МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
СХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ ІМ. В. ДАЛЯ
ФАКУЛЬТЕТ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ ТА ЕЛЕКТРОНІКИ
КАФЕДРА КОМП'ЮТЕРНИХ НАУК ТА ІНЖЕНЕРІЇ

До захисту допускається
Т.в.о. завідувача кафедри
_____ Сафонова С.О.
«____»_____ 2020 р.

МАГІСТЕРСЬКА РОБОТА

НА ТЕМУ:

Методи підвищення захисту персональних даних в медичних інформаційних системах

Освітньо-кваліфікаційний рівень "Магістр"
Спеціальність 123 – "Комп'ютерна інженерія"

Науковий керівник роботи:	_____ (підпис)	Деркач М.В. (ініціали, прізвище)
Консультант з охорони праці:	_____ (підпис)	Критська Я.О. (ініціали, прізвище)
Студент:	_____ (підпис)	Газіна Д.І. (ініціали, прізвище)
Група:		КІ-18дм

Сєвєродонецьк 2020

МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
СХІДНОУКРАЇНСЬКИЙ НАЦІОНАЛЬНИЙ УНІВЕРСИТЕТ
ІМЕНІ ВОЛОДИМИРА ДАЛЯ

Факультет Інформаційних технологій та електроніки
Кафедра Комп'ютерних наук та інженерії
Освітньо-кваліфікаційний рівень магістр
Напрям підготовки _____
(шифр і назва)
Спеціальність 123 – "Комп'ютерна інженерія"
(шифр і назва)

ЗАТВЕРДЖУЮ:

Т.в.о. завідувача кафедри

_____С.О. Сафонова
«_____» _____2020 р.

З А В Д А Н Н Я
НА МАГІСТЕРСЬКУ РОБОТУ СТУДЕНТУ

Газіній Дар'ї Ігорівні
(прізвище, ім'я, по батькові)

1. Тема роботи Методи підвищення захисту персональних даних в медичних інформаційних системах

керівник проекту(роботи) к.т.н., ст. викл. Деркач М.В.
(прізвище, ім'я, по батькові, науковий ступінь, вчене звання)
затверджені наказом вищого навчального закладу від "11" 10 2019 р. № 135/15.15
2. Строк подання студентом роботи 16.01.2020 р.
3. Вихідні дані до роботи матеріали переддипломної практики

4. Зміст розрахунково-пояснювальної записки (перелік питань, які потрібно розробити) Функціональні можливості МІС. Дослідження сучасних засобів захисту ПДн в МІС. Практичне дослідження ефективності запропонованого метода підвищення захисту ПДн в МІС. Охорона праці та безпека в надзвичайних ситуаціях.
5. Перелік графічного матеріалу (з точним зазначенням обов'язкових креслень) електронні плакати

6. Консультанти розділів проекту (роботи)

Розділ	Прізвище, ініціали та посада консультанта	Підпис, дата	
		завдання видав	завдання прийняв
Охорона праці та безпеки в надзвичайних ситуаціях	ст. викл. Критська Я.О.		

7. Дата видачі завдання 02.09.2019 р.

Керівник _____
(підпис)

Завдання прийняв до виконання _____
(підпис)

КАЛЕНДАРНИЙ ПЛАН

№ з/п	Назва етапів дипломного проекту (роботи)	Строк виконання етапів проекту (роботи)	Примітка
1	Отримання завдання, збір матеріалів	02.09.19- 04.10.19	
2	Огляд літератури й обґрунтування необхідності дослідження	05.10.19 –23.10.19	
3	Аналіз сучасних апаратних, програмних та криптографічних засобів захисту ПДн	24.10.19 – 24.11.19	
4	Розробка технології підвищення захисту ПДн в МІС	11.11.19 –20.11.19	
5	Формування комплексного підходу до забезпечення захисту ПДн та медичних ПДн з урахуванням виявлених недоліків	03.12.20 – 10.12.20	
6	Дослідження ефективності розробленого підходу	12.12.20 – 13.12.20	
7	Оформлення пояснювальної записки	14.12.20 – 08.01.20	
8	Підготовка та подання магістерської роботи до захисту	09.01.20 – 16.01.20	

Студент _____ Газіна Д.І.
(підпис) (прізвище та ініціали)

Науковий керівник _____ Деркач М.В.
(підпис) (прізвище та ініціали)

АНОТАЦІЯ

Газіна Д.І. Методи підвищення захисту персональних даних в медичних інформаційних системах.

Розглянуто концептуальну модель побудови медичних інформаційних систем, методи та засоби захисту інформації в медичних інформаційних системах. Запропоновано технологію підвищення захисту персональних і медичних персональних даних. Розроблено комплексне рішення, завдяки якому є можливість уникнути використання додаткових апаратних витрат, збільшити швидкість шифрування/дешифрування даних, підвищити криптографічний захист.

Ключові слова: медична інформаційна система, персональні дані, медичні персональні дані, методи та засоби захисту інформації, криптографічні алгоритми.

АННОТАЦИЯ

Газина Д.И. Методы повышения защиты персональных данных в медицинских информационных системах.

Рассмотрено концептуальную модель построения медицинских информационных систем, методы и средства защиты информации в медицинских информационных системах. Предложена технология повышения защиты персональных и медицинских персональных данных. Разработано комплексное решение, благодаря которому есть возможность избежать использования дополнительных аппаратных затрат и увеличить скорость шифрования/дешифрования данных, повысить криптографическую защиту.

Ключевые слова: медицинская информационная система, персональные данные, медицинские персональные данные, методы и средства защиты информации, криптографические алгоритмы.

ABSTRACT

Hazina D.I. Methods for enhancing the protection of personal data in medical information systems.

The conceptual model of construction of medical information systems, methods and means of information protection in medical information systems is considered. The technology of increasing protection of personal and medical personal data is proposed. A comprehensive solution has been developed to avoid the use of additional hardware costs, increase the speed of data encryption/decryption, and increase cryptographic security.

Keywords: medical information system, personal data, medical personal data, methods and means of information protection, cryptographic algorithms.

ЗМІСТ

СКОРОЧЕННЯ ТА УМОВНІ ПОЗНАКИ

АЗ	Апаратні засоби
АРМ	Автоматизоване робоче місце
БД	База даних
ДССЗЗІ	Державна служба спеціального зв’язку та захисту інформації
ЕЦП	Електронний цифровий підпис
ІБ	Інформаційна безпека
ІС	Інформаційна система
ІТ	Інформаційні технології
КЗІ	Криптографічний захист інформації
КСЗІ	Комплексна система захисту інформації
ЛПЗ	Лікувально-профілактичний заклад
МІС	Медична інформаційна система
МОЗ	Міністерство охорони здоров’я України
НСД	Несанкціонований доступ
НСЗУ	Національна служба здоров’я України
ОС	Операційна система
ПДн	Персональні дані
ПЗ	Програмне забезпечення
ПК	Персональний комп’ютер
СКБД	Система керування базами даних
ЦП	Цифровий підпис

ВСТУП

Актуальність теми. З розвитком процесів інформатизації суспільства, створенням нових, інтеграцією існуючих інформаційних систем, орієнтованих на обслуговування населення, все більша увага приділяється організації обробки персональних даних (ПДн). ПДн складають важливу частину інформаційного простору, що містить відомості про фізичних осіб – суб'єктів ПДн. Виділення таких даних в категорію, що захищається спеціальним чином, обумовлено особливими вимогами до організації їх обробки (діям з ПДн), пов'язаними з можливістю нанесення шкоди суб'єктам ПДн. Тому, як в зарубіжних країнах, так і в Україні розвивається і вдосконалюється законодавча база, яка регламентує правила збору, обробки ПДн і реалізацію прав громадян на конфіденційність відносно їх особистої інформації.

Особлива увага приділяється питанням захисту ПДн в медичних інформаційних системах (МІС). Вимоги до захисту конфіденційних даних в МІС, відповідно до низки документів, враховують категорію і кількість ПДн, специфіку вирішуваних завдань і ряд інших показників. Виконання цих вимог, як правило, пов'язано з істотними фінансовими витратами, та технічною складністю, що викликано необхідністю побудови комплексної системи захисту інформації (КСЗІ), отриманням сертифікату Державної служби спеціального зв'язку, та захисту інформації України (ДССЗЗІ), та подальшим впровадженням такої системи.

У зв'язку з цим представляють інтерес дослідження спрямовані на аналіз і розробку методів підвищення захисту ПДн, що дозволяють знизити витрати на забезпечення безпеки в МІС.

Для реалізації цього підходу потрібно розробити комплексне рішення, та технологію підвищення захисту ПДн.

Своєчасність заданого напрямку досліджень обумовлена зростаючою потребою в побудові КСЗІ при впровадженні різних державних програм щодо автоматизації процесів в медичних закладах, посиленням відповідальності за забезпечення безпеки ПДн і необхідністю, в зв'язку з цим, підвищувати ефективність створюваних систем при одночасному зниженні витрат на їх експлуатацію, що можливо при наявності досить універсального підходу.

Значний внесок у розвиток криптографічних методів захисту інформації внесли такі відомі вчені, як Бєльшев Д.В., Гаріф'янов Д.М., Гольдберг Д.Л., Гулієв Я.І., Євсєєв С.П., Істратова О.О., Тарнавський Ю.А.

Переважна більшість досліджень, присвячена загальним питанням концепції МІС, їх класифікації, основним аспектам функціонування та властивостям цього класу систем. Існуючі програмні аналоги мають ряд недоліків, пов'язаних з великими витратами щодо впровадження та подальшої експлуатації КСЗІ.

Мета і задачі дослідження. Метою роботи є дослідження та вибір підходів, методів і технічних засобів підвищення захисту ПДн в МІС. Для досягнення поставленої мети передбачається вирішення таких задач:

– аналітичний огляд нормативно-правової бази, наукових публікацій з тематики роботи;

– дослідження проблем щодо забезпечення надійності та безпеки ПДн;

– аналіз сучасних апаратних, програмних та криптографічних засобів захисту ПДн;

– розгляд методів та засобів захисту ПДн в МІС;

– розробка технології підвищення захисту ПДн в МІС;

– формування комплексного підходу до забезпечення захисту ПДн та медичних ПДн з урахуванням виявлених недоліків;

– дослідження ефективності розробленого підходу.

Об'єкт дослідження – комплекс апаратно-програмних засобів захисту ПДн в МІС.

Предмет дослідження – медичні ПДн в МІС.

Методи дослідження визначалися специфікою вирішуваних завдань і поставленою метою. В роботі використовувалися методи криптографічного захисту інформації, апаратні і програмні засоби (ПЗ) побудови КСЗІ при проектуванні МІС.

