншому випадку, актуальність підписаного ЕД обмежена терміном дії СВК. Спільним наказом Держкомінформнауки та Держспецзв'язку затверджені "Технічні специфікації форматів представлення базових об'єктів національної системи електронного цифрового підпису (протокол фіксування часу)". Вимоги цих Технічних специфікацій є обов'язковими для надійних засобів ЕЦП, програмнотехнічних комплексів АЦСК. Правильність реалізації протоколу та наведених форматів у засобах ЕЦП повинна бути підтверджена сертифікатом відповідності або позитивним експертним висновком за результатами державної експертизи у сфері криптографічного захисту інформації. Технічні специфікації визначають процедуру формування позначки часу, зокрема дії, які при цьому виконують користувач та ЦСК. Згідно з процедурою, користувач попередньо обчислює хеш-код (хеш-значення) ЕД (електронного набору даних). Слід зазначити, що обчислення цього коду є проміжним технологічним етапом при формуванні ЕЦП, що накладається на ЕД. Після цього користувач формує запит на формування позначки часу, який містить, у тому числі й обчислений хеш-код, і передає його до ЦСК. В свою чергу, ЦСК перевіряє правильність формату запиту та виконує його обробку, формує позначку часу та відповідь, що містить цю позначку, чи відповідь з інформацією про відмову у формуванні позначки часу. За результатом опрацювання цієї послуги ЦСК пересилає користувачеві відповідь, що містить позначку часу, засвідчену ЕЦП центру. Сформована позначка часу, тобто сукупність електронних даних, створена за допомогою технічних засобів, містить у тому числі й хеш-код ЕД (електронного набору даних), для яких було сформовано позначку, час її формування та серійний номер. Користувач після отримання відповіді, отриманої від ЦСК, перевіряє результат обробки свого запиту у відповіді центру. За позитивного результату обробки користувачем перевіряється відповідність імені суб'єкта, що підписав позначку часу, власне імені ЦСК, наявність у центру права формувати позначки часу, чинність СВК центру та справжність ЕЦП, накладеного на отриману від центра позначку. Після цього користувач порівнює попередньо обчислений ним хеш-код ЕД та хеш-код,

записаний у позначці часу. За позитивним результатом порівняння позначка часу може бути додана до ЕД. Перевірка позначки часу може бути виконана будь-яким суб'єктом (верифікатором) за допомогою СВК, що належить ЦСК, автономно, без взаємодії з цим центром. З цією метою верифікатор витягує позначку часу з ЕД, до якого вона була прикріплена, і отримує з неї ідентифікаційну інформацію про ЦСК. На її основі може бути отриманий СВК, що належить ЦСК, який зберігається у ЦЗО (засвідчувальному центрі). За допомогою чинного (на момент формування позначки) СВК центру сертифікації ключів версифікатор перевіряє справжність ЕЦП, накладеного на позначку часу. Після цього, шляхом порівняння обчисленого хешкоду ЕД та хеш-коду, що зберігається у позначці часу, можна вже перевірити відповідність позначки часу та ЕД, до якого вона була прикріплена. Позначка часу на ЕД засвідчує точний час, на який цей документ вже існував і тому за її допомогою в подальшому можна буде розв'язувати конфлікти, пов'язані з використанням цього документа. Зокрема, за її допомогою можна забезпечити не відмовність автора ЕД від свого ЕЦП. Наявність позначки часу, доданої до ЕД, дозволяє продовжувати термін дії накладеного на нього ЕЦП. Така позначка (штамп) засвідчує, наприклад, що ЕЦП був накладений на ЕД до того, як відповідний СВК був анульований (відкликаний). Таким чином, для перевірки справжності ЕЦП, накладеного на ЕД до моменту відкликання СВК, можна використовувати ВК, що міститься у вже анульованому або відкликаному сертифікаті. Ланцюжок позначок часу дозволяє створювати системи архівного зберігання ЕД, причому зі збереженням справжності ЕЦП, накладених на ці документи. В іншому випадку, справжність підписаного ЕД обмежена терміном дії СВК, який був чинним на момент накладання ЕЦП. Слід підкреслити, що для отримання позначки часу користувач не повинен надсилати до ЦСК ні сам ЕД (електронний набір даних), ні накладений на нього ЕЦП. Тобто процедура формування позначки часу жодним чином не може порушити конфіденційність ЕД (електронного набору даних) і вона може бути використана, наприклад, як один з механізмів у підтвердженні авторства на літературний твір,

аудіовізуальний твір у цифровому форматі, базу даних, комп’ютерну програму тощо.

Останнім часом все більш отримують поширення комбіновані методи шифрування, такі як програмно-апаратні. В даному випадку в комп'ютері застосовується оригінальний "криптографічний співпроцесор" - обчислювальний прилад, спрямоване на виконання криптографічних операцій (додавання по модулю, зсув і т.д.). Змінюючи програмне забезпечення для такого приладу, можливо обирати той чи інший спосіб шифрування. Подібний спосіб включає в себе позитивні сторони програмних і апаратних засобів [16].

Наказом Національної служби здоров'я від 30.09.2019 р. № 385 МІС заборонено зберігати паролі КЕП та файли приватних ключів [17].

Деякі документи в МІС завіряються двома та більше підписами (лікар, завідувач відділом, заступник головного лікаря). На сьогоднішній день ця процедура виглядає, як послідовне накладання КЕП декількома користувачами, що складається з декількох етапів: підписання лікарем, підписання завідувачем, підписання, при необхідності, третім користувачем. На рис. 2.2 зображен алгоритм додаткового підпису документів, коли вже підписаній документ завіряється ще одним підписом.


Рисунок 2.2 – Додатковий підпис документів

Так як процедура додаткових підписів є часозатратнна та не зручна, в роботі пропонується в МІС реалізовувати можливість колективного електронного підпису. Схема зображена на рис. 2.3. Електронний цифровий підпис звичайного розміру повинен свідчить про те, що бідь-який електронний документ підписано кожним користувачем з деякої кількості користувачів МІС: лікаря, завідувача відділенням, членів консиліуму, у разі необхідності – адміністрацією медичного закладу. При цьому до колективного електронного цифрового підпису (КЕЦП) висуваються наступні вимоги:

– цілісність (неможливість виявлення правильного підпису);
– незалежність від користувачів: КЕЦП може сформувати будь-яка група користувачів, незалежно від їх кількості та складу;

– синхронність генерації КЕЦП: всі складові, що з'являються на проміжних етапах процедури генерації КЕЦП, не повинні бути відповідними підписами до будь-яких повідомлень;
– невід'ємність: за конкретним колективним підписом неможливо сформувати іншу КЕЦП [18].

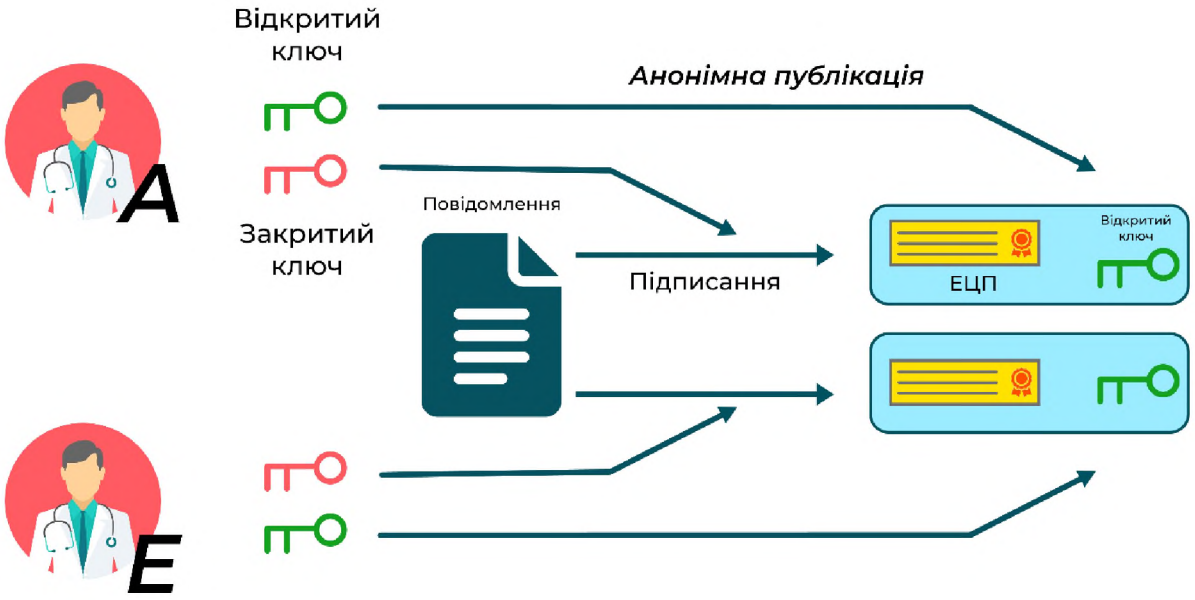


Рисунок 2.3 – Схема колективного електронного підпису

В якості базової ідеї протоколу КЕЦП приймається концепція використання колективного відкритого ключа, що є функцією відкритих ключів користувачів. Колективний відкритий ключ деякої довільно задається сукупності m користувачів, кожен з яких є власником відповідного відкритого ключа з безлічі $y_1, y_2, \ldots, y_m$, являє собою деяке значення $y = f(y_1, y_2, \ldots, y_m)$. Загальна схема формування КЕЦП була реалізована у вигляді задовольняють перерахованим вимогам конкретних алгоритмів і протоколів з використанням наступних важких обчислювальних задач:

– витяг коренів великий простий ступеня за великим простому модулю;
– дискретного логарифмування в мультиплікативної групі великого простого порядку;
– дискретного логарифмування в групі точок еліптичної кривої спеціального виду.

Особливий інтерес представляють алгоритми, засновані на останній з перерахованих важких завдань, оскільки в цьому випадку забезпечується максимальна продуктивність процедур генерації і перевірки підпису. Гідність запропонованої концепції КЕЦП полягає в використанні стандартної інфраструктури відкритих ключів.