Наукова новизна одержаних результатів пов'язана з розробкою комплексного апаратно-програмного рішення побудови МІС в лікувально-профілактичному закладі (ЛПЗ) на основі запропонованої технології, яка дозволяє підвищити рівень захисту ПДн в МІС, шляхом збільшення циклів шифрування даних і зменшення вартості обладнання при проектуванні та побудові КСЗІ.

Практичне значення одержаних результатів полягає в тому, що на основі проведених теоретичних досліджень та відповідних розрахунків:

– запропоновано технологію підвищення захисту ПДн в МІС;

– розроблено комплексний апаратно-програмний підхід до організації захисту інформації в МІС на основі запропонованої технології;

– отримано експериментальні оцінки ефективності розробленого підходу та методів.

Особистий внесок здобувача. Усі результати магістерської роботи, що виносяться на захист, отримані автором самостійно.

Апробація результатів. Основні результати магістерської атестаційної роботи докладалися на IX Всеукраїнській науково-практичній конференції «ЕЛЕКТРОНІКА ТА ТЕЛЕКОМУНІКАЦІЇ», XXII Міжнародній науково-технічній конференції «ТЕХНОЛОГІЯ-2019» (м. Сєвєродонецьк), «ІТ-Ідея» (Сєвєродонецьк, 2019).

Публікації. Основні результати магістерської атестаційної роботи опубліковано в 3 наукових працях, серед яких 3 тези доповідей.

Структура та обсяг роботи. Магістерська робота складається зі вступу, чотирьох розділів, загальних висновків, додатків, списку використаних літературних джерел, а також має 77 сторінок основного тексту, 11 рисунків, 14 таблиць, 6 сторінок додатків. Список використаних джерел містить 46 найменування і займає 5 сторінок. Загальний обсяг роботи − 88 сторінки.

1 ФУНКЦІОНАЛЬНІ МОЖЛИВОСТІ МІС

1.1 Теоретичні та нормативно-правові аспекти захисту ПДн

З масовим впровадженням комп'ютерів в усі сфери діяльності людини, обсяг інформації, що зберігається в електронному вигляді, виріс в багато разів. Під впливом інформатизації всі сфери життя суспільства стають більш гнучкими та динамічними. Однак, одночасно з цим, зростає і потенційна вразливість суспільних процесів від інформаційного впливу. У зв'язку з масовою інформатизацією сучасного суспільства все більшої актуальності набуває знання морально-етичних норм і правових основ використання засобів нових інформаційних технологій (ІТ) у повсякденній практичній діяльності.

Особливо актуальна проблема інформаційної безпеки (ІБ) в сферах діяльності, де доступ до інформації законодавчо обмежується або забороняється до поширення. Інформація обмеженого доступу поділяється на відомості, які становлять: державну таємницю, комерційну таємницю, службову таємницю, професійну таємницю, а також ПДн громадян.

Забезпечення безпеки і конфіденційності даних є одним з найважливіших питань в сучасних інформаційних системах (ІС) і його вирішення в інформаційно-комунікаційних, обчислювальних системах є актуальною вимогою. В даний час сформульовано три базові принципи ІБ, завданням якої є забезпечення:

- цілісності інформації;
- конфіденційності інформації;
- доступності інформації.

Визначення понять конфіденційність, цілісність та доступність дається в указі «Про Положення про технічний захист інформації в Україні» [1]:

Порушення хоча б однієї з трьох складових призводить до порушення ІБ в цілому. Так, порушення доступності ускладнює (робить неможливим) доступ до інформації, порушення цілісності призводить до фальсифікації інформації і, нарешті, порушення конфіденційності призводить до розкриття інформації. Дана тенденція стосується і системи охорони здоров'я.

Однією з найважливіших сфер життя сучасного суспільства є система охорони здоров'я, роль якої – забезпечувати гарантії прав людини і суспільства на збереження, охорону і відновлення здоров'я, що є не тільки умовою існування окремої особистості, а й метою суспільного розвитку. Система охорони здоров'я охоплює всі відомчі і галузеві

рівні економіки держави, являє собою не тільки сукупність ЛПЗ, а і тісно пов'язана з екологією, охороною праці, соціальними програмами і т. п.

Система охорони здоров'я сприймається, як невід'ємна складова рівня і якості життя, зокрема, грає найважливішу роль в економічному розвитку держави, що забезпечує відтворення і якість трудових ресурсів та створює базу для соціально-економічного зростання.

На сьогоднішній день, медичні організації кожного дня накопичують і обробляють величезні обсяги даних. Від того, наскільки ефективно ця інформація використовується лікарями та керівниками цих закладів, залежить якість медичної допомоги, загальний рівень життя населення, рівень розвитку країни в цілому і кожного її територіального суб'єкта зокрема. Тому необхідність використання великих, і при цьому постійно зростаючих обсягів інформації при вирішенні діагностичних, терапевтичних, статистичних, управлінських та інших завдань, обумовлює створення МІС в медичних закладах.

На рис. 1.1 наведено концептуальну модель побудови МІС.

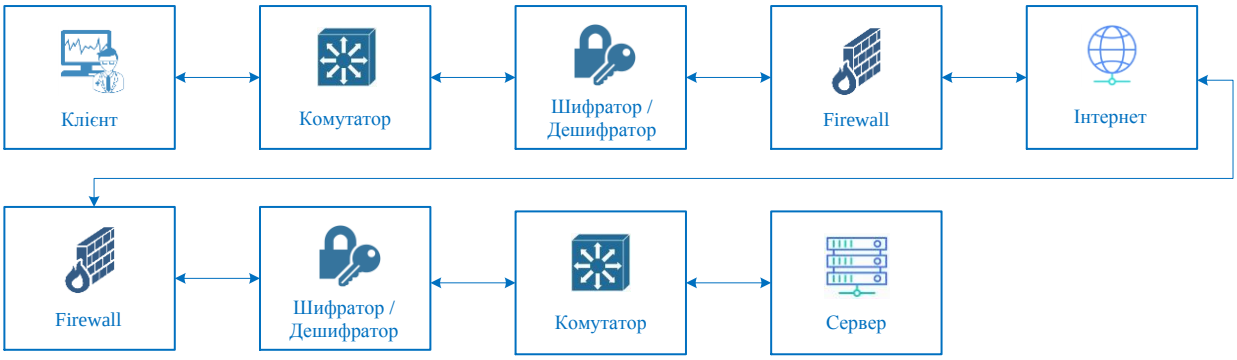

Рисунок 1.1 – Концептуальна модель побудови МІС в ЛПЗ

До недавнього часу ефективність медичного обслуговування в Україні була дуже низькою. В системі охорони здоров'я України майже повністю були відсутні ознаки автоматизації. Медичні карти, історії хвороби, результати обстеження здоров'я, адміністративні звіти, облік пацієнтів та лікарських препаратів – весь документообіг проводився на папері. Це позначалося на швидкості, а отже, і якості обслуговування пацієнтів, ускладнювало роботу лікарського, медичного персоналу, що призводило до лікарських помилок, суттєвої втрати робочого часу на заповнення карт, складання звітів. Це ускладнювало процес керівництва ЛПЗ, так як був відсутній контроль роботи підрозділів, і нестача інформації, як необхідної в поточний момент, так і тієї, яка потрібна для аналізу діяльності установи.

Серйозність і гострота проблеми потребували від органів державної влади прийняття конкретних заходів щодо її врегулювання. Внаслідок чого, уряд розробив Концепцію розвитку системи охорони здоров'я в Україні до 2020 року. В основі цієї Концепції є Реформа Міністерства охорони здоров'я України, яка стартувала в 2018 році і вже дала результати – в структурі галузі відбуваються істотні зміни. Надалі, ті медичні організації, які не готові до них, ризикують не тільки втратити нові можливості, але й відмовитися від значної частини сьогоднішніх стратегічних планів.

Вона розрахована на три роки (2018-2020 роки) і проходить в три етапи. Перший етап трансформації в охороні здоров'я розпочалася з первинної ланки медицини. На цьому рівні до 90% проблем з хворим вирішуються сімейним лікарем. Кожен пацієнт самостійно обирає собі сімейного лікаря та укладає з ним декларацію про медичне обслуговування, а лікар в свою чергу реєструє цю декларацію в системі. Наступний етап – вторинна ланка із поступовим переходом до третинної ланки (спеціалізована та високоспеціалізована допомога).

Не менш важливо, що медична реформа є причиною принципової зміни структури системи охорони здоров'я в Україні, схеми її фінансування і механізмів управління ефективністю. Однією з найважливіших цілей проведеного в даний час реформування системи охорони здоров'я є адаптація цієї галузі до умов ринкових відносин, що розвиваються в усіх сферах соціально-економічного життя суспільства.

Це обумовлює необхідність розробки і впровадження нових організаційних, інформаційних та інших технологій, спрямованих на якнайшвидше проведення реформи, розвиток сучасних форм і методів управління в новій економічній і медико-соціальній ситуації. Особливого значення набуває впровадження в медичну галузь нових інформаційних технологій.

Таким чином, інформаційні технології одночасно з вдосконаленням законодавства дозволили розробити і представити єдину електронну систему охорони здоров'я «E-Health» (рис. 1.1). Згідно Постанови Кабінету Міністрів України від 25.04.2018 р. №411 «Деякі питання електронної системи охорони здоров'я» [2] було затверджено Порядок функціонування електронної системи охорони здоров'я. Система «E-Health» в загальному розумінні є сукупністю інформаційних сервісів в галузі охорони здоров'я, яка забезпечує обмін надійною медичною аналітичною інформацією про пацієнта між керівниками і працівниками різного рівня. «E-Health» охоплює інформаційних простір різних галузей охорони здоров'я – медичну практику, управління медичними закладами, медичне право, фармацевтику, інформаційні сервіси для пацієнтів тощо. Система являє собою сервер бази

даних (БД) та локальних користувачів, які об’єднані в локальну мережу, та дозволяє автоматизоване ведення медичної документації.

Пацієнти мають можливість реєстрації користувачів у центральній БД, використовуючи засоби електронної ідентифікації, можливість створення, внесення, перегляду та обміну деклараціями про вибір лікаря, який надає первину медичну допомогу, рецептами, направленнями, медичними записами, іншою інформацією та документами через електронні кабінети відповідно до прав доступу користувачів, можливість укладення, зміни та припинення договорів про медичне обслуговування населення за програмою державних гарантій медичного обслуговування населення, формування та подання електронних звітів, первинних, розрахункових, та інших документів за договорами через центральну БД. Завдяки повноцінній оптимізації та автоматизації доступу до даних, зростає швидкість прийняття рішень та контроль їх виконання, що якісно покращує лікувальний процес.