Протокол КЕЦП реалізується в такий спосіб. Кожен користувач формує відкритий ключ виду:

$$y_i = \alpha^{z_i} \cdot mod\ p \tag{2.1}$$

де:

$z_i$ – особистий (секретний) ключ, i = 1, 2, ..., m.

Колективним відкритим ключем є добуток:

$$y = y_1 \cdot y_2 \cdot y_3 \ldots y_m\ mod\ p \tag{2.2}$$

Кожен користувач вибирає разовий випадковий секретний ключ – число $k_i$, потім обчислює $R_i = (\alpha^{k_i} \bmod p) \bmod q$ і надає це значення для колективного використання. Далі обчислюється добуток:

$$R = R_1 \cdot R_2 \cdot R_3 \ldots R_m\ mod\ q \tag{2.3}$$

Потім кожен користувач по визначеній ним значенням $R_i$ і величиною H обчислює свою частину підпису за формулою:

$$S_i = k_i\ H + z_i \cdot R\ mod\ q \tag{2.4}$$

Колективної підписом є пара чисел (R, S), де S обчислюється за формулою:

$$S = S1 + S2 + S3 + \ldots + S_m \bmod q \tag{2.5}$$

Перевірка колективного підпису здійснюється за формулою (1). Якщо R = R', то КЕЦП сукупності m користувачів є справжньою, так як вона могла бути сформована тільки за участю кожного користувача з цієї групи, оскільки для її формування потрібне використання секретного ключа кожного з них. Відзначимо,

що аутентифікація значень $R_i$ здійснюється автоматично при перевірці автентичності колективної ЕЦП. Якщо порушник спробує підмінити будь-яка з цих значень або замінити на раніше використані значення, то факт втручання в протокол буде відразу ж виявлено при перевірці достовірності ЕЦП, тобто буде отримано $R' \neq R$. Очевидно, що розмір КЕЦП не залежить від m.

Покажемо коректність запропонованого алгоритму КЕЦП. Підставивши підпис (R, S), де S та R обчислюються за формулами:

$$S = \sum_{i=1}^{m} S_i \, mod \, q \tag{2.6}$$

та

$$R = \prod_{i=1}^{m} R_i \, mod \, q \tag{2.7}$$

Відповідно до статті 9 Закону України “Про електронний цифровий підпис” ЦСК, акредитований в установленому порядку, є АЦСК. Процедура акредитації, яка здійснюється на добровільних засадах, документально засвідчує компетентність ЦСК здійснювати діяльність, пов’язану з обслуговуванням ПСВК. При цьому АЦСК має виконувати усі зобов’язання та вимоги, встановлені законодавством для ЦСК, та додатково зобов’язаний використовувати для надання послуг ЕЦП надійні засоби ЕЦП. Відповідно до “Порядку застосування електронного цифрового підпису органами державної влади, органами місцевого самоврядування, підприємствами, установами та організаціями державної форми власності” установа, тобто будь-який суб’єкт, зазначений в цьому Порядку, отримує на договірних засадах послуги ЕЦП від АЦСК. При цьому установа може отримувати такі послуги лише від одного АЦСК, а використання підписувачами (працівниками установи) ОК, відповідні ВК яких засвідчені іншими АЦСК, забороняється. На виконання постанови Кабінету Міністрів України “Про затвердження Порядку акредитації центру сертифікації ключів” наказом

Департаменту спеціальних телекомунікаційних систем та захисту інформації Служби безпеки України (його правонаступником є Адміністрація Держспецзв'язку) затверджено "Правила посиленої сертифікації", які визначають організаційні, технічні і технологічні вимоги до АЦСК під час обслуговування ними ПСВК та забезпечення їх використання. Відповідно до зазначеного Порядку та з метою створення умов технологічної сумісності програмно-технічних комплексів АЦСК та засобів ЕЦП спільним наказом Держкомінформнауки та Держспецзв'язку були затверджені "Технічні специфікації форматів представлення базових об'єктів національної системи електронного цифрового підпису", що містять:

- формат підписаних даних;
- протокол фіксування часу;
- протокол визначення статусу ПСВК.

Вимоги цих Технічних специфікацій є обов'язковими для надійних засобів ЕЦП, програмно-технічних комплексів АЦСК. Правильність реалізації наведених форматів у засобах ЕЦП повинна бути підтверджена сертифікатом відповідності або позитивним експертним висновком за результатами державної експертизи у сфері КЗІ. Тип формату ЕЦП обирається залежно від вимог до зберігання підписаних даних. Згідно із законодавством СВК можуть розповсюджуватися в електронній формі або у формі документа на папері та використовуватися для ідентифікації особи підписувача. При цьому ПСВК є СВК, який відповідає вимогам Закону України "Про електронний цифровий підпис", виданий АЦСК, засвідчувальним центром, ЦЗО. Відповідно до статті 8 цього Закону ЦСК зобов'язаний забезпечувати цілодобово доступ користувачів до СВК та відповідних електронних переліків СВК через загальнодоступні телекомунікаційні канали. Користувачі у разі необхідності отримують СВК підписувача з бази даних сертифікатів ЦСК і при цьому перевіряється статус цього СВК (чинний, заблокований, скасований). Перевірка ЕЦП може здійснюватися за допомогою ВК, що міститься у СВК, лише у разі, коли на цей

момент сертифікат є чинним. Схематично процес перевірки ЕЦП зображено на рис. 2.4.

Обов'язкова передача документованої інформації центрів сертифікації ключів Сукупність СВК, які зберігаються АЦСК, відповідні реєстри, та інша документована інформація є головною інформаційною складовою ІВК. За її неповноти коло суб'єктів, що застосовують ЕЦП, буде обмеженим і може звестися лише до корпоративних груп, які самостійно будуть обмінюватися між собою ВК. Для забезпечення захисту прав суб'єктів, які використовують ЕЦП, та стабільного існування ІВК необхідно створити юридичні та організаційні умови, за яких гарантовано буде збережено зазначену інформацію. Відповідно до статті 14 Закону України "Про електронний цифровий підпис" ЦСК припиняє свою діяльність відповідно до законодавства. Про рішення щодо припинення своєї діяльності ЦСК повідомляє підписувачів за три місяці, якщо інші строки не визначено законодавством. При цьому АЦСК додатково повідомляє про рішення щодо припинення діяльності ЦЗО або відповідний засвідчувальний центр і протягом доби, визначеної як дата припинення його діяльності, відповідно до постанови Кабінету Міністрів України "Про затвердження Порядку обов'язкової передачі документованої інформації" передає ПСВК, відповідні реєстри ПСВК та документовану інформацію, яка підлягає обов'язковій передачі, відповідному засвідчувальному центру або ЦЗО.

Розглянемо один з сценаріїв використання КЕП під час роботи лікаря в МІС:

1) лікар заходить до системи під персональним логіном та паролем;
2) для посилення безпеки система запитує КЕП;
3) лікар вносить інформацію до електронної медичної картки на етапах у відповідності до інструкції її заповнення;
4) в разі корректировки даних внесену інформацію завіряє КЕП (алгоритм зображений на рис. 2.4);
5) на час, коли лікарю слід покинути робоче місце, вихід з системи завіряється КЕП;

6) по закінченню робочого дня та відправкою обробленої інформації на сервер виконана робота підтверджується КЕП як самого лікаря, так й завідувача відділенням;
7) щомісячно, під час експертизи медичної документації, електронні медичні картки перевіряються та завіряються КЕП заступників керівника медичного закладу у відповідності до «Системи експертної оцінки» конкретного закладу.

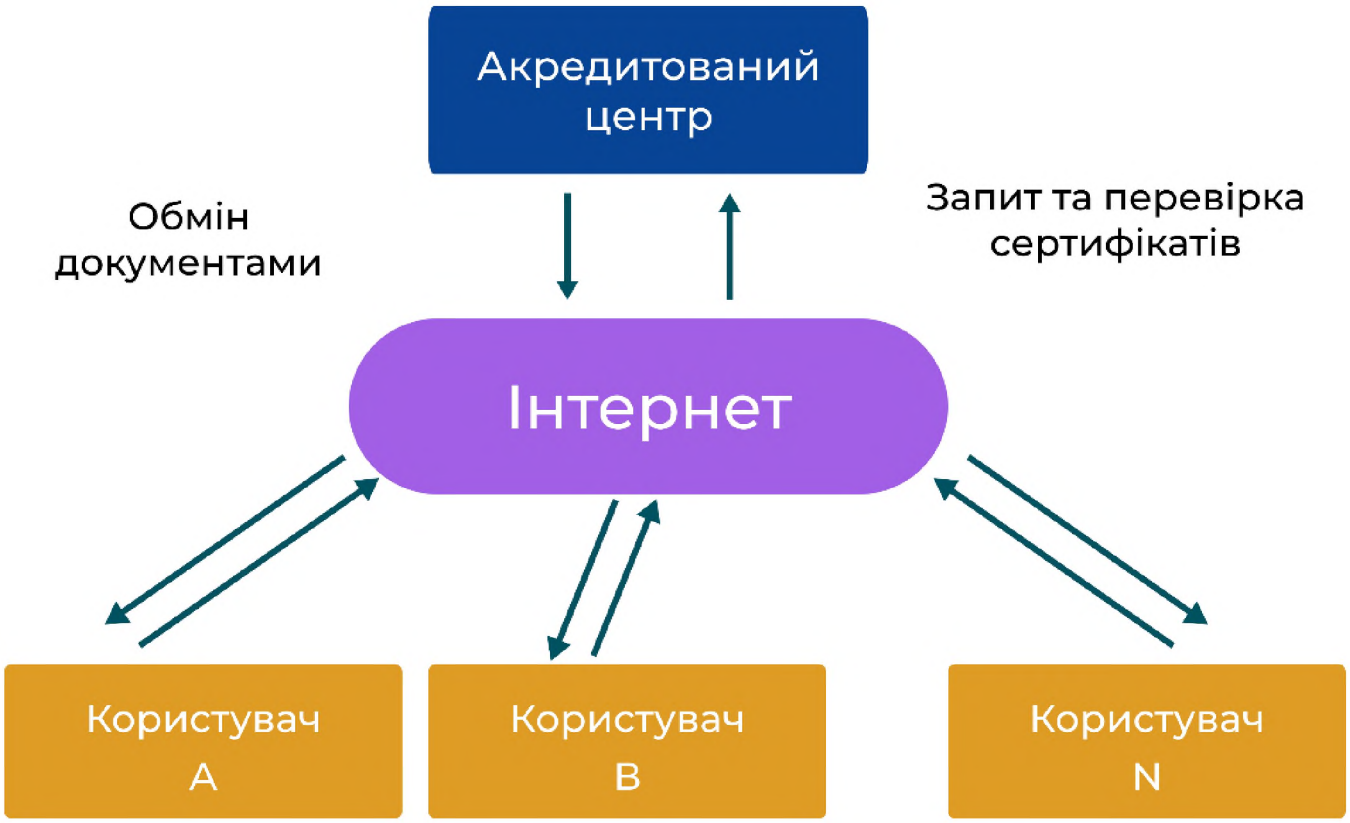


Рисунок 2.4 – Схема процесу перевірки КЕП


Рисунок 2.5 – Механізм накладання КЕП

Перелік подій, що підлягають обов'язковому фіксуванню КЕП при роботі с електронною історією хвороби:

- створення медичної картки;
- внесення паспортної частини;
- записи первинного огляду пацієнта;
- план обстеження та лікування;
- записи про проведенні дослідження, інтервенції, маніпуляції;
- записи щоденників;
- рекомендації після виписки;
- епікриз.

### 2.3.3. Обґрунтування засобів реалізації автентифікації відправника

На даний час в електронних медичних системах в Україні в більшості використовується кваліфікований електронний підпис, який базується на кваліфікованому сертифікаті відкритого ключа. Саме тут ми спостерігаємо вразливість системи захисту: кваліфікований сертифікат відкритого ключа можливо скопіювати на пристрій, що не належить власнику. Таким чином є шлях для неправомірного його використання, в тому числі для неправдивої

коректировки електронних записів. У відповідності до Законну України «Про електронні довірчі послуги» КЕП повинні зберігатись на захищених носіях, токенах. Захищений носій ключової інформації являє собою пристрій, призначений для безпечного зберігання КЕП. По суті це апаратно-програмний засіб КЕП, виконаний у вигляді токена – USB-пристрою (зовні схожого на флешку) або смарт-карти (пластикової картки з чіпом). Особливості захищених носіїв:

- неможливість вилучення КЕП з носія: копіювання, крадіжка або зчитування виключено;
- генерація ключа і всі операції з ним виконуються всередині носія;
- токен захищений паролем доступу із обмеженням на кількість спроб підбору пароля, що захищає ключ від несанкціонованого використання в разі втрати носія;

Генерація КЕП відбувається безпосередньо в токені, ключ існує тільки в єдиному екземплярі. Виключається можливість підміни, кражі та неправомірне використання КЕП

Існують різновидності токенів: активні (інтелектуальні із властивістю переробки інформації) та пасивні (пасивні, наділені функцією зберігання інформації) Переважним аргументом використання токенів в медичній інформаційній системі є можливість та безпека їх використання по відкритій мережі, паролі до них постійно генеруються та змінюються. Основним недоліком токенів є їх висока вартість: їх треба замовляти, забезпечувати співробітників, що працюють в медичній інформаційній системі, відшкодовувати випадки втрати, існує потреба у додатковому придбанні спеціальним пристроїв читання.

### 2.3.4. Дотримання вимог існуючого законодавства у використанні цифрових електронних підписів

Відповідно до пункту 5 розділу VII Закону України ”Про електронні довірчі послуги” користувачі електронних довірчих послуг мать право використовувати електронні цифрові підписи, які підтверджуються з використанням посилених

сертифікатів відкритих ключів та були видані відповідно до вимог Закону України ”Про електронний цифровий підпис» як кваліфіковані електронні підписи до закінчення строку дії посиленого сертифіката відкритого ключа, але не пізніше двох років з дня набрання чинності Закону (тобто до 7 листопада 2020 р.). Зокрема постановою Кабінету Міністрів України від 03 березня 2020 р. №193 (далі — Постанова) зазначається, що до 31 грудня 2021 року реалізується експериментальний проект до дня набрання чинності змінами до Закону щодо забезпечення можливості використання удосконалених електронних підписів і печаток, які базуються на кваліфікованих сертифікатах відкритих ключів та передбачає можливість використання таких засобів. Відповідно до отриманих НСЗУ листів від Адміністрації Держспецзв'язку та Міністерства цифрової трансформації України: лікарі, представники закладів охорони здоров'я та аптек для електронної взаємодії з НСЗУ можуть використовувати електронний цифровий підпис та кваліфікований електронний підпис відповідно до вимог Закону, або удосконалений електронний підпис, який базується на кваліфікованому сертифікаті відкритого ключа згідно з положеннями Постанови.

## 2.4. Методика забезпечення послуги реєстрації подій (HP-2)

Кожен користувач МІС реєструється адміністратором. Користувач, який встановлює систему, автоматично призначається головним адміністратором і має майже всі доступні привілеї. Адміністратор має право створювати, вилучати та корегувати права доступу кожного користувача. Бажано, щоб саме адміністратор вів журнал реєстрації подій МІС. В журнал фіксується дії та інформація про здійснення певної керівники інформації в МІС (початок і завершення сеансу роботи користувачем, спроби несанкціонованого доступу, доступ до конфіденційної інформації тощо) у спеціальних журнальних файлах. Це забезпечує наступність і дозволяє адміністраторові стежити за тим, як дотримується доступ до інформації з боку користувачів, і коригувати на підставі цього параметри конфігурації комплексу засобів захисту.

Послуга реєстрації подій реалізує наступні завдання:

- мотивація користувачів та адміністратора до дотримання етики в роботі в інформаційній системі;
- можливість реконструкції хронології подій, що дає дозвіл на виявлення вразливості в системі захисту, відстеження вторгнення або ненавмисної помилки;
- контроль за спробами порушень безпеки інформації;
- формування звітів для виявлення і аналізу проблем системи захисту.

Ефективне протоколювання передбачає перелік подій, що потрібно протоколювати та ступені їх деталізації.

Події, що підлягають протоколюванню:

- вхід в систему та його результат (успішний чи ні);
- закінчення роботи в системі;
- відправлення запиту до віддаленої системи;
- здійснення маніпуляцій над файлами (відкриття, закриття, перейменування, видалення);
- зміна прав доступу користувачів.

Журнал подій має містити наступну інформацію:

- дата і час події;
- індентифікатор користувача, що спричинив дію;
- вид події;
- вихід дії (успішний чи невдалий);
- джерело запиту (наприклад, ім'я, код комп'ютеру);
- назви файлів, з якими відбувались маніпуляції;
- перелік змін в статусах безпеки об'єктів.

Іноді використовують вибіркове протоколювання щодо певних користувачів, чи їх групи або вибіркових подій.

Реалізація послуги реєстрації подій в медичній інформаційній системі має свої труднощі. Деякі компоненти, важливі для безпеки (наприклад, маршрутизатори), можуть не володіти своїми ресурсами протоколювання, тому їх потрібно екранувати іншими елементами, які можуть реалізувати функції

протоколювання. Необхідно пов'язувати між собою події в різних елементах системи.

Зберігання журналу припускається локально, в хмарному сервісі, в межах України. Інформація журналу повинна синхронізувати із інформацією в МІС: паралельна робота системи протоколювання. Приклад структурі ЕСОЗ з надбудовою над МИС зображена на рис. 2.6.

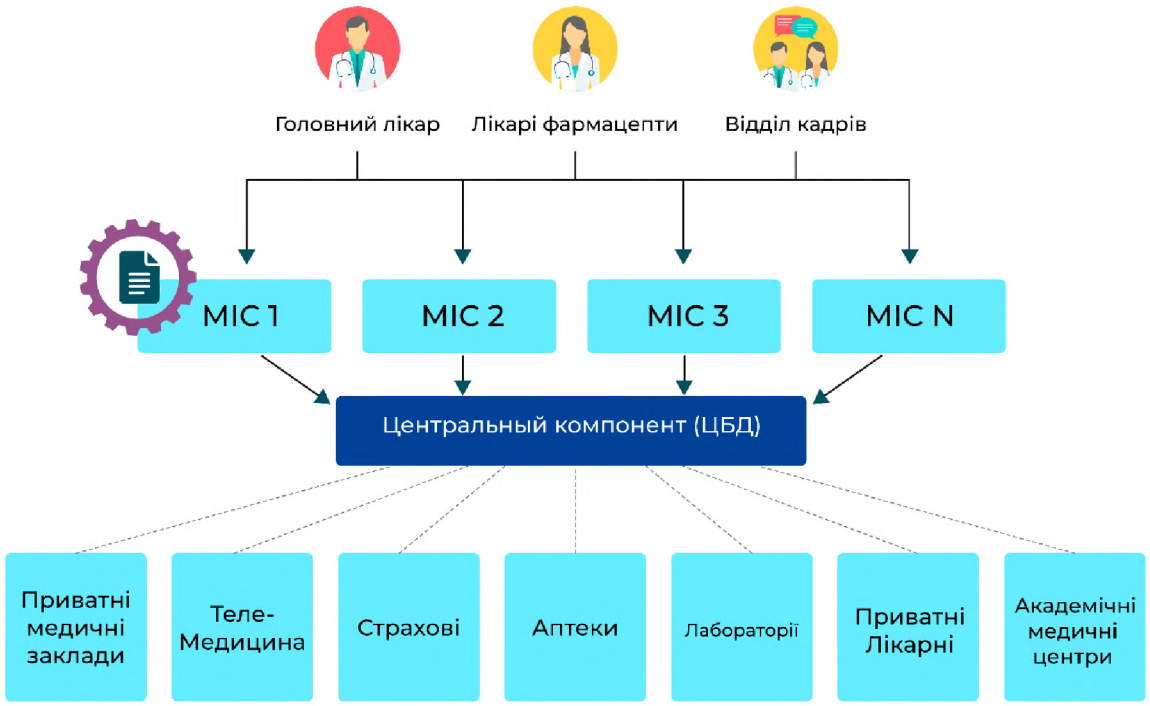


Рисунок 2.5 – Структурна схема ЕСОЗ з надбудовою журналу подій у МІС

Ведення журналу забезпечує користувач з числа керівників медичного закладу (адміністратор), що має окремий обліковий запис, не працює в медичній інформаційній системі, в його функції покладено ведення журналу.