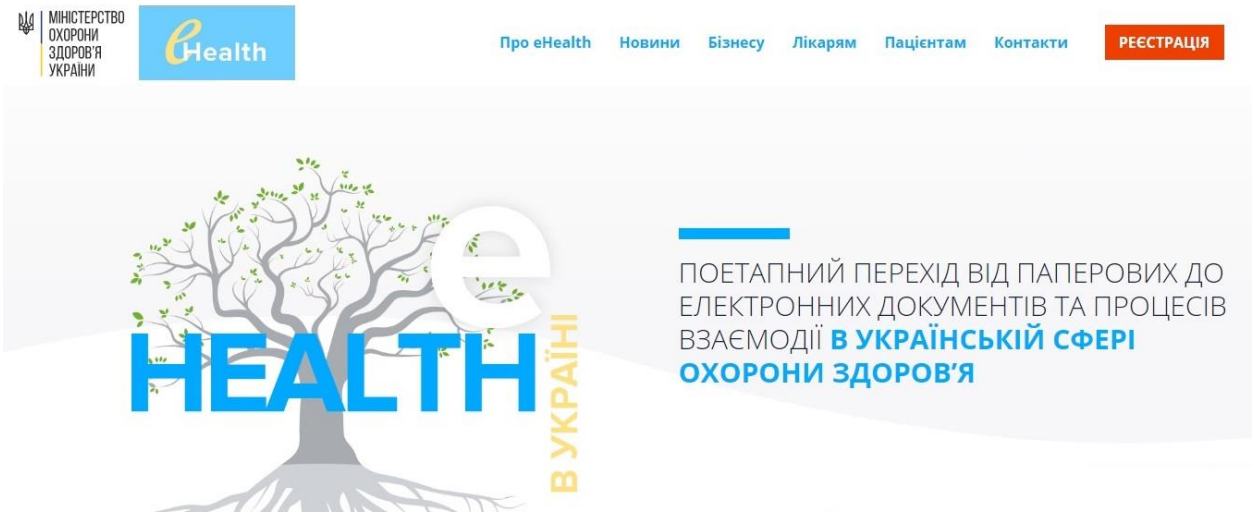

Рисунок 1.1 – Сайт проектного офісу «E-Health»

Система eHealth складається з:

– центральної БД (центральний компонент «E-Health»);

– електронних МІС – систем, які дають змогу автоматизувати роботу медичних закладів з центральної БД (периферійний компонент «E-Health»).

Центральний компонент – це спеціальне ПЗ, яке накопичує інформацію, що надходить з периферійного компоненту «E-Health» – медичних інформаційних систем або іншого ПЗ – за певними правилами.

Периферійний компонент – це або ПЗ, або МІС, з якими безпосередньо працюють медичні працівники в медичних лікувальних закладах на місцях.

Таким чином, сформовано нові вимоги до усієї системи охорони здоров'я в цілому, а саме необхідність автоматизації управління лікувальним закладом, лікувально-діагностичних процесів, обов'язкове використання МІС, як інструменту підвищення якості охорони здоров'я в країні.

Дана реформа поставила перед керівниками медичних закладів нові виклики щодо інформатизації. Впровадження сучасних технологій центральними органами влади задає високу планку використання найсучасніших комунікаційних технологій для медичних закладів. Але водночас з цим, робота з даними населення вимагає і відповідного рівня захисту інформації. З огляду на це, багато вітчизняних ЛПЗ намагаються використовувати в своїй діяльності послуги МІС.

МІС є комплексною ІС, спрямованою на оптимізацію та автоматизацію усіх рівнів робочих і технологічних процесів діяльності медичного закладу, починаючи від лікарських амбулаторій в високоспеціалізованих медичних закладах, закінчуючи науково-дослідними центрами. Вона організаційно впорядковує електронні медичні записи про пацієнтів, дані медичних досліджень в цифровій формі, дані моніторингу стану пацієнта з медичних приладів, фінансові та адміністративні дані, засоби обчислювальної техніки і зв'язку, що реалізують інформаційні процеси.

Відмінністю МІС від інших програмних продуктів перш за все є те, що в них зберігається і обробляється персональна та конфіденційна інформація, а це обумовлює особливу форму відносин між тими, хто її формує, і тими, хто її використовує. Це тягне за собою необхідність організації обробки і захисту ПДн відповідно до вимог чинного законодавства в даній області.

Закон України «Про захист персональних даних» [3] № 2297-VI від 01.06.2010 р., (з урахуванням усіх прийнятих пізніше змін і доповнень) є основним нормативно-правовим документом, який регулює правові відносини, пов'язані зі збором, обробкою та забезпеченням безпеки ПДн, дає визначення терміну, а саме ПДн – це будь-яка інформація про фізичну особу (суб'єкт ПДн): прізвище, ім'я, по батькові, дата і місце народження, адреса, ідентифікаційні дані документів, сімейне, соціальне, майнове становище, освіта, професія, доходи та інша інформація.

Персональні медичні дані пацієнта – це відомості про фізіологічні особливості організму, перенесені захворювання, стан здоров'я та наданої пацієнтові медичної допомоги. Саме ці дані накопичуються в ІС медичних установ.

Юридично, при використанні ПДн має дотримуватися право пацієнта на «збереження в таємниці інформації про факт звернення за медичною допомогою, про стан

здоров’я, діагноз та інші відомості, отримані під час його обстеження та лікування» (відповідно до «Основ законодавства України про охорону здоров’я громадян» [4]).

Це означає, що будь-який медичний працівник, який одержує доступ до МІС, несе повну (моральну, адміністративну і кримінальну) відповідальність за забезпечення конфіденційності інформації, яку він обробляє. Перелік працівників ЛПЗ, що мають доступ до ПДн у зв’язку з виконанням ними своїх посадових обов’язків, затверджується наказом головного лікаря ЛПЗ.

Зовнішній доступ до ПДн пацієнта або працівника дозволяється тільки при наявності його письмової згоди. Для цього необхідна заява із зазначенням переліку необхідної інформації і цілей для яких вона буде використана. Повідомлення відомостей про ПДн пацієнта його родичам, членам сім’ї, іншим близьким йому людям, також проводиться тільки при отриманні письмової згоди суб’єкта ПДн. Суб’єкт ПДн, про який запитуються відомості, що відносяться до ПДн, повинен бути повідомлений про передачу його ПДн третім особам. Без згоди доступ до інформації про пацієнта можливий у випадках:

– наявності ознак прямої загрози життю пацієнта;
– за умови неможливості отримання згоди такого пацієнта чи його законних представників (до часу, коли отримання згоди стане можливим);
– за рішенням суду.

Забороняється передача ПДн в комерційних цілях без згоди суб’єкта ПДн, а також інше використання ПДн в неслужбових цілях.

Під обробкою ПДн мають на увазі:

– збір;
– систематизацію;
– накопичення;
– зберігання;
– уточнення (оновлення, зміну);
– використання, поширення (в тому числі передачу);
– знеособлення;
– блокування;
– знищення ПДн.

Доступ до обробки цих даних обмежений і мають його тільки посадові особи ЛПЗ, які використовують їх безпосередньо у службових цілях (адміністратори локальної мережі медичного закладу, головний лікар, лікарі медичної установи, співробітники реєстратури, керівники структурних підрозділів, співробітники відділу кадрів) Уповноважені

адміністрацією медичної установи на обробку ПДн особи, мають право отримувати тільки ті персональні дані, які необхідні для виконання своїх посадових обов'язків.

Як зазначалося раніше, при наданні послуг медичної допомоги, передбаченої програмою державних гарантій громадянам на безкоштовну медичну допомогу, пацієнт підписує декларацію з лікарем, в яку обов'язково входить письмова згода на обробку його ПДн, за винятком випадків, передбачених законодавством України, коли така згода не є обов'язковою.

Інформація, яка є власністю держави, або інформація, захист якої гарантується державою, повинна оброблятись в МІС, що має відповідний сертифікат відповідності Міністерства охорони здоров'я (МОЗ) України, в іншому випадку використання даної МІС неправомірно. Для цього, ДССЗЗІ, відносно Закону України «Про захист інформації в інформаційно-телекомунікаційних системах» [5] повинна провести державну експертизу на наявність побудови КСЗІ у МІС.

КСЗІ – сукупність організаційних і інженерно-технічних заходів, які спрямовані на забезпечення захисту інформації від розголошення, витоку і несанкціонованого доступу (НСД).

Побудовою КСЗІ може займатися організація, що має відповідну ліцензію. МІС повинна мати, або свою систему шифрування, яка має сертифікат ДССЗЗІ, або потрібно кожний раз будувати нову КЗСІ на об'єкті замовника. Це можливо зробити або силами замовника (якщо є ліцензія), або розробником МІС (якщо є ліцензія), або третьою стороною, яка має відповідну ліцензію.

Відповідальність за відсутність або неналежне здійснення захисту інформації в ІС несе керівник компанії, згідно діючого законодавства України.

Таким чином можна зробити висновок, що для використання МІС в закладах системи охорони здоров'я необхідно вирішення низки програмних, організаційно-технічних питань, в першу чергу пов'язаних з дотриманням лікарської таємниці і захистом ПДн.

1.1.1 Класифікація типів інформації в МІС з точки зору системи безпеки

Для основоположного розуміння того, яка інформація циркулює в МІС ЛПЗ треба визначити види цієї інформації і можливі операції над нею, а також систематизувати ці дані у відповідність з рівнями секретності та актуальності для ЛПЗ.

Перш за все, треба виділити фрагменти інформації про пацієнта. Це інформація:

Про факт звернення

Інформація про факт звернення до лікувального закладу віднесена законодавством до особистої таємниці пацієнта і зобов'язана дотримуватися співробітниками ЛПЗ, як таємниця професійна.

ПДн пацієнта ЛПЗ

ПДн пацієнта віднесені законодавством до особистої таємниці пацієнта. Більш того, вони виділені в особливу категорію, що захищається спеціальним чином. Як і у випадку з інформацією про факт звернення, конфіденційність ПДн пацієнта повинна дотримуватися співробітниками ЛПЗ, як таємниця професійна. Даний вид інформації характеризується тим, що для процесу лікування пацієнта не є чимось необхідним.

Належність до групи

До таких даних належать стать і вік пацієнта, регіон його проживання, належність до деяких професій, пільгових категорій, тощо. Ці дані агрегуються і, при достатньому рівні абстрагування, не є конфіденційною інформацією, тому що по ним не можливо однозначно ідентифікувати персону. Таких даних, як правило, достатньо для лікування пацієнта. Призначення лікаря, перш за все, ґрунтується саме на належності до якоїсь групи і на стані людини, які лікар визначає для конкретного пацієнта, зважаючи на об'єктивність даних, особисті свідчення і медичну історію пацієнта, а не на його ПІБ, адресі та номері паспорта.