### 2.4.1. Обґрунтування механізму реєстрації подій

Під час роботи МІС повинна фіксувати всі події що відбуваються із інформацією, в тому числі ті, які можуть вплинути на безпеку інформації. Зазначені події зберігаються у відповідних файлах системи. Адміністратор повинен періодично переглядати вказані файли і аналізувати звіти, які в ній

з’являються. В разі виникнення небезпечної чи некоректної події має вжити відповідних заходів.

## 2.5. Основні положення політики безпеки

Політика безпеки регламентує використання основних сервісів мережі і доводить до відома користувачів мережі їхні права доступу, що і є процедурою автентифікації користувачів. До політики інформаційної безпеки об’єкта, як до регламентуючого документу, варто відноситися серйозно, бо всі інші стратегії захисту будуються на припущенні, що правила політики безпеки неухильно дотримуються.

Інформаційну систему об’єкта захисту можна вважати захищеною, якщо всі операції виконуються згідно зі строго визначеними правилами, що забезпечують безпосередній захист об’єктів, ресурсів і операцій. Основу для формування вимог до захисту складає список загроз. Коли такі вимоги відомі, можуть бути визначені відповідні правила забезпечення захисту, що визначають необхідні функції і засоби захисту. Чим суворіші вимоги до захисту і більше відповідних правил, тим ефективніші її механізми і тим більше захищеною виявляється інформаційна система [19].

Аналіз ризику – основна умова, що визначає політику безпеки. Саме аналіз ризику приносить найбільшу кількість інформації про ступень захисту, його вразливість, є підставою для формулювання та прийняття рішень, забезпечує ефективність затрат на системи захисту, спрямовуючи ресурси безпеки на найшкідливіші фактори, а саме на блокування загроз.

Основні епати аналізу ризику:

1) ресурси інформаційної системи: технічні (персональні комп'ютери), програмне забезпечення, інформація, документація, задіяні співробітники;
2) формулювання вразливих місць – з'ясовуються вразливі місця по кожному ресурсу інформаційної системи з ранжуванням витоку загроз;
3) експертиза потенціальних загроз;

4) визначення можливих втрат;
5) розгляд та експертиза методик захисту інформаційної системи;
6) оцінка ефективності прийнятих рішень. У випадку перевищення рівня втрат припустимого порогу приймається рішення про посилення заходів безпеки.

Після проведення аналізу ризику приймається політика безпеки та складається план захисту, що вміщує наступні елементи:

1) початковий стан: стан системи безпеки на момент планування;
2) рекомендательний: обирання засобів захисту для забезпечення політики
3) визначення відповідальності: формулювання переліку користувачів та їх рівні повноважень;
4) графік роботи: періодичне визначення наступності елементів системи захисту та контролю;
5) контроль виконання графіку.

На початковому етапі визначається особа, в обов'язки якої покладається контроль за системою безпеки, так званий адміністратор баз даних.

Основні положення при визначенні відповідальності:

– рішення про політику інформаційної безпеки в медичному закладі приймає адміністрація із документальним підтвердженням;
– функціонування системи безпеки медичної інформаційної системи може бути забезпечено тільки відповідними спеціалістами;
– ефективність заходів безпеки – пріоритет адміністрації медичного закладу.

На адміністратора баз даних медичного закладу покладається створення умов для роботи медичної інформаційної системи, які мінімізують вразливість системи, а саме:

– створення умов для фізичного захисту комп'ютерних систем;
– визначення регламенту технологічних процесів;

- визначення регламенту роботи із інформацією, що містить конфіденційні дані;
- забезпечення регламенту процедур резервування бази даних;
- ведення журналу подій;
- визначення регламенту роботи користувачів медичної інформаційної системи;
- навчання персоналу роботі в медичній інформаційній системі;
- забезпечення заходів контролю за ефективністю системи безпеки. Застосовуються до подібних ситуацій;

Політика безпеки об'єкта повинна мати процедури для взаємодії з зовнішніми організаціями, в число яких входять правоохоронні органи, інші організації, команди "швидкого реагування", засоби масової інформації. У процедурах повинно бути визначено, хто має право на такі контакти, і як саме вони відбуваються.

Крім політичних положень, необхідно продумати й описати процедури, що виконуються у випадку виявлення порушень режиму безпеки. Для всіх видів порушень мають бути заготовлені відповідні процедури.

## 2.6. Висновки

В результаті проведеного дослідження, було запропоноване до розробки рішення, яке дозволить збільшити рівень безпеки медичної інформаційної системи шляхом впровадження журналу реєстрації дій. Запропоноване рішення дає можливість контролю за діями користувачів системи, попередження навмисних чи ненавмисних ушкоджень цілісності інформації. Додавання зазначеної послуги безпеки відповідає сучасним потребам медичної галузі, коли в окремих випадках для надання медичної допомоги, медичні працівники мають доступ до інформації, що не відноситься до їх функцій, але зміни в цій інформації чи запит на неї можливо відстежити та попередити незаконні маніпуляції.

Головним аргументом на користь розробки такого рішення є безпека даних громадян України та покращення аспектів безпеки інформації в медичної галузі

країни загалом. Можливі недоліки впровадження журналу реєстрації дій мають різні шляхи вирішення.

Обов'язковою умовою є оцінка можливих збитків у випадку витоку даних. До того ж значним ризиком є можливе зловживання медичним персоналом закладів охорони здоров'я, які на сьогодні отримують дані про пацієнтів у необмеженому обсязі. Доки із розвитком реформування охорони здоров'я України йде робота над удосконаленням законодавства з питань захисту персональних даних громадян, технічні засоби захисту інформації в медичних інформаційних системах тим часом зможуть частково вирішувати питання збереження даних.

# 3. ЕКОНОМІЧНА ЧАСТИНА

Метою розділу є обґрунтування економічної доцільності розробки та впровадження в роботу МІС журналу реєстрації подій. Журнал реєстрації дій, як система, що слід впроваджувати в роботу МІС, вимагає використання ресурсів як часового, людського, так і фінансового. Оцінити ефективність можливих витрат можна шляхом порівняння можливих витрат на розробку підсистеми з можливими втратами, які зазнають власники інформації – система ЕСОЗ, а також безпосередньо особи, чиї персональні дані зазнали витоку. Також, треба розрахувати вартість підтримки такого рішення у майбутньому, відносно зростаючої кількості даних та ймовірну їх цінність.

У зв'язку з особливостями роботи підприємств з розробки програмного забезпечення, усі використані грошові одиниці конвертовані з доларів США до української гривні за курсом НБУ 09 грудня 2020 р. і дорівнює 2809 грн за 100 доларів США.

## 3.1. Основні положення політики безпеки

Першочергово, розрахуємо показник необхідного часу для розробки запропонованого програмного рішення. Для цього використовується формула для оцінки трудомісткості, яка визначається тривалістю кожної робочої операції, починаючи з складання технічного завдання і закінчуючи оформленням документації:

$$t = t_{тз} + t_{в} + t_{а} + t_{пр} + t_{опр} + t_{тст} + t_{д}, \text{ годин} \quad (3.1)$$

у якій:

$t_{тз}$ – тривалість розробки технічної документації, дизайну системи та алгоритмів;

$t_{в}$ – тривалість вивчення ТЗ, літературних джерел за темою, відвідування зборів з обговорень завдання;

$t_{а}$ – тривалість розробки блок-схеми алгоритму;

$t_{пр}$ – тривалість програмування за готовою блок-схемою;

$t_{опр}$ – тривалість опрацювання програми на ПК;

$t_д$ – тривалість написання тестів покриття розробленого функціоналу, розробка технічної документації.

Необхідне для обчислень значення складової трудомісткості визначаються за формулою 3.2, на підставі умовної кількості операторів у програмному продукті Q:

$$Q = q \cdot c\,(1 + p), \quad \text{штук}, \tag{3.2}$$

у якій:

Коефіцієнт складності рекомендацій с визначає відносну складність рекомендації щодо типового завдання, складність якого дорівнює одиниці. Діапазон його зміни – 1,25…2,0. Коефіцієнт корекції рекомендацій р береться з діапазону 0,05...0,1, що відповідає внесенню 3...5 корекцій і переробці 5-10% готової програми.

Розрахуємо цей показник для розробки даного рішення за наступними даними: с = 1,5, р = 0,07. Також припустимо, що для початкової розробки нам необхідно 40 осіб, серед яких: 3 менеджера, 3 аналітика, 22 розробника та додані до них архітектор ПЗ та системний адміністратор, а також 10 тестувальників. Окремо розрахуємо значення для кожної підгрупи:

$$Q_м = Q_а = 3 \cdot 1{,}5(1 + 0{,}05) = 4 \text{ штуки};$$

$$Q_п = 24 \cdot 1{,}5(1 + 0{,}05) = 37 \text{ штук};$$

$$Q_т = 10 \cdot 1{,}5(1 + 0{,}05) = 15 \text{ штук}.$$

$$Q = Qм + Qа + Qп + Qт = 60 \text{ штук}.$$

Оцінимо тривалість складання технічного завдання на розробку рішення $t_{тз.}$ у 96 годин.