У той же час слід враховувати те, що в разі низького рівня деталізації, навіть такі дані можуть однозначно визначити людину, тобто, зіграти роль ПДн.

Діагноз

Інформація стосовно діагнозу пацієнта є його особистою таємницею, і зобов'язана дотримуватися співробітниками ЛПЗ, як таємниця професійна. Цей вид інформації характеризується тим, що становить лікарську таємницю тільки в поєднанні з ПДн пацієнта.

Анамнез

Під час збору анамнезу, лікарю, найчастіше доводиться мати справу з особистими даними. Причому, не тільки з особистими даними самого пацієнта, які він повідомляє лікарю самостійно, а й з особистою таємницею близьких пацієнтові людей, які згоди на поширення і обробку такої інформації про них не давали. Всі ці відомості, з одного боку, необхідні в постановці вірного та повного діагнозу і сприяють вибору вірного способу лікування. З іншого боку, збирання та обробка цих даних суперечить законодавчій базі, тому що дана інформації стає вже таємницею не того пацієнта, про збереження здоров'я якого йде мова, а зовсім інших людей. Дані, що входять до анамнезу, також

характеризуються тим, що становлять лікарську таємницю тільки в поєднанні з ПДн пацієнта.

Призначення і рекомендації

У поєднанні з персональною інформацією про пацієнта ці дані становлять лікарську таємницю, так як можуть розповісти про діагноз пацієнта і про стан його здоров'я. У поєднанні з діагнозом, але без ПДн, такі відомості не є конфіденційними.

Найголовніша відмінність цього виду інформації в тому, що в поєднанні з даними, які ідентифікують пацієнта ці відомості критично важливі для лікування пацієнта.

Якщо раніше йшла мова саме про збереження конфіденційності даних, то у випадку з призначеннями і рекомендаціями життєво важливе значення набуває саме збереження цих даних від втрати, випадкової несанкціонованої, а тим більше від шкідливої модифікації при їх обробці в МІС. І тим більшої значущості ця обставина набуває в стаціонарі, де безпосередньо виконуються призначення, і де стан здоров'я пацієнтів, як правило, більш важкий, ніж при амбулаторному лікуванні. Несанкціонована зміна таких даних може привести до ситуації, коли пацієнтові будуть проведені лікувальні маніпуляції не тільки не показані при його захворюванні/стані, але і прямо шкодять його здоров'ю.

Стан, про хід лікування

У поєднанні з персональною інформацією про пацієнта ці дані становлять лікарську таємницю, так як можуть розповісти про діагноз пацієнта і про стан його здоров'я. У поєднанні з діагнозом, але без ПДн, такі відомості не є конфіденційними.

Структура інформації про співробітника ЛПЗ:

ПДн пацієнта

ПДн віднесені законодавством до особистої таємниці людини та захищаються спеціальним чином. Але ПДн співробітника ЛПЗ, як фахівця, який лікує людей, носять суперечливий характер. Для того, щоб пацієнти могли ідентифікувати фахівця, до якого вони звертаються, фрагменти ПДн лікарів, надаються широкому колу користувачів. Наприклад, вони фігурують в розкладі прийому, доступному необмеженому колу людей.

Спеціалізація

Спеціалізація медичного співробітника визначає його роль в лікувально-діагностичному процесі. Ці відомості є базовими в описі ЛПЗ. Зважаючи на трактування ПДн, яке наведене в попередньому підрозділі, спеціалізацію медичного працівника можна, найчастіше віднести до складової його ПДн.

Кадрова інформація

Дані про освіту, про призначення на посаду, про заохочення/стягнення тощо, складають, як особисту таємницю співробітника, так і службову інформацію ЛПЗ. Співробітники відділу кадрів зобов'язані зберігати конфіденційність цих відомостей.

Графік роботи

Графік роботи фахівця, а також інформація про вільний проміжок часу в графіку його прийому відносяться до базових даних в описі ЛПЗ. Графік роботи необхідний пацієнтам, як потенційним споживачам робочого часу лікаря, так і персоналу лікарні для оптимізації робочих процесів та медичного закладу взагалі.

1.1.2 Класифікація загроз безпеки ПДн в медичних закладах

Поява нових ІТ і розвиток потужних комп'ютерних систем зберігання і обробки інформації підвищило рівень вимог щодо захисту інформації та викликало необхідність в тому, щоб ефективність захисту інформації зростала разом зі складністю архітектури зберігання даних.

Так поступово захист конфіденційної інформації стає обов'язковим: розробляються і формуються різні документи та рекомендації щодо захисту цієї інформації. Таким чином, загроза захисту інформації зробила засоби забезпечення ІБ однією з обов'язкових характеристик ІС.

Під ІБ розуміється захищеність інформації та підтримка інфраструктури, яка її захищає, від будь-яких випадкових або зловмисних дій, результатом яких може бути нанесення збитку самій інформації, її власникам або інфраструктурі.

ІБ медичного закладу – стан захищеності інформаційного середовища ЛПЗ, що забезпечує її формування, використання і розвиток.

Основні загрози безпеки ПДн:

- загрози витоку інформації технічними каналами;
- загрози НСД до ПДн, оброблюваних на автоматизованому робочому місці (АРМ).

Загрози витоку інформації технічними каналами включають в себе:

- загрози витоку акустичної інформації;
- загрози витоку видової інформації;
- загрози витоку даних по каналах зв'язку.

Виникнення загроз витоку акустичної інформації, можливо при наявності функцій голосового введення ПДн в МІС або функцій відтворення ПДн акустичними засобами.

Реалізація загрози витоку видової інформації можлива за рахунок перегляду інформації за допомогою оптичних засобів з екранів дисплеїв і інших засобів відображення, засобів обчислювальної техніки, інформаційно-обчислювальних комплексів, технічних засобів обробки графічної, відео- і буквено-цифрової інформації, що входять до складу МІС.

Загрози з зовнішніх мереж включають в себе:

– загрози «аналізу мережевого трафіку» з перехопленням переданої в зовнішні мережі і прийнятої з зовнішніх мереж інформації;
– загрози сканування, спрямовані на виявлення вразливостей в системі;
– загрози виявлення паролів;
– загрози впровадження по мережі шкідливих програм.

Загрози зараження персонального комп'ютера (ПК) виникають через поширення шкідливого ПЗ через:

– знімні носії;
– заражені Web-сторінки;
– електронну пошту;
– дірки в мережевій безпеці;
– заражені файли і документи.

Таким чином, в сучасних умовах інформатизації медицини, наявність розвиненої системи ІБ стає однією з найважливіших умов конкурентоспроможності і навіть життєздатності будь-якого медичного закладу. Тому особливу увагу при модернізації лікувально-профілактичних процесів керівництвом ЛПЗ повинно приділятися розробці основних напрямків політики безпеки і спеціальних програм, спрямованих на забезпечення ІБ.

1.2 Аналітичний огляд ступеня наукової розробленості теми дослідження

За останні роки, значно збільшилась кількість наукових робіт присвячених питанням автоматизації процесів медичної сфери, функціональним модулям МІС, окремим аспектам їх застосування в практиці, апаратним та програмним вимогам. Концептуальні засади створення МІС і методи забезпечення надійності та безпеки ПДн розглянуті в роботах вітчизняних і зарубіжних авторів.

Серед них слід відзначити праці таких авторів, як: Бєльшев Д.В., Гаріф'янов Д.М., Гольдберг Д.Л., Гулієв Я.І., Євсєєв С.П., Істратова О.О., Тарнавський Ю.А.

Основними джерелами, які розкривають нормативно-правові основи щодо захисту ПДн в закладах охорони здоров'я є роботи «Защита персональных данных» [6] Євсєєва С.П., Лінд Е.О., Носика О.М., «Основные аспекты обеспечения защищенности персональных данных в медицинских информационных системах» [7] Гольдберга Д. Л., Григор'єва П.Є., Оленчука О. В., «Особенности защиты персональных данных в медицинских информационных системах» [8] Істратової О. О., Молчанова О.П. У цих роботах розглядається і проводиться порівняльний аналіз законодавчих актів країн Євросоюзу, США та пострадянського простору, обґрунтування необхідності застосування комплексного підходу до питання захисту ПДн та розробки захищених каналів зв'язку між МІС і центром обробки даних.

Проблеми перманентного розвитку і трансформації медичної галузі, архітектура сучасної МІС, питання інтеграції, моделі предметної галузі, функціональні можливості, висвітлені у статті «Основные аспекты разработки медицинских информационных систем» [9] Гулієва Я. І.

Робота «Обеспечение информационной безопасности в медицинских организациях» [10] Гулієва Я. І., Цвєткова О.О. в значній мірі сприяла визначенню актуальних загроз і заходів щодо забезпечення ІБ в МІС, розумінні того, якою має бути модель архітектури захищеного інформаційного середовища медзакладу.

На основі статті «Защита персональных данных в медицинских информационных системах» [11] Гаріф'янова Д. М-Х., Вахітова І. Х. детально розглянуто особливості захисту ПДн в МІС та створення мережевої інфраструктури для філії поліклініки, з урахуванням вимог щодо забезпечення безперервності медичних процесів, ІБ за рахунок використання криптографічного захисту, використання мережевого екрану, запобігання вторгнень та фільтрації трафіку.

Оцінка ефективності проекту інформатизації ЛПЗ з урахуванням специфіки витрат і вигоди була зроблена у роботі «Подход к оценке экономической эффективности медицинских информационных систем» [12] Гулієва Я. І., Гулієвой І. Ф., Рюміна Є. В, Малих В. Л., Фохт О. О., Тавлибаєвої Е. Ф., Вахріної О. Ю. У статті підведені підсумки практичної оцінки інвестиційних проектів інформатизації декількох ЛПЗ різного типу.

Деякі із вище зазначених авторів на протязі багатьох років займаються дослідженням широкого кола актуальних питань, пов'язаних з розвитком медичних систем. Одним із таких авторів є к.т.н. Гулієв Я.І. В своїх публікаціях, він розглядає різні аспекти застосування інформаційних технологій в охороні здоров'я, а зокрема, і МІС, порушує питання, пов'язані зі стандартизацією в медичній інформатиці, особливості медичних даних і управління ними, наводить огляд розробок в області МІС.

Аналіз статей «Информационные системы в управлении лечебно-профилактическим учреждением» Гулієва Я. І., Назаренко Г. І., «Особенности решения проблем информационной безопасности в медицинских информационных системах» Фохт О. О., Гулієва Я. І., Міхєєва А.Є., Назаренко Г. І., Горбунова П. А., Фохт І. О., «Изменение функциональных требований к МИС в процессе перестройки систем здравоохранения» Бєлишева Д. В. Гулієва Я. І. Міхєєва А. Є., «Подход к экономической эффективности медицинских информационных систем» Вахріна О. Ю., Фохт. О. О., Гулієва Я. І., Малих В. Л., Гулієвої І. Ф., Рюміна Є. В., Тавлибаєва Е.Ф., дав остаточне розуміння концепції МІС, основних функцій та властивостей цього класу систем, технологічних вимог, яким повинні відповідати сучасні МІС, перспективи їх розвитку.