Тривалість вивчення технічного завдання, опрацювання довідкової літератури з урахуванням уточнення ТЗ і кваліфікацію виконавця оцінюється за формулою:

$$t_в = \frac{Q \cdot B}{(75...85) \cdot k}, \text{ годин}, \tag{3.3}$$

у якій:

В – коефіцієнт збільшення тривалості етапу внаслідок недостатнього опису завдання. В = 1,2...1,5;

k – коефіцієнт, що враховує кваліфікацію виконавця і визначається стажем роботи за фахом.

Для даної розробки: В = 1,3; k = 1. Виходячи з цього тривалість вивчення технічного завдання для усіх груп дорівнює:

$$t_в = \frac{60 \cdot 1,3}{78 \cdot 1,1} = 0,9 \text{ годин},$$

тривалість розробки блок-схеми алгоритму, приймають участь аналітики та окрема частина розробників більш вищого рівня (0,1-0,2 від загальної команди), а також планування процесів менеджерським складом:

$$ta = \frac{Q}{(20...25) \cdot k}, \text{ годин}, \quad (3.4)$$

$$t_а = t_м = \frac{4}{20 \cdot 1,1} = 0,18 \text{ годин},$$

$$t_р = \frac{6}{20 \cdot 1,1} = 0,27 \text{ години},$$

тривалість створення програми за готовою блок-схемою та написанню тестових сценаріїв:

$$t_{пр,\,р} = \frac{37}{20 \cdot 1,1} = 1,68 \text{ годин},$$

$$t_{пр,\,т} = \frac{15}{20 \cdot 1,1} = 0,68 \text{ години},$$

тривалість опрацювання програми на ПК та тестування функціоналу:

$$tonp = \frac{1,5Q}{(4...5) \cdot k}, \text{ годин}, \quad (3.5)$$

$$t_{опр,\,р} = \frac{1,5 \cdot 37}{20 \cdot 1,1} = 2,52 \text{ години},$$

$$t_{опр,\,т} = \frac{1,5 \cdot 15}{20 \cdot 1,1} = 1,02 \text{ години},$$

тривалість підготовки технічної документації та додаткових відомостей:

$$t_д = \frac{Q}{(15...20) \cdot k} + \frac{Q}{(15...20)} \cdot 0,75 \text{ годин}, \quad (3.6)$$

$$t_{д,р} = \frac{37}{16 \cdot 1,1} + \frac{37}{16} \cdot 0,75 = 3,83 \text{ години};$$

$$t_{д,т} = \frac{15}{16 \cdot 1,1} + \frac{15}{16} \cdot 0,75 = 1,55 \text{ годин};$$

$$t_{д,а} = t_{д,м} = \frac{4}{16 \cdot 1,1} + \frac{4}{16} \cdot 0,75 = 0,22 \text{ години};$$

Виходячи з отриманих даних трудомісткість створення обґрунтованих рекомендацій дорівнює:

$$t_а = t_м = 0,22 + 0,18 = 0,4 \text{ години}$$

$$t_т = 1,55 + 1,02 + 0,68 = 3,25 \text{ годин}$$

$$t_р = 3,83 + 2,52 + 1,68 + 1,27 = 9,3 \text{ години}$$

$$t = t_а + t_м + t_р + t_т = 96 + 0,4 + 3,25 + 9,3 + 0,4 = 109,35 \text{ годин}$$

## 3.2. Розрахунок витрат на створення програмного продукту

Витрати на створення програмного продукту $К_{пз}$ складаються з витрат на заробітну плату виконавця програмного забезпечення $З_{зп}$ і вартості витрат машинного часу, що необхідний для опрацювання програми на ПК $З_{мч}$:

$$К_{пз} = З_{зп} + З_{мч} . \quad (3.7)$$

Заробітна плата виконавця враховує основну і додаткову заробітну плату, а також відрахування на соціальне потреби, визначається за формулою:

$$З_{зп} = З_{пр} \cdot t, \text{ грн}, \quad (3.8)$$

у якій:

t – загальна тривалість створення ПЗ, годин;

$З_{пр}$ – средньогодинна заробітна плата програміста з нарахуваннями, грн/годину.

Згідно до визначених технологій, які будуть застосовуватися до розробки, а також умову, що розробка відбувається у межах України, середньогодинну заробітну плату програміста розрахуємо за формулою:

$$Зпр = \frac{Зсм}{20 \cdot t_{дн}}, \text{ грн}, \quad (3.9)$$

у якій:

$t_{дн}$ – нормована тривалість робочої доби;

$З_{см}$ – средньомісячна заробітна плата співробітника з нарахуваннями, грн/годину

Згідно до статті 60 КЗоП, нормована тривалість робочого часу працівників не може перевищувати 40 годин на тиждень [20]. Тому визначаємо $t_{дн}$ = 8 годин. Згідно до відкритих даних з провідного ІТ ресурсу України, отримаємо середньою заробітну платню кожного співробітника [21].

У зв'язку з тим, що ми маємо додаткову градацію заробітних плат всередині кожної групи, додатково розрахуємо середню заробітну платню групи:

$$З_{с,а} = \frac{2 \cdot 1500 + 2200 + 3400}{4} \cdot 23{,}6 = 50{,}740 \text{ тис.грн}$$

$$З_{с,м} = \frac{2 \cdot 1000 + 1500 + 3000}{4} \cdot 23{,}6 = 38{,}350 \text{ тис.грн}$$

$$З_{с,р} = \frac{14 \cdot 817 + 14 \cdot 1800 + 5 \cdot 3100 + 3 \cdot 4000 + \cdot 4400}{37} \cdot 23{,}6 = 43{,}716 \text{ тис.грн}$$

$$З_{с,т} = \frac{7 \cdot 680 + 7 \cdot 1365 + 3000}{15} \cdot 23{,}6 = 27{,}242 \text{ тис.грн}$$

Середньогодинна заробітна плата:

$$З_{пр,\,а} = \frac{50740}{20 \cdot 8}, \text{ грн} = 317 \text{ грн}$$

$$З_{пр,\,м} = \frac{38350}{20 \cdot 8}, \text{ грн} = 239{,}7 \text{ грн}$$

$$З_{пр,\,р} = \frac{43716}{20 \cdot 8}, \text{ грн} = 273{,}2 \text{ грн}$$

$$З_{пр,\,т} = \frac{27242}{20 \cdot 8}, \text{ грн} = 170{,}2 \text{ грн}$$

$$З_{пр} = \frac{170{,}2 + 273{,}2 + 239{,}7 + 317}{4} = 250 \text{ грн}$$

Середня заробітна плата виконавця становить:

$$З_{зп,а} = 317 * 109{,}35 = 34{,}663 \text{ тис.грн}$$

$$З_{зп,м} = 239{,}7 * 109{,}35 = 26{,}211 \text{ тис.грн}$$

$$З_{зп,р} = 273{,}2 * 109{,}35 = 29{,}848 \text{ тис.грн}$$

$$З_{зп,т} = 170,2 * 109,35 = 18,611 \text{ тис.грн}$$

$$З_{зп} = \frac{Ззп,м + Ззп,р + Ззп,а + Ззп,т}{4} = 27,335 \text{ тис.грн}$$

Вартість машинного часу для налагодження програми на ПК визначається за формулою:

$$З_{мч} = С_{мч} \cdot t, \text{ грн}, \quad (3.11)$$

у якій:

$t_{опр}$ – трудомісткість налагодження програми на ПК, годин;

$t_д$ – трудомісткість підготовки документації на ПК, годин;

$С_{мч}$ – вартість 1 години машинного часу ПК, грн./година.

В свою чергу, вартість 1 години машинного часу ПК визначається за формулою:

$$Смч = P \cdot t_{нал} \cdot Се + \frac{Ф_{зал} \cdot На}{F_р} + \frac{К_{лпз} \cdot На_{пз}}{F_р}, \text{ грн}, \quad (3.12)$$

у якій:

Р – встановлена потужність ПК, кВт. Р = 1,5 кВт;

$С_е$ – тариф на електричну енергію, грн/кВт·година. $С_е$ = 1,68 грн/кВт·година;

$Ф_{зал}$ – залишкова вартість ПК на поточний рік, грн.;

$Н_а$ – річна норма амортизації на ПК, частки одиниці;

$Н_{апз}$ – річна норма амортизації на ліцензійне програмне забезпечення, частки одиниці;

$К_{лпз}$ – вартість ліцензійного програмного забезпечення, грн.;

$F_р$ – річний фонд робочого часу; $F_р$ = 1993 для 40-годинного робочого тижня.

Мінімально допустимий строк корисного використання $Т_а$ ПК складає 3 роки, тобто річна норма амортизації не має перевищувати:

$$Н_а = \frac{1}{Т_а} \cdot 100\% \quad (3.13)$$

$$Н_а = \frac{1}{Т_а} \cdot 100\% = 33,3\%$$

Строк дії права користування ліцензійним програмним забезпеченням не може складати менш ніж 1 рік, в такому випадку, $Н_{апз}$ не має перевищувати 100%.

Визначимо залишкову вартість одного ПК $Ф_{зал}$ як середньою вартість наданих розробникам пристроїв, які зазначені у таблиці 3.1

Таблиця 3.1 – Специфікація комп'ютерів

| Кількість пристроїв | Назва пристрою | Специфікація | Вартість за пристрій |
|---|---|---|---|
| 6 | MacBook Pro 13 | Процесор Apple M1, відеокарта AMD Radeon Pro 5300M, оперативна пам’ять 8GB DDR4, жорсткий диск SSD 512 GB | 57,000 тис. грн |
| 14 | Lenovo ThinkPad Z680 | Процесор Intel Core i7-9550U, оперативна пам’ять 16 ГБ DDR4, жорский диск SSD 256 GB | 26,237 тис. грн |
| 40 | ПК | Процесор Intel Core i5, відеокарта GTX 950, оперативна пам’ять HP 8 GB DDR4, жорсткий диск SSD 512 GB, додаткова периферія | 43,000 тис. грн |
| **Загальна вартість** | | | 2,429,318 млн.грн |

Таким чином, середня балансова вартість ПК на кінець 2020 року становить 40,488 тис. грн. Загальна вартість $К_{аз.}$ становить 2,429,318 грн. Вартість ліцензійного програмного забезпечення на один рік вираховується як загальна вартість таких ліцензій, які визначені у таблиці 3.2.