В статті «Forward Secure Digital Signature for Electronic Medical Records» [13] Yao-Chang Yu, To-Yeh Huang, Ting-Wei Hou, проводиться аналіз недоліків використання звичайних цифрових підписів (ЦП) в ЕМІ і пропозиція щодо впровадження методу прямого захищеного ЦП для забезпечення надійності в умовах оновлення ключа (сертифіката).

Стаття «Selected aspects of information security management in entities performing medical activity» [14] Dominika Lisiak-Felicka, Pawel Nowak, Maciej Szmit присвячена питанням, які пов’язані з управлінням ІБ в медичних закладах. В ній автори на основі анкетування-інтерв’ю ІТ-менеджерів медичних закладів, провели аналіз і оцінку системи управління ІБ в цих закладах. В результаті дослідження були визначені і описані шляхи управління ІБ (зокрема, такі аспекти, як види інформації, які повинні бути захищені в суб’єктах охорони здоров’я, інциденти ІБ, управління ризиками, бюджет на ІБ, навчання і загальне впровадження регламентів захисту даних).

Практичний досвід реалізації сучасних комплексних МІС відображений в розробках вітчизняних ІТ-компаній. Детальний аналіз існуючих програмних продуктів в сфері охорони здоров’я на ринку України, показав наявність великої кількості приватних спеціалізованих МІС, які характеризуються зручною архітектурною побудовою системи, можливістю впровадження та супроводу, рівнем захисту даних та підтримкою інтеграції зі сторонніми продуктами. Істотний внесок у розуміння концепції роботи МІС, функціональних та технічних вимог, внесла супровідна інформація (презентації, матеріли офіційних сайтів, оцінка фахівців) таких систем: Доктор ЕЛЕКС [15], EMCiMED [16], МедІнфоСервіс [17], e-Life [18]. Дані системи були вибрані зважаючи на функціональну складову та кількість підключених до них ЛПЗ.

Також розглянуто ряд законодавчих документів, що регулюють захист ПДн в установах охорони здоров’я. Такими документами були: Закон України «Про захист

персональних даних» від 01.06.2010 р. № 2297-VI [3], Закон України Про внесення змін до Закону «Про захист персональних даних» від 20.11.2012 № 5491-VI [19], Наказ МОЗ України «Про затвердження Порядку вибору лікаря, який надає первинну медичну допомогу, та форми декларації про вибір лікаря, який надає первинну медичну допомогу» від 19.03.2018 р. № 503 [20].

Теоретично-наукові дослідження в області інформатизації системи охорони здоров'я, присвячені переважно загальним питанням концепції МІС: базовим поняттям в МІС, їх класифікації, аспектам функціонування, розгляду особливостей архітектури цих систем.

Однак, питання розробки комплексного рішення відносно забезпечення захисту ПДн та медичних ПДн в МІС розглянуті на рівні загальних підходів. Це пов'язано насамперед з тим, що публікації з даної тематики в українських періодичних виданнях тільки починають з'являтися, а кількість зарубіжних робіт з предмету дослідження є доволі обмеженою.

Таким чином, зроблений ґрунтовний аналіз показує необхідність розвитку теоретичних основ і методологічної бази, а також розробки науково-обґрунтованих рекомендацій щодо її застосування.

1.3 Аналіз існуючих аналогів МІС

На сьогоднішній день в Україні спостерігається період значного зростання числа МІС в ЛПЗ, причому, як у великих медичних центрах з великими потоками інформації, так і в медичних центрах середніх розмірів. В рамках здійснюваної в даний час медичної реформи на рівні МОЗ України, медичні заклади самостійно вибирають МІС з наявних на ринку програмних рішень і після запровадження такої системи з її допомогою підключаються до Центрального компоненту. Станом на 2018 рік 97% медичних закладів, що надають первинну медичну допомогу вже долучилися до трансформації. На даний момент, до електронної системи охорони здоров'я «E-Health» підключено близько двадцяти різних МІС.

Для забезпечення захисту інформації медичні організації використовують ряд засобів. Таким чином, всі МІС можна умовно поділити на дві групи: ті, що реалізують захист ПДн за допомогою апаратних засобів (АЗ) захисту і ті, основою захисту ПДн яких є ПЗ.

МІС будуть проаналізовані з точки зору апаратної, програмної складової, криптографічних засобів захисту інформації та побудови КСЗІ.

МІС «Доктор ЕЛЕКС» – комплексне програмне рішення автоматизації та інтеграції усіх основних аспектів роботи сучасних медичних закладів.

Основні функції МІС «Доктор ЕЛЕКС»:

– систематизація роботи медичного закладу;
– впровадження контролю за процесом лікування;
– забезпечення гармонійної співпраці персоналу;
– підвищення якості обслуговування пацієнтів;
– можливість швидкого доступу до інформації.

У своїй роботі МІС «Доктор ЕЛЕКС» використовує ключові компоненти, які забезпечують широкі можливості і майже необмежену масштабованість, та надають можливість користувачам цієї системи працювати швидше і ефективніше.

Логічна архітектура МІС «Доктор ЕЛЕКС» складається з трьох рівнів:

– рівень БД;
– рівень сервера комунікації;
– рівень клієнтської програми.

Архітектура МІС «Доктор ЕЛЕКС» (рис. 1.3) допускає розширення функціонального і інформаційного складу шляхом підключення додаткових програмних модулів із застосуванням документованих інтерфейсів, або додаткових серверів БД.

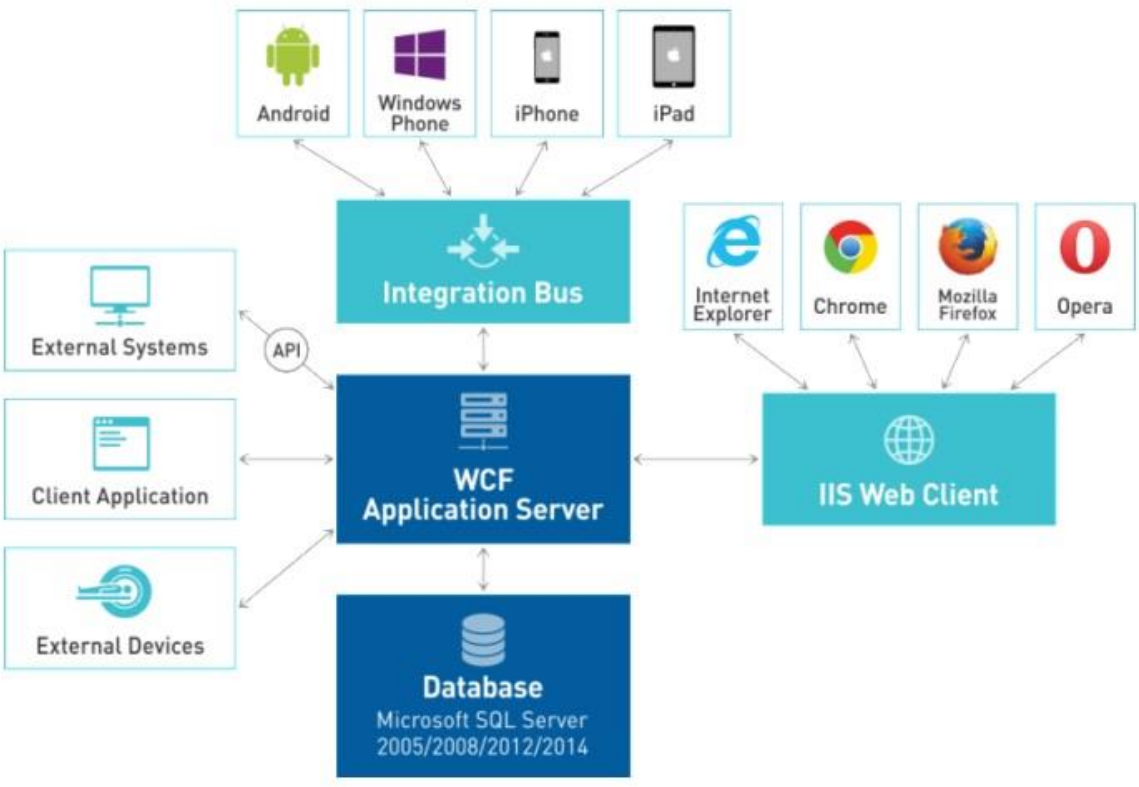

Рисунок 1.3 – Логічна архітектура системи «Доктор ЕЛЕКС»

БД побудована на основі платформи Microsoft SQL Server 2005/2008/2012/2014. Ця платформа має сертифікат ДССЗЗІ, який дозволяє використовувати її для розробки захищеного рішення.

Сервер комунікації імплементований на основі технології Windows Communication Foundation (WCF). Сервер комунікації взаємодіє з клієнтськими додатками і зовнішніми медичними пристроями за допомогою протоколу TCP/ IP, а також передбачає інтеграцію з зовнішніми системами за допомогою прикладного програмного інтерфейсу API.

Клієнт системи «Доктор ЕЛЕКС» побудований за допомогою технології Microsoft Windows Forms з використанням платформи .Net Framework 3.5. Для безпечної комунікації в мережі використовується інфраструктура безпеки доменів Windows за допомогою служби Active Directory. Повнофункціональна клієнтська програма працює під управлінням операційної системи (ОС) Microsoft Windows, а веб-клієнт - за допомогою web-браузерів.

Для взаємодії БД з мобільними додатками використовується інтеграційна шина, побудована на базі WCF. Обмін даними здійснюється по протоколу HTTP в форматі JSON, що є найкращим рішенням для мобільних платформ, які часто обмежені в ресурсах.

Вимоги до технічних засобів

Нижче перелічено мінімальні та рекомендовані вимоги до апаратного і ПЗ для успішної інсталяції та подальшої ефективної роботи сервера «Доктор ЕЛЕКС» (табл. 1.1 – 1.2).