Таблиця 3.2 – Вартість ліцензійного програмного забезпечення

| Назва програмного забезпечення | Вартість на перший рік, тис. грн (за одну ліцензію, грн) | Вартість на другий рік, тис. грн (за одну ліцензію, грн) |
|---|---|---|
| ReSharper Professional | 173,766 (4694) | 138,838 (3752) |
| Windows 10 Corporate license | 254,880 (4720) | 254,880 (4720) |
| Office 365 corporate licence | 212,400 (3540) | 212,400 (3540) |
| **Загальна вартість** | 641,046 тис.грн | 467,418 тис.грн |

Таким чином, загальна вартість ліцензійного програмного забезпечення $К_{ппз}$ дорівнюється 641,046 тис. грн. Окремо для розробників – 37 · 4694 + 31 · 4720 + 37 · 3540 = 450,978 тис.грн

Отримавши усі необхідні дані, розрахуємо вартість 1 години машинного часу пристроїв для окремих користувачів:

$$Смч,р = 1,5 \cdot 1,68 + \frac{40488 \cdot 0,33}{1993} + \frac{450978 \cdot 1}{1993} = 244,35 \text{ грн}$$

$$Смч,т,а,м = 1,5 \cdot 1,68 + \frac{40488 \cdot 0,33}{1993} + \frac{190068 \cdot 1}{1993} = 4 \cdot 108,47 = 433,88 \text{грн}$$

$$Смч = \frac{Смч,р + Смч,т,а,м}{2} = 339,1 \text{грн}$$

Вартість машинного часу для користувачів:

$$З_{мч,т,а,м} = 108,4 \cdot 1,02 + 1,55 = 4 \cdot 112,18 = 448,72 \text{ грн}$$

$$З_{мч,р} = 244,35 \cdot 2,52 + 3,83 = 619,6 \text{ грн}$$

$$Змч = \frac{448,72 + 619,6}{2} = 534,16 \text{ грн}$$

Капітальні (фіксовані) витрати на проектування та впровадження проектного варіанта системи інформаційної безпеки визначають за формулою:

$$К = К_{пр} + К_{зпз} + К_{пз} + К_{аз} + К_{н}, \qquad (3.14)$$

у якій:

$К_{пр}$ – вартість розробки проекту інформаційної безпеки та залучення для цього зовнішніх консультантів, 25,000 тис. грн;

$К_{зпз}$ – вартість закупівель ліцензійного основного й додаткового програмного забезпечення (ПЗ), тис. грн; $К_{зпз}$ = 641,046 тис. грн

$К_{пз}$ – вартість створення основного й додаткового програмного забезпечення, тис. грн;

$К_{аз}$ – вартість закупівлі апаратного забезпечення та допоміжних матеріалів, млн. грн; $К_{аз}$ = 2429318;

$К_{н}$ – витрати на встановлення обладнання та налагодження системи інформаційної безпеки, тис. грн; $К_{н}$ = 30 тис. грн

Визначемо, що $К_{пз}$ = 27335 + 534,16 = 27,869 тис. грн. Таким чином, капітальні фіксовані витрати на проектування та впровадження запропонованого рішення упродовж 1 року складає:

$$К = 25000 + 641046 + 2429318 + 27849 + 30000 = 3153213 \text{ грн}$$

## 3.3. Розрахунок експлуатаційних витрат

Річні експлуатаційні витрати на функціонування системи складають:

$$С = С_{в} + С_{к} + С_{ак}, \quad \text{тис. грн} \qquad (3.15)$$

у якій:

$С_{в}$ - витрати на оновлення системи;

$С_{к}$ - витрати на керування системою.

Витрати на керування системою ($С_{к}$) складають:

$$Ск = Са + Сз + Сєв + Сел + Стос, \text{ грн} \qquad (3.16)$$

у якій:

$С_{а}$ - річний фонд амортизаційних відрахувань;

$С_{з}$ - річний фонд заробітної плати інженерно-технічного персоналу;

$С_{ел}$ - вартість електроенергії, що споживається апаратурою;

$С_{тос}$ - витрати на технічне й організаційне адміністрування;

$С_{єв} = С_з \cdot 0,22$

Річний фонд амортизаційних відрахувань визначається у відсотках від суми капітальних інвестицій, і дорівнює:

$$С_{а,аз} = \frac{2429318}{3} = 809772 \text{ грн.}$$

$$С_{а,пз} = \frac{641046}{3} = 213682 \text{ грн.}$$

$$С_а = 1023454 \text{ грн.}$$

Річний фонд заробітної плати інженерно-технічного персоналу, що обслуговує систему інформаційної безпеки ($С_з$), складає:

$$С_з = З_{осн} + З_{дод} \text{ , грн} \qquad (3.17)$$

де $З_{осн}$, $З_{дод}$ – основна і додаткова заробітна плата відповідно, грн на рік.

Основна заробітна плата визначається, виходячи з місячного посадового окладу, а додаткова заробітна плата – в розмірі 22% від основної заробітної плати.

$$С_з = 27335 \cdot 12 + (27335 \cdot 0,22) \cdot 12 = 400184,4 \text{ , грн.}$$

Вартість електроенергії, що споживається апаратурою системою інформаційної безпеки протягом року ($С_е$), визначається за формулою:

$$С_{ел} = Р \cdot F_р \cdot Ц_е \text{ , грн,} \qquad (3.18)$$

У якій:

Р – встановлена потужність апаратури; 1,2 кВт·годину;

$F_р$ – річний фонд робочого часу системи 1993;

$Ц_е$ – тариф на електроенергію - 1,68 грн/кВт·годину.

$$С_{ел} = 1,2 \cdot 1993 \cdot 1,55 = 3706,98$$

Витрати на технічне й організаційне адміністрування та сервіс системи інформаційної безпеки ($С_{тос}$) визначається за даними організації або у відсотках від вартості капітальних витрат (1-3%). $С_{тос} = 70000$ грн.

Також, додамо витрати на оренду хмарних сервісів для розміщення підсистеми у розмірі 250000 грн.

$$С_k = 70000 + 4017,8 + 1023454 + 360882 + 79394 + 250000 =$$

= 1787748 грн.

C = 1787748 + 233709 + 1214659 = 3236116 грн

## 3.4. Оцінка величини можливого збитку

Визначимо загальний збиток внаслідок витоку інформації щодо медичних записів за формулою 3.19:

$$B = n*A*R \quad (3.19)$$

де n – кількість медичних записів в одній МІС, що зазнали ураження

A – відшкодування за скомпрометований запис однієї особи; A = 17000 грн (1000 неоподаткованих мінімумів)

У зазначеній в роботі МІС станом на листопад 2020 року обробляються 22 тисячі медичних записів. Враховуючи те, що зазначена система працює в дослідженому закладі охорони здоров'я лише чотири місяці, припустимо, що в рік буде оброблятись понад 100 тисяч записів. Розглянемо варіант витоку медичних записів за причини внутрішніх чинників , що складають 25%, 100 тисяч записів про 1 тисячу пацієнтів, коли кожному необхідно компенсувати це у обсязі 1000 неоподаткованих мінімумів після витоку даних закладу охорони здоров'я.

B = 1000· 17000*0,25 = 4250000 грн

Загальний ефект від впровадження підсистеми розраховується за формулою (3.20):

$$E = B - C, \quad (3.20)$$

Загальний ефект від впровадження в роботу МІС журналу реєстрації подій:

E = 4250000 – 3236116 = 1013884 грн.

## 3.5 Аналіз показників економічної ефективності впровадження в роботу МІС журналу реєстрації подій

Економічна ефективність впровадження підсистеми інформаційної безпеки визначається за допомогою коефіцієнту повернення інвестицій та терміну окупності.

Коефіцієнт повернення інвестицій визначається за наступною формулою:

$$ROSI = \frac{E}{K}, \text{ частки одиниці,} \quad (3.21)$$

де Е – загальний ефект від впровадження підсистеми

К – капітальні інвестиції за варіантами, що забезпечили цей ефект, тис. грн.

Отже, коефіцієнт повернення інвестицій становить:

$$\text{ROSI} = \frac{1013884}{3153213} = 0{,}32$$

Термін окупності капітальних інвестицій То показує, за скільки років капітальні інвестиції окупляться за рахунок загального ефекту від впровадження підсистеми розмежування доступу:

$$T_O = \frac{K}{E} = \frac{1}{ROSI}, \text{ років.} \quad (3.22)$$

Термін окупності складає:

$$T_o = 3{,}125 \text{ років}$$

## 3.6 Висновок за економічним розділом

В результаті проведеного економічного аналізу, розробка та впровадження в існуючу МІС додатково журналу реєстрації дій дозволить уникнути величезних витрат, що було продемонстровано на прикладі однієї МІС, яка містить дані однієї тисячі користувачів при одноразовому витоку даних у розмірі 100 тисяч записів. Збитки на виплати компенсацій постраждалим від витоку медичних даних в сотні разів більші за необхідні витрати на розробку журналу реєстрації подій та його реалізацію в межах діючої МІС.

Отриманий термін окупності системи лише відносно одного випадку дорівнює 1,42 років демонструє доцільність розробки такого рішення, особливо якщо такі випадки будуть повторюватися або кількість пошкоджених записів буде збільшуватися. Капітальні затрати дорівнюють 3153213 грн, а загальна трудомісткість дорівнює 109,35 годин. Саме цих витрат необхідно для досягнення загального економічного ефекту у більш ніж 1 мільйони гривень.

# ВИСНОВКИ

Під час виконання кваліфікаційної роботи відбувся ретельний аналіз функціонування медичної інформаційної системи, відповідності ведення електронної медичної картки існуючим нормам законодавства. Як визначилось під час аналізу, доступ до електронної медичної картки не обмежено колом фахівців, що приймають участь у наданні медичної послуги, інформація медичної картки доступна великій кількості користувачів, що сприяє можливості неадекватної корекції даних чи їх витоку.

Рішення цієї проблеми пропонується шляхом розробки та впровадження в роботу медичної інформаційної системи журналу реєстрації дій. Його метою є попередження зловживань медичних працівників в використанні медичної інформації. Також, в зазначену опцію було закладена можливість впровадження в роботу медичної інформаційної системи без порушень її теперішніх функцій та конфігурацій. Рекомендованим варіантом розміщення журналу було обране розташування в хмарному сховищі на території України. Доступ до інформації журналу реєстрації дій має користувач, в обов'язки якого входить ведення цього журналу, аналіз та надання пропозицій для покращення комплексу системи безпеки.

Економічними розрахунками була обґрунтована доцільність розробки журналу. Дивлячись на те, що станом на сьогодні в розглянутій медичній інформаційній системі оброблено понад 22 тисячі медичних записів про біля тисячі пацієнтів, можна припустити обсяги витоку інформації при подальшому збільшенні масиву даних. Відносно цього, розробка журналу реєстрації подій, який частково вирішує велику ваду системи, потребує набагато менше витрат, в той час як одержуваний ефект позитивно позначається не тільки на безпеці даних, але і на рівні розвитку медичної галузі країни загалом.

# ПЕРЕЛІК ПОСИЛАНЬ

1. Число витоків з медичних установ за 2019, (Електрон. ресурс) / Спосіб доступу: URL: https://www.infowatch.ru/analytics/digest/15414

2. КОВАЛЕНКО Л.П., Інформаційно-правове регулювання документованої інформації, (Електрон. ресурс) / Спосіб доступу: URL: http://ippi.org.ua/sites/default/files/13klprdi.pdf

3. Терешко Христина Ярославівна УДК 347.15/.17:614.256 Дисертація Іінформація як об'єкт цивільних правовідносин у сфері медичного обслуговування, (Електрон. ресурс) / Спосіб доступу: URL: http://idpnan.org.ua/files/2019/tereshko-h.ya.-informatsiya-yak-ob_ekt-tsivilnih-pravovidnosin-u-sferi-medichnogo-obslugovuvannya_a_.rtf

4. Стратегія розвитку медичної освіти, (Електрон. ресурс) / Спосіб доступу: URL: https://moz.gov.ua/strategija

5. Електронна система охорони здоров'я отримала атестат відповідності КСЗІ, (Електрон. ресурс) / Спосіб доступу: URL: https://www.kmu.gov.ua/news/elektronna-sistema-ohoroni-zdorovya-otrimala-atestat-vidpovidnosti-kszi-derzhavnim-vimogam-zahistu-informaciyi

6. Електронна медична карта пацієнта. Взаємосумісність та стандартизація / В. О. Качмар, А. І. Хвищун. Укр. журнал телемедицини та медичної телематики. – 2008. – № 1, т. 6. – С. 76–79.

7. Статистика ведення електронних медичних записів в ЕСОЗ, (Електрон. ресурс) / Спосіб доступу: URL: https://nszu.gov.ua/e-data/dashboard/emz-stats

8. Як і для чого НСЗУ верифікує дані в електронній системі охорони здоров'я, (Електрон. ресурс) / Спосіб доступу: URL: https://nszu.gov.ua/novini/yak-i-dlya-chogo-nszu-verifikuye-dani-v-elektronnij-sistemi-24

9. Підключені до eHealth Медичні Інформаційні Системи, (Електрон. ресурс) / Спосіб доступу: URL: https://ehealth.gov.ua/pidklyucheni-do-ehealth-mis

10 Кваліфікаційної роботи ступеню магістра спеціальності 125м Кібербезпека Овєчкіна А.В. за темою "Підсистема контролю доступу в електронній системі охорони здоров'я «eHealth»"

11. Про організацію клініко-експертної оцінки якості надання медичної допомоги та медичного обслуговування, (Електрон. ресурс) / Спосіб доступу: URL: https://zakon.rada.gov.ua/laws/show/z0285-16#Text

12. Інструкція щодо заповнення форми первинної облікової документації № 003/о "Медична карта стаціонарного хворого №____", (Електрон. ресурс) / Спосіб доступу: URL: https://zakon.rada.gov.ua/laws/show/z0662-12#Text

13. Алгоритми і технології забезпечення безпеки інформації в медичній інформаційній системі, (Електрон. ресурс) / Спосіб доступу: URL: http://www.swsys.ru/index.php?page=article&id=3404

14. Удосконалені методи автентифікації в системах обміну миттєвими повідомленнями, (Електрон. ресурс) / Спосіб доступу: URL: https://ela.kpi.ua/bitstream/123456789/27191/1/Lobanov_magistr.pdf

15. Про електронний цифровий підпис, (Електрон. ресурс) / Спосіб доступу: URL: https://zakon.rada.gov.ua/laws/show/852-15#Text

16. Криптографічні засоби захисту інформації, (Електрон. ресурс) / Спосіб доступу: URL:http://infosecmd.narod.ru/gl5.html

17. НАЦІОНАЛЬНА СЛУЖБА ЗДОРОВ'Я УКРАЇНИ НАКАЗ від 30.09.2019 р. № 385 «Про внесення змін до наказу Національної служби здоров'я України від 06.02.2019 р. № 28», (Електрон. ресурс) / Спосіб доступу: URL: https://www.apteka.ua/article/517396

18. Реалізація протоколу колективних підписів основі стандартів ЕЦП, (Електрон. ресурс) / Спосіб доступу: URL: https://cyberleninka.ru/article/n/realizatsiya-protokola-kollektivnoy-podpisina-osnove-standartov-etsp/viewer

19. Політика інформаційної безпеки об'єкта, (Електрон. ресурс) / Спосіб доступу: URL: https://ela.kpi.ua/bitstream/123456789/8581/1/24_p23.pdf

26. Використання блокчейн технологій у електронних медичних системах, (Електрон. ресурс) / Спосіб доступу: URL: https://blockgeeks.com/guides/blockchain-in-healthcare/

27. Перелік ролей та довзолів у ЦБД, (Електрон. ресурс) / Спосіб доступу: URL: edenlab.atlassian.net/wiki/spaces/EH/pages/2004415/Scopes+model

# ДОДАТОК А. ВІДОМІСТЬ МАТЕРІАЛІВ КВАЛІФІКАЦІЙНОЇ РОБОТИ

Таблиця А.1 – Перелік матеріалів кваліфікаційної роботи

| № | Формат | Найменування | Кількість листів | Примітки |
|---|---|---|---|---|
| 1 | А4 | Реферат | 3 | |
| 2 | А4 | Список умовних скорочень | 1 | |
| 3 | А4 | Зміст | 2 | |
| 4 | А4 | Вступ | 1 | |
| 5 | А4 | Стан питання. Постановка задачі | 21 | |
| 6 | А4 | Спеціальна частина | 33 | |
| 7 | А4 | Економічний розділ | 12 | |
| 8 | А4 | Висновки | 1 | |
| 9 | А4 | Перелік посилань | 2 | |
| 10 | А4 | Додаток А | 1 | |
| 11 | А4 | Додаток Б | 7 | |
| 12 | А4 | Додаток В | 1 | |
| 13 | А4 | Додаток Г | 1 | |
| 14 | А4 | Додаток Д | 2 | |

# ДОДАТОК Б. ВІДОМІСТЬ МАТЕРІАЛІВ КВАЛІФІКАЦІЙНОЇ РОБОТИ

Таблиця Б.1 – Перелік матеріалів кваліфікаційної роботи

| Пункт Інструкції* | Вміст пункту (цитування) | Забезпечення в МІС |
|---|---|---|
| 5 | У пунктах 1-9 форми № 003/о зазначаються дата (число, місяць, рік) та час (години, хвилини) госпіталізації, прізвище, ім'я, по батькові хворого, стать (чоловіча, жіноча), дата народження (число, місяць, рік), вік (кількість повних років, для дітей: до 1-го року - місяців; до 1-го місяця - днів), назва та номер документа, що посвідчує особу, код країни, громадянином якої є хворий. місце роботи, посада (для дітей, учнів, студентів - найменування навчального закладу; для інвалідів - вид і група інвалідності), найменування та код закладу охорони здоров'я, який направляє хворого до стаціонару. Зазначені пункти заповнюються медичним працівником у приймальному відділенні закладу охорони здоров'я. | Забезпечено повністю |
| 6 | У пункті 10 вказуються діагноз при госпіталізації та код захворювання згідно з Міжнародною статистичною класифікацією хвороб та споріднених проблем охорони здоров'я Десятого перегляду (далі - МКХ-10). | Забезпечено повністю |
| 7 | У пунктах 11, 12 вказуються коди відділень закладів охорони здоров'я при госпіталізації та при виписці відповідно до додатка до форми | Забезпечено повністю |

| | | |
|---|---|---|
| | первинної облікової документації № 066/о «Карта пацієнта, який вибув із стаціонару, № __», затвердженої наказом Міністерства охорони здоров'я України від 14 лютого 2012 року № 110, зареєстрованим в Міністерстві юстиції України 28 квітня 2012 року за № 661/20974 (у редакції наказу Міністерства охорони здоров'я України від 21 січня 2016 року № 29) (далі - форма № 066/о). | |
| 8 | У пункті 13 зазначається вид госпіталізації: ургентна - 1; планова - 2. | Забезпечено повністю |
| 9 | У пунктах 14-17 зазначаються дата (число, місяць, рік) обстеження на ВІЛ-інфекцію, група крові хворого, резус-приналежність, дата (число, місяць, рік) проведення реакції Вассермана. | Забезпечено повністю |
| 10 | Пункт 18 містить інформацію щодо алергічних реакцій, гіперчутливості чи непереносимості лікарського засобу (вказуються назва лікарського засобу, характер побічної дії). | Забезпечено повністю |
| 11 | У пункті 19 зазначається госпіталізація з приводу цього захворювання в цьому році: вперше - 1; повторно - 2. | Забезпечено повністю |
| 12 | У пункті 20 зазначаються дата (число, місяць, рік) та час (година) виписки/смерті хворого. | Забезпечено повністю |
| 13 | У пункті 21 вказується кількість проведених хворим у закладі охорони здоров'я ліжко-днів (день госпіталізації і день виписки/смерті рахуються як один день). | Не виконується |