Таблиця 1.1 – Вимоги до АЗ для серверів «Доктор ЕЛЕКС»

К-сть Робочих місць	**АЗ**		
1-20	**Мінімальні характеристики**		**Рекомендовано**
	Процесор	2–3 ГГц Core2Duo	2–3 ГГц Core2Duo або Core i3/Core i5
	Оперативна пам’ять	4 ГБ	4 ГБ
	Дисковий простір	20–100 ГБ	40–200 ГБ
	DVD-ROM привід	Так (для інсталяції архівів)	Так (для інсталяції архівів)
21-50	**Мінімальні характеристики**		**Рекомендовано**
	Мережа	Від 100 Мбіт	Від 100 Мбіт
	Процесор	2 ГГц Intel i5, Xeon (від 4 потоків)	2–3 ГГц Intel Core i5, Core i7, Xeon (від 8 робочих потоків)
	Оперативна пам’ять	8 ГБ	8–16 ГБ
	Жорсткий диск	Масив 3×160 ГБ SAS in RAID5 або 4×160 ГБ SAS in RAID10 + 2x500 ГБ SATA3 RAID0 для архіву БД	Масив 4×500 ГБ SATA3 RAID (10 або 5) + 2x500 ГБ SATA3 RAID0 для архіву БД

Продовження таблиці 1.1 – Вимоги до АЗ для серверів «Доктор ЕЛЕКС»

К-сть Робочих місць	**АЗ**		
1-20	**Мінімальні характеристики**		**Рекомендовано**
	DVD-ROM привід	Так (для інсталяції архівів)	Так (для інсталяції архівів)
21-50	**Мінімальні характеристики**		**Рекомендовано**
	Мережа	Від 100 Мбіт	Від 100 Мбіт
	Процесор	2 ГГц Intel i5, Xeon (від 4 потоків)	2–3 ГГц Intel Core i5, Core i7, Xeon (від 8 робочих потоків)
	Оперативна пам’ять	8 ГБ	8–16 ГБ
	Жорсткий диск	Масив 3×160 ГБ SAS in RAID5 або 4×160 ГБ SAS in RAID10 + 2x500 ГБ SATA3 RAID0 для архіву БД	Масив 4×500 ГБ SATA3 RAID (10 або 5) + 2x500 ГБ SATA3 RAID0 для архіву БД
	DVD-ROM привід	Так (для інсталяції архівів)	Так (для інсталяції архівів)
51-100	**Мінімальні характеристики**		**Рекомендовано**
	Мережа	1 Гбіт	1 Гбіт
	Процесор	2 ГГц Intel Xeon	2 ГГц Intel Xeon
	Оперативна пам’ять	16–24 ГБ	24–32 ГБ ECC
	Жорсткий диск	Масив 3×160 ГБ SAS in RAID5 або 4×160 ГБ SAS in RAID10 + 2x500 ГБ SATA3 RAID0 для архіву БД	Масив 4×160 ГБ SAS RAID (10 або 5) + 2x500 ГБ SATA3 RAID0 для архіву БД

Таблиця 1.2 – Вимоги до ПЗ для серверів «Доктор ЕЛЕКС»

К-сть Робочих місць	**Апаратне забезпечення**		
1-20	**Мінімальні характеристики**		**Рекомендовано**
	ОС	ОС Windows 7 Professional	ОС Windows 7 Professional
	Система керування БД	Microsoft SQL Server 2008 R2/2012/2014/2016 Express Edition (при перевищенні ліміту у 10 ГБ на розмір БД необхідно придбати платну ліцензію)	Microsoft SQL Server 2008 R2/2012/2014/2016 Express Edition (при перевищенні ліміту у 10 ГБ на розмір БД необхідно придбати платну ліцензію)
21-50	**Мінімальні характеристики**		**Рекомендовано**
	ОС	MS Windows Server 2008R2/2012R2/201 6 Standard (Essential у випадку до 25 р.м.)	MS Windows Server 2008R2/2012R2/2016 Standard
	Система керування БД	Microsoft SQL Server 2008 R2/2012/2014/2016 Express Edition (при перевищенні ліміту у 10 ГБ на розмір БД необхідно придбати платну ліцензію)	Microsoft SQL Server 2008 R2/2012/2014/2016 Express Edition (при перевищенні ліміту у Оперативна 10 ГБ на розмір БД необхідно придбати платну ліцензію)
51-100	**Мінімальні характеристики**		**Рекомендовані**
	ОС	MS Windows Server 2008R2/2012R2/201 6 Standard + клієнтські ліцензії	MS Windows Server 2008R2/2012R2/2016 Standard + клієнтські ліцензії

Продовження таблиці 1.2 – Вимоги до ПЗ для серверів «Доктор ЕЛЕКС»

К-сть Робочих місць	**Апаратне забезпечення**		
	Мінімальні характеристики		**Рекомендовано**
51-100	Система керування БД	Microsoft SQL Server 2008 R2/2012/2014/2016 Standard + клієнтські ліцензії	Microsoft SQL Server 2008 R2/2012/2014/2016 Standard + клієнтські ліцензії

МІС «EMCiMED» – програмний комплекс, який дозволяє автоматизувати діяльність учасників процесу надання медичної допомоги незалежно від форми власності і типів допомоги, кадрового складу і рівня організації.

Ключові процеси в медицині, які автоматизує МІС «EMCiMED»:

– створення електронної медичної карти;

– формування БД пацієнта;

– автоматизація ресурсного управління;

– створення робочих зон з певними рівнями прав кожного співробітника: лікарі, лаборанти, медсестри, провізори і фармацевти, та інші;

– облік і контроль лікарських засобів;

– робота з результатами лабораторних досліджень, збереження результатів діагностичних процедур тощо. При потребі – синхронізація з лабораторними ІС.

Відповідно до результатів державної експертизи у сфері технічного захисту інформації, автоматизована МІС «EMCiMED» є засобом, який дозволений для забезпечення технічного захисту державних інформаційних ресурсів та інформації.

Для збереження і передачі необхідної інформації на робочі місця медперсоналу, використовується трирівнева система: SQL-сервер баз даних – Application Server – Client.

Це означає, що сервер додатка спілкується тільки з сервером БД, де знаходяться всі дані, введені в систему, а клієнт-машина спілкується тільки з сервером додатка. Таким чином, ніхто зі співробітників не має прямого доступу до БД, що робить неможливим хакерський злом будь-якої окремої робочої станції.

Для уникнення випадкових дій з боку самого користувача в системі «EMCiMED» є можливість розмежування прав доступу і функцій для різних груп користувачів, а також вбудована система логування. З її допомогою ведеться запис кожної дії, вчиненої кожним користувачем системи, включаючи дату цієї дії і всі пов’язані з нею подробиці.

Серверні програмні компоненти МІС «EMCiMED»:

– сервер управління БД на основі продуктів Microsoft SQL Server (сервер БД);

– сервер додатків на основі технологій COM+ від Microsoft (App-сервер);

– сервер зберігання зображень та управління DICOM пристроями (PACS-сервер власної розробки).

Вимоги до технічних та програмних засобів наведені в таблиці 1.3 – 1.4

Таблиця 1.3 – Вимоги до технічних засобів в МІС «EMCiMED»

Назва	**Технічні засоби (Специфікація)**
Фізичний сервер	x86 / x64-сумісні автоматизовані системи з такими мінімальними (min) та рекомендованим (opt) основними характеристиками: CPU: min-2.6 GHz / opt-3.0 GHz; RAM: min-4Gb / opt-8 Gb; VRAM: min-1 Gb / opt-2 Gb; HDD (обсяг вільного місця на диску): min-100Gb / opt-250 Gb (або вище).
Робочі станції адміністраторів/ користувачів	x86 / x64-сумісні автоматизовані системи з такими основними характеристиками: 2 ядра (1.6 GHz) CPU, 4Gb RAM; 1 Gb HDD (або вище), які відповідають умовам (або вище).
Засіб криптографічного захисту інформації (КЗІ)	Засоби КЗІ, які надаються кваліфікованими надавачами електронних довірчих послуг (відповідно до довірчого списку (реєстру) Центрального засвідчувального органу Міністерства юстиції України). Засоби КЗІ які мають позитивний експертний висновок за результатами державної експертизи в сфері криптографічного захисту інформації.
Мережевий екран (маршрутизатор)	Пристрої мережевої безпеки які мають позитивний експертний висновок за результатами державної експертизи в сфері технічного захисту інформації.
Система зберігання даних (сховище backup)	NAS-сховище, або інше рішення, які забезпечують резервування даних СКБД МІС ЕМСІМЕД та мають загальній обсяг запам’ятовуючих пристроїв ї не менш ніж 4Tb (або вище).
Комутатор	Технічний засіб з підтримкою стандартів передачі даних Fast Ethernet (10/100 Мбит/с), реалізованим режимом «некерованого комутатора» та функцією керування потоком даних.
Джерело безперебійного живлення	Має потужність ні менш ніж 600 Вт та спроможне забезпечити роботу, з максимальною потужністю, на протязі ні менш ніж 1 хвилини.

Таблиця 1.4 – Вимоги до ПЗ в МІС «EMCiMED»

Встановлені (використовуються у складі технічного засобу)	**Програмні засоби**
Фізичний сервер	ОС MS Windows Server (Datacenter/Standard/Enterprise) 2008R2/2012R2/2016 Служба Active Directory у складі ОС Компонент DirectAccess and VPN у складі ОС Application Server role App-V МІС «ЕМСІМЕД»-server.v5 Компонент EMCMED PACS (за необхідності) СКБД MS SQL Server 2008R2/2012/2016/2017 Модуль взаємодії з центральною БД електронної системи охорони здоров’я (E-Health) Програмний продукт антивірусного захисту інформації - засіб антивірусного захисту інформації який має позитивний експертний висновок за результатами державної експертизи в сфері технічного захисту інформації
Робочі станції адміністраторів/ користувачів	MS Windows 7, MS Windows 8 (8.1, 8.1Pro), MS Windows 10 (Professional/Enterprise) МІС «ЕМСІМЕД» Програмний продукт антивірусного захисту інформації - засіб антивірусного захисту інформації який має позитивний експертний висновок за результатами державної експертизи в сфері технічного захисту інформації
Засіб КЗІ	Правильно реалізовані криптографічні алгоритми (у складі засобу КЗІ)

Продовження таблиці 1.4 – Вимоги до ПЗ в МІС «EMCiMED»

Встановлені (використовуються у складі технічного засобу)	**Програмні засоби**
Мережевий екран (маршрутизатор)	Спеціалізована операційна система (у складі технічного засобу)
Система зберігання даних (сховище backup)	Спеціалізована операційна система (у складі технічного засобу)
Комутатор	Спеціалізована операційна система (у складі технічного засобу)
Джерело безперебійного живлення	-

МІС «МедІнфоСервіс» використовує аналогічні з вищенаведеними МІС, апаратні та програмні складові. Даний програмний продукт автоматизує лікувальні процеси медичних закладів та формує медичну статистичну звітність. МІС «МедІнфоСервіс» акредитована МОЗ і підключена до електронної системи охорони здоров'я «E-Health». Може бути впроваджена в закладах первинного, вторинного та третинного рівня медичної допомоги.