| | | |
|---|---|---|
| 14 | Пункт 22 містить інформацію щодо заключного клінічного діагнозу хворого при виписці/смерті (у випадку травми зазначається її вид: виробнича - 1; невиробнича - 2). За наявності у хворого ускладнень основного діагнозу або супутніх захворювань лікуючий лікар зазначає їх після основного діагнозу: ускладнення основного діагнозу - 1; супутні захворювання - 2 та проставляє відповідні коди згідно з МКХ-10. | Забезпечено повністю |
| 15 | У пункті 23 (якщо хворому проводились хірургічні втручання або процедури) вказуються дата (число, місяць, рік), тривалість проведення (кількість годин, хвилин), код і назва процедури/хірургічної | Забезпечується повністю |
| 16 | У пункті 24 вказуються інші види медичного лікування для онкологічних хворих: спеціальне, паліативне, симптоматичне. | Не виконується |
| 17 | У пунктах 25, 26 зазначаються дані щодо тимчасової непрацездатності хворого. | Забезпечено повністю |
| 18 | У пункті 27 вказується висновок для хворих, які потребують проведення медико-соціальної експертизи. | Забезпечено частково |
| 19 | У пункті 28 зазначається результат медичного лікування хворого: виписаний(а) з: одужанням - 1; поліпшенням - 2; погіршенням - 3; без змін - 4; помер(ла) - 5; переведений(а) до іншого закладу охорони здоров'я - 6; здоровий(а) - 7. | Забезпечено частково |
| 20 | пункті 29 зазначаються дати (число, місяць, | Забезпечено |

| | | |
|---|---|---|
| | рік) проведення профілактичного медичного огляду на наявність злоякісного новоутворення (онкологічний профілактичний огляд) та профілактичного медичного огляду на виявлення туберкульозу (обстеження органів грудної порожнини) за період стаціонарного лікування. | частково |
| 21 | У пункті 30 ставляться відмітки щодо страхування хворого (наявність та номер страхового поліса, найменування компанії-страхувальника). | Забезпечено частково |
| 22 | У пунктах 10-30 всі записи здійснює лікуючий лікар. Після цього у пункті 31 він зазначає свої прізвище, ім'я, по батькові, підпис і реєстраційний номер. | Не виконується |
| 23 | У пункті 32 завідувач відділення зазначає свої прізвище, ім'я, по батькові, підпис та реєстраційний номер. | Не виконується |
| 24 | Пункти 33-39 заповнює лікар приймального відділення.<br>У пункті 33 зазначаються скарги хворого.<br>У пунктах 34-36 стисло вказуються дані анамнезу хвороби та життя, об'єктивний стан хворого.<br>Пункти 37, 38 містять інформацію щодо оглядів на коросту та педикульоз.<br>У пункті 39 відмічається, чи ознайомлений хворий із режимом дня та забороною паління, зазначаються дата (число, місяць, рік) | Забезпечено частково |

| | | |
|---|---|---|
| | ознайомлення та підпис хворого.<br>У пункті 40 лікар приймального відділення проставляє свої прізвище, ім'я, по батькові, підпис та реєстраційний номер. | |
| 25 | У пункті 41 лікуючий лікар зазначає скарги пацієнта, анамнез хвороби, анамнез життя, об'єктивний стан хворого, попередній діагноз, план обстеження та план медичного лікування. | Забезпечено повністю |
| 26 | У пункті 42 відмічаються результати обстежень (лабораторні, ультразвукові, рентгенологічні, функціональна діагностика тощо). | Забезпечено частково |
| 27 | У пункті 43 лікар здійснює записи про стан здоров'я та медичного лікування хворого або щогодини, або щодня, або щотижня залежно від стану хворого та місця його перебування Щоденникові записи засвідчуються підписом лікуючого лікаря.<br>У період перебування хворого в стаціонарі форма № 003/о зберігається у лікуючого лікаря. | Забезпечено частково |
| 28 | Призначення лікуючого лікаря записуються у щоденнику Записи ведуться розбірливо, чітко, детально із зазначенням дат призначення та відміни лікарських засобів і засвідчуються підписом лікуючого лікаря. | Забезпечено частково |
| 29 | У пункті 44 зазначаються результати оглядів та консультацій хворого лікарями-спеціалістами. | Забезпечено повністю |
| 30 | У пункті 45 при виписці хворого лікуючий | Забезпечено |

| | | |
|---|---|---|
| | лікар складає виписний епікриз, у якому коротко резюмує дані про стан хворого при госпіталізації та виписці. | повністю |
| 31 | У пунктах 46-53 зазначаються результати клінічних аналізів | Забезпечено повністю |
| 32 | У пунктах 54, 55 вказуються заключний клінічний діагноз, проведені обстеження та лікувальні заходи, аналізується їх ефективність. | Забезпечено частково |
| 33 | У пункті 56 лікуючий лікар зазначає подальші лікувальні рекомендації та режим хворого. | Забезпечено повністю |
| 34 | У пункті 57 вказується результат медичного лікування хворого. | Забезпечено повністю |
| 35 | У пунктах 58-64 у разі смерті хворого лікар-патологоанатом після розтину заповнює виписку з протоколу (карти) патологоанатомічного обстеження. | Забезпечено повністю |
| 36 | У пункті 65 здійснюється запис згідно, у якому зазначаються патологічні стани, що призвели до безпосередньої причини смерті. | Забезпечено повністю |
| 37 | У пунктах 66, 67 лікар-патологоанатом і завідувач патологоанатомічного відділення зазначають свої прізвища, імена, по батькові, підписи та реєстраційні номери. | Не виконується |
| 38 | На підставі даних форми № 003/о лікуючий лікар заповнює форму № 066/о, після чого форма № 003/о передається в кабінет статистики для обробки, а потім до архіву закладу охорони здоров’я | Забезпечено частково |

| | | |
|---|---|---|
| 39 | У разі ведення форми № 003/о в електронному форматі вона повинна включати в себе всі дані, які містяться на паперовому носії інформації. | Забезпечено частково |
| 40 | Строк зберігання форми № 003/о - 25 років. | Передбачено |

*Пункт Інструкції щодо заповнення форми первинної облікової документації № 003/о “Медична карта стаціонарного хворого № __”(ЗАТВЕРДЖЕНО Наказ Міністерства охорони здоров’я України 14.02.2012 № 110 (у редакції наказу Міністерства охорони здоров’я України 21.01.2016 № 29)

# ДОДАТОК В. ПЕРЕЛІК ДОКУМЕНТІВ НА ОПТИЧНОМУ НОСІЇ

1. Пояснювальна записка Донченко. І. В.docx
2. Презентація Донченко. І. В.pptx

## ДОДАТОК Г. ВІДГУК КЕРІВНИКА ЕКОНОМІЧНОГО РОЗДІЛУ

Відгук керівника економічного розділу:

Керівник розділу _____ _____
(підпис) (ініціали, прізвище)

# ДОДАТОК Д. ВІДГУК КЕРІВНИКА КВАЛІФІКАЦІЙНОЇ РОБОТИ

Відгук
на кваліфікаційну роботу магістра на тему:
«Методика реєстрації дій над інформацією, що потребує захисту в медичних інформаційних системах»
студента групи 125м-19-1
Донченка Іллі Вікторовича

Мета роботи – забезпечення спостереженості за діями користувачів в електронній системі охорони здоров'я.

Тема роботи безпосередньо пов'язана з об'єктом діяльності фахівця за спеціальністю 125 Кібербезпека – розвиток методик реєстрації дій користувачів в автоматизованих системах.

Задачі роботи (аналіз основних законодавчих та нормативних актів, що регламентують захист інформації в медичних системах, аналіз актуальних загроз, аналіз структури електронної системи охорони здоров'я, формування та формалізація вимог до розробки, обґрунтування вибору методів та засобів реалізації запропонованих рішень, адаптація протоколів електронного цифрового підпису) віднесені в освітньо-кваліфікаційній характеристиці магістра до класу евристичних, вирішення яких основане на знаково-розумових уміннях фахівця.

Оригінальність технічних рішень полягає у розробці уніфікованого підходу, без втручання в роботу вже існуючих елементів системи розмежування доступу.

Практичне значення результатів проектування полягає в можливості забезпечення вимог чинних нормативних документів, щодо ведення документації в медичних закладах. Слід заначити, що робота виконувалась на базі реального медичного закладу

До недоліків дипломної роботи відносяться:

– недостатньо обґрунтовано вибір протоколу ЕЦП;
– недостатньо обґрунтовано функції адміністратора журналу подій;
– не в повному обсязі представлена політика безпеки;
– відсутність апробації та практичної перевірки ефективності запропонованих рішень.

Оформлення пояснювальної записки до дипломного проекту виконано з деякими відхиленнями від стандартів.

Рівень запозичень у кваліфікаційній роботі не перевищує вимог положення про систему виявлення та запобіганню плагіату.

Ступінь самостійності виконання дипломної роботи висока.

За час дипломування Донченко І.В. виявив себе фахівцем, здатним самостійно, на достатньо високому рівні вирішувати поставлені задачі.

В цілому кваліфікаційна робота виконана у відповідності до вимог, що ставляться до кваліфікаційної роботи магістра, заслуговує оцінки “добре”, а Донченко І.В. присвоєння йому кваліфікації магістр з кібербезпеки, освітньо-професійна програма «Кібербезпека».

Керівник спеціальної частини
дипломної роботи магістра,
старший викладач _____ О.В. Кручінін

Керівник дипломної
роботи магістра,
д.т.н., професор _____ В.І. Корнієнко