Конфіденційність медичних даних забезпечується Модулем шифрування даних для СКБД Firebird виробництва компанії «Сайфер». Модуль шифрування побудований на основі бібліотек криптографічних примітивів Шифр +, що володіють чинним позитивним експертним висновком ДССЗЗІ України.

Функції, які входять до складу бібліотек, реалізують:

– шифрування/дешифрування та формування імітовставки згідно алгоритму ГОСТ 28147-89;

– створення/перевірка ЦП згідно алгоритму ДСТУ 4145-2002;

– генерація ключової пари: особистого та відкритого ключа ЦП згідно алгоритму ДСТУ 4145-2002;

– обчислення геш-функції даних згідно алгоритму ГОСТ 34.311-95;

– генерація ключової пари: особистого та відкритого ключа для протоколу Діффі-Гелмана ДСТУ ISO/IEC 15946-3;

– генерація криптостійкої псевдовипадкової послідовності згідно алгоритму ДСТУ 4145-2002.

КСЗІ може бути:

– програмною;

– апаратною;

– програмно-апаратною.

Програмна КСЗІ – потребує впровадження алгоритмів, програмних методів та засобів сертифікованих ДССЗЗІ, сертифікується один раз.

Апаратна КСЗІ – найбільш захищена система захисту інформації, але недоліком є вартість впровадження. Після побудови обов'язково повинна пройти сертифікацію ДСЗЗІ і включати в себе лише ті АЗ, що вже мають сертифікат ДССЗЗІ.

Програмно-апаратна КСЗІ – об'єднання двох попередніх підходів.

Всі програмні компоненти КСЗІ (ОСна робочому місці, ОС на сервері, ПЗ МІС) – повинні мати сертифікат ДССЗЗІ.

Таблиця 1.5 – Переваги та недоліки проаналізованих МІС

ПЗ	**Переваги**	**Недоліки**
Доктор ЕЛЕКС	-	Компанія не має ліцензію на побудову КСЗІ та будує її за схемою затвердження моделі, яка використовується у замовника. Персональні та медичні дані зберігаються на сервері розробника.
ЕМСІМЕД	Компанія має ліцензію на побудову КСЗІ та будує її за схемою затвердження моделі, яка використовується у замовника на основі АЗ.	Потребує побудови КСЗІ
Medstar	Компанія має ліцензію на побудову КСЗІ та будує її за схемою затвердження моделі, яка використовується у замовника на основі АЗ.	Потребує побудови КСЗІ

МІС «Доктор ЕЛЕКС» – комплексне ПЗ, яке не використовує систем захисту інформації, не встановлює та не розробляє КЗСІ.

МІС «EMCiMED» – має тільки шифрування даних, що передаються від клієнта до сервера та в зворотному напрямку. Але компанія-розробник має ліцензію на побудову КЗСІ і будує її на основі апаратного шифрування з використанням апаратних брандмауерів та приладів шифрування від ІІТ (інститут інформаційних технологій), який також є акредитованим центром сертифікації ключів.

1.4 Постановка задачі магістерської роботи

Мета і задачі дослідження. Метою роботи є дослідження та вибір підходів, методів і технічних засобів підвищення захисту ПДн в МІС.

Об'єктом дослідження магістерської роботи є комплекс апаратно-програмних засобів захисту ПДн в МІС.

Предметом дослідження магістерської роботи є медичні ПДн в МІС

На основі вищерозглянутої предметної області можна сформувати мету роботи, що полягає у дослідженні і виборі методів та технічних засобів підвищення захисту ПДн в МІС.

Для досягнення поставленої мети, у магістерській роботі передбачається вирішення таких задач:

– аналітичний огляд нормативно-правової бази, наукових публікацій з тематики роботи;

– дослідження проблем щодо забезпечення надійності та безпеки ПДн;

– аналіз сучасних апаратних, програмних та криптографічних засобів захисту ПДн;

– розгляд методів та засобів захисту ПДн в МІС;

– розробка технології підвищення захисту ПДн в МІС;

– формування комплексного підходу до забезпечення захисту ПДн та медичних ПДн з урахуванням виявлених недоліків;

– дослідження ефективності розробленого підходу.

1.5 Висновки до першого розділу

У першому розділі магістерської роботи проведено аналіз предметної галузі, описано основні вимоги до ІБ, встановлено зв’язок між законодавчою основою інформатизації медичної сфери і впровадженням МІС в роботу ЛПЗ.

Розглянуто базові поняття в МІС та типи інформації, яка в них циркулює, з точки зору системи безпеки. Окремо проаналізовано об’єкт захисту, а саме ПДн та медичні ПДн, детально розглянуто аспекти, та практика правового регулювання захисту цих даних. Також проведено аналіз та огляд нормативно-правових актів, що регламентують захист ПДн в Україні. Для розуміння поточної тенденції розвитку сучасних комплексних МІС взагалі та ступеня захисту ПДн в цих системах зокрема, досліджено вітчизняний ринок в сфері охорони здоров’я та теоретично-наукові роботи з даної тематики. Надано ґрунтовний аналіз найбільш популярніших і лідируючих на ринку рішень МІС. Аналіз виявив і показав, що незважаючи на зростаючу кількість програмних продуктів націлених на автоматизацію лікувально-діагностичних та супутніх процесів, існує низка недоліків пов’язана з забезпеченням ІБ та достатньо високою собівартістю впровадження даних систем, а в наукових роботах відсутні дослідження націлені на підвищення захисту ПДн та медичних ПДн в МІС.

Спираючись на науково-методологічну базу і враховуючи вище розглянуту інформацію, можна зробити висновок, що ІБ є комплексним завданням. Це означає, що для дотримання усіх законодавчо встановлених вимог до захисту конфіденційної інформації при її автоматизованій обробці в медичних закладах, повинно бути розроблене комплексне рішення щодо забезпечення інформаційної безпеки.

2 ДОСЛІДЖЕННЯ СУЧАСНИХ ЗАСОБІВ ЗАХИСТУ ПДН В МІС

2.1 Класифікація методів і засобів захисту інформації

Побудова будь-якої МІС передбачає наявність КСЗІ, до складу якої можуть входити різні засоби захисту інформації.

На першому етапі розвитку концепції забезпечення безпеки, перевага віддавалася технічним засобам захисту. Але практика показала, що для забезпечення ІБ цього не завжди достатньо і з точки зору вартості, реалізація даного підходу не завжди є економічно вигідною, тому почався інтенсивний розвиток альтернативних підходів.

При формування системного підходу до проблеми забезпечення ІБ, виникла необхідність комплексного застосування методів захисту та нових, створених на їх основі засобів і механізмів. На рис. 2.1 наведена класифікація методів і засобів захисту інформації.

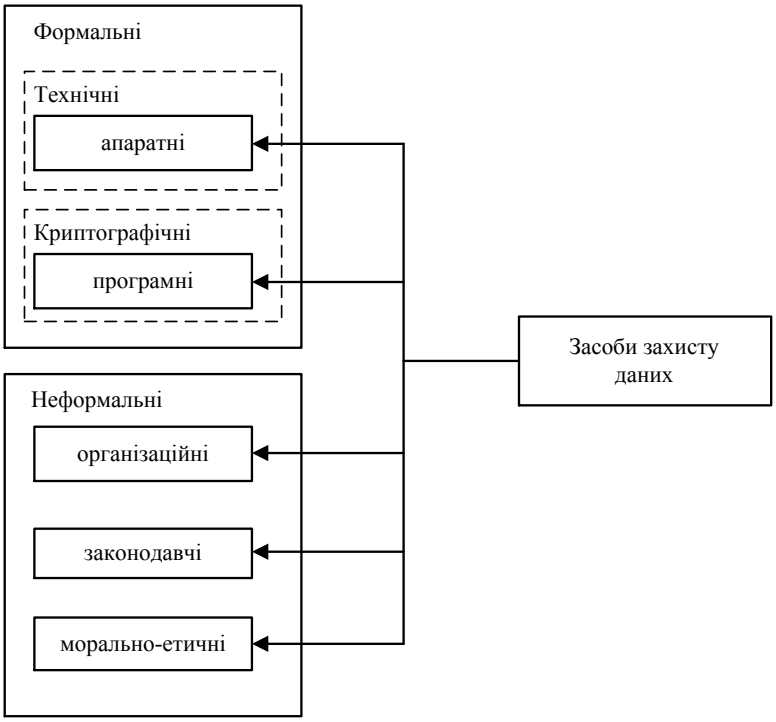

Рисунок 2.1 – Класифікація методів і засобів захисту інформації

2.2 Програмні засоби захисту ПДн

Програмний захист інформації – це система спеціальних програм, які призначені для виконання функцій захисту і включаються до складу програмних засобів систем обробки даних.

Виділяють наступні напрямки використання програм для забезпечення безпеки конфіденційної інформації:

1) Захист інформації від НСД. Для захисту від стороннього вторгнення обов'язково передбачаються певні заходи безпеки, це:

а) ідентифікація суб'єктів і об'єктів;

б) розмежування доступу до обчислювальних ресурсів та інформації;

в) контроль і реєстрація дій з інформацією і програмами.

Процедура ідентифікації і підтвердження автентичності передбачає перевірку, чи є суб'єкт, який здійснює доступ, тим, за кого себе видає.

Найбільш поширеним методом ідентифікації є ідентифікація з використанням пароля. Після виконання процедур ідентифікації та встановлення автентичності, користувач отримує доступ до обчислювальної системи, і захист інформації здійснюється на трьох рівнях: ПЗ, АЗ і даних.

2) Захист від копіювання. Засоби захисту від копіювання запобігають використання нелегальних копій ПЗ і є в даний час єдино надійним засобом, що захищає авторське право розробників. Під такими засобами розуміються засоби, що забезпечують виконання програмою своїх функцій тільки при впізнанні деякого унікального не копійованого елемента. Таким елементом може бути визначена частина комп'ютера, або спеціальний пристрій.

3) Захист інформації від руйнування. Одним із завдань забезпечення безпеки для усіх випадків користування комп'ютером є захист інформації від руйнування. Так як причини руйнування інформації досить різноманітні, то проведення захисних заходів обов'язково для усіх користувачів комп'ютера.

Програмний захист інформації є найбільш поширеним видом захисту, чому сприяють такі позитивні властивості даного засобу, як універсальність, гнучкість, простота реалізації, практично необмежені можливості зміни і розвитку.

2.2.1 Операційне середовище функціонування

Для надання МІС, сертифікату відповідності КСЗІ, ПЗ захисту інформації ІС повинні бути включені до переліку засобів технічного захисту інформації, дозволених для забезпечення технічного захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом [21]. Таким чином, система захисту інформації, яка використовує ПЗ (наприклад ОС, СКБД або сервер додатків), яке не включене до переліку ДССЗЗІ, не зможе отримати позитивний експертний висновок за результатами

державної експертизи в сфері програмного захисту інформації, тому що її загальносистемне ПЗ не відповідає висунутим вимогам.

Повнофункціональна робота МІС не можлива без використання в ній ОС. На даний момент, перелік ДССЗЗІУ налічує декілька сертифікованих програмних рішень, що відносяться до класу «ОС», але більшість з функціонуючих МІС, включаючи популярні і лідируючі на ринку рішення, використовують дві з них: «Microsoft Windows 10 Professional» і «Ubuntu*Pack 18.04». Дані ОС призначені для програмного захисту інформації з обмеженим доступом, яка циркулює на АРМ або Сервері. Вони забезпечують комплексний захист інформаційних об’єктів при обробці даних. Зазначені вище програмні продукти максимально відповідають вимогам щодо надійності роботи, державним та міжнародним відкритим стандартам, тому саме ці ОС можуть бути потенційно застосовані для МІС.

2.2.2 Прикладне середовище функціонування

Для повноцінного функціонування МІС, а саме зберігання даних, в її архітектурі присутні сервери БД. В свою чергу для забезпечення їх роботи використовується спеціальне програмне середовище – система керування БД. В галузі ДССЗЗІ такою системою є програмний продукт «Microsoft SQL Server 2019» (рекомендовано 2019).

2.2.3 Засоби антивірусного захисту інформації

Для досягнення найбільшого ефекту при організації захисту інформації, необхідно керуватися рядом принципів. Найбільш важливим принципом є обов’язкова наявність сертифікованих засобів антивірусного захисту інформації, як складової частини КСЗІ. На сьогоднішній день в Україні, такими засобами є програмні продукти «ESET» і «Avast Premium Security», експертні висновки яких підтверджують відповідність даної продуктової лінійки нормативним документам, які регламентують вимоги до засобів технічного захисту інформації згідно діючого законодавства України. Таким чином, рішення «ESET» і «Avast Premium Security» можуть бути використані у всіх державних, фінансових, міжнародних та інших організаціях.

Антивірусне ПЗ «ESET» призначене для захисту робочих станцій користувачів від дій шкідливого ПЗ, та реагування на виявлення даних програм та інформації, а також мережевих атак. Відповідає вимогам нормативних документів системи технічного захисту

інформації в Україні в обсязі функцій, зазначених у технічній документації, сукупність яких визначається функціональним профілем.

Програмний комплекс антивірусного захисту «Avast» забезпечує ІБ окремих ПК, корпоративних обчислювальних мереж, шляхом багаторівневого захисту інформаційних ресурсів ЕОМ від проникнення шкідливих та потенційно небезпечних об’єктів з будь-яких зовнішніх джерел.

2.2.4 Засоби криптографічного захисту інформації

Для підвищення рівня безпеки інформації в МІС, як правило, додатково використовуються засоби криптографічного захисту інформації, які мають позитивний експертний висновок за результатами державної експертизи в сфері криптографічного захисту інформації.

Криптографічні засоби захисту інформації – це сукупність спеціальних методів шифрування, кодування, або іншого перетворення даних, в результаті якого їх зміст стає недоступним для противника без надання ключа криптограми і зворотного перетворення.

Криптографічний метод захисту, безумовно, самий надійний метод захисту, так як охороняється безпосередньо сама інформація, а не доступ до неї. Даний метод захисту реалізується у вигляді програм або пакетів програм.

Узагальнена схема криптографічної системи, що забезпечує шифрування даних, які передаються, наведена на рисунку 2.2. Відправник генерує відкритий текст вихідного повідомлення *M*, яке повинно бути передано законному одержувачу по незахищеному каналу зв’язку. В цей час, за каналом може стежити зловмисник з метою перехоплення і розкриття переданого повідомлення. Для того щоб зловмисник не зміг дізнатися зміст повідомлення *M*, відправник шифрує його за допомогою зворотного перетворення $E_к(M)$ і отримує шифртекст $C= E_к(M)$, який відправляє одержувачу.

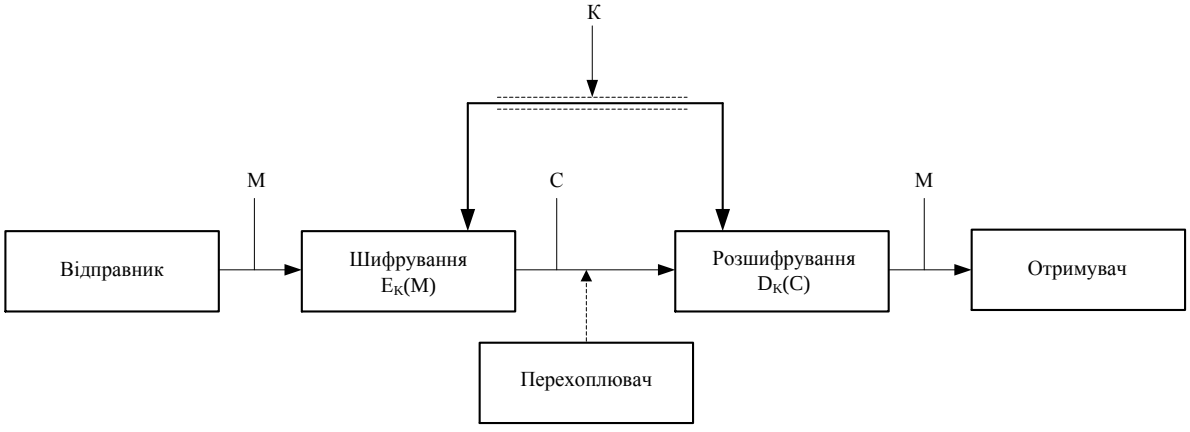

Рисунок 2.2 – Концептуальна схема криптосистеми

Законний одержувач, прийнявши шифртекст *C*, дешифрує його за допомогою зворотного перетворення (2.1) і отримує вихідне повідомлення у вигляді відкритого тексту *M*.

$$D = E^{-1} \tag{2.1}$$

Криптосистема має різні варіанти реалізації: набір інструкції, АЗ, комплекс програм комп'ютера, які дозволяють зашифрувати відкритий текст і дешифрувати зашифрований текст різними способами, один з яких вибирається за допомогою конкретного ключа *K*.

Для шифрування/дешифрування даних в КСЗІ використовуються сертифіковані криптографічні алгоритми:

- алгоритм шифрування/дешифрування ДСТУ ГОСТ 28147-2009;
- алгоритм створення та перевірки ЕЦП ДСТУ 4145-2002;
- алгоритм розрахунку геш-функцій ГОСТ 34.311-95;
- протокол Діффі-Гелмана;
- алгоритм генерації випадкових двійкових послідовностей А ДСТУ 4145-2002.

Алгоритм шифрування даних ДСТУ ГОСТ 28147:2009

В галузі КСЗІ Україні діють чотири стандарти: ГОСТ 28147:2009, ГОСТ 34.310-95, ГОСТ 34.311-95, ДСТУ 4145-2002, з яких останні три пов'язані з технологіями ЦП, а перший є стандартом шифрування. Особливістю двох останніх стандартів є те, що для їх реалізації необхідно застосовувати алгоритм ГОСТ 28147:2009.

ГОСТ 28147:2009 є українським стандартом симетричного шифрування. Повна назва – «ДСТУ ГОСТ 28147:2009 Система обробки інформації. Захист криптографічний. Алгоритм криптографічного перетворення» [22]. Блочний алгоритм шифрування на основі мережі Фейстеля. Даний алгоритм шифрує інформацію 64-бітними блоками тому є «блоковим» з використанням 256-бітного ключа шифрування. При цьому виконується 32 раунди перетворень. Сенс схеми Фейстеля полягає в тому, що блок шифрованої інформації розбивається на два, або більше субблоків, частина яких обробляється за певним законом, після чого результат цієї обробки накладається операцією побітового складання по модулю 2 на необроблювані субблоки. Потім субблоки міняються місцями, після чого обробляються знову.

У структурі алгоритму розрізняють:

- основний крок – послідовність дій, що виконується в кожному базовому циклі (з різними значеннями підключів);

– базові цикли (*«32-З», «32-Р», «16-З»*) – відрізняються числом повторень основного кроку і порядком використання елементів ключа;

– режими роботи – спеціальні методи забезпечення криптографічної стійкості, що використовують результати шифрування попередніх блоків для шифрування наступних.

Основний крок складається з таких операцій (рис. 2.3):

– один з 32-бітових субблоків даних складається з 32-бітним значенням ключа раунду K_i по модулю 2^{32};

– результат попередньої операції розбивається на 8 фрагментів по 4 біта, які паралельно «проганяються» через 8 таблиць замін S1 ... S8;

– 4-бітові фрагменти (після замін) об'єднуються назад у 32-бітний субблок;

– значення отриманого субблоку циклічно зсувається вліво на 11 біт.

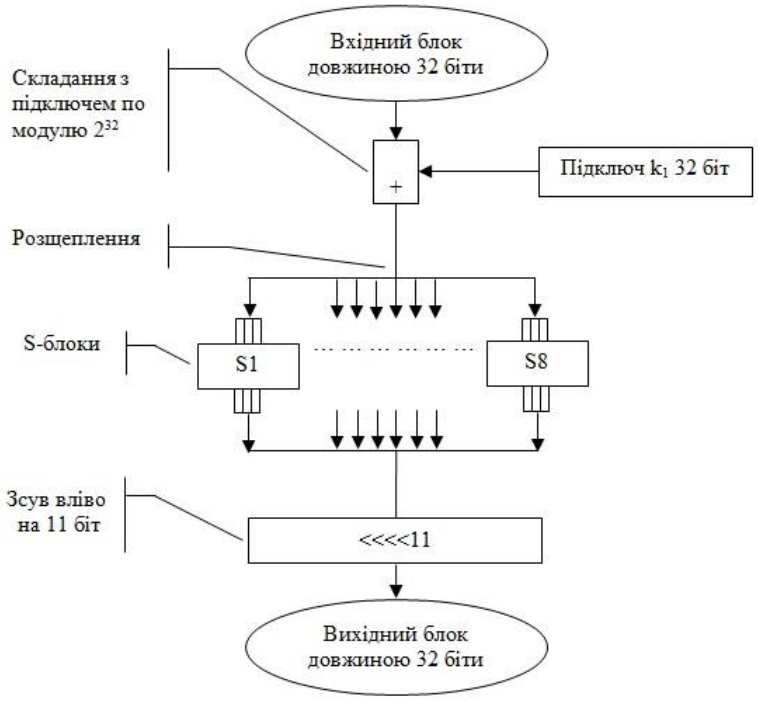

Рисунок 2.3 – Структура функції шифрування для ГОСТ 28147:2009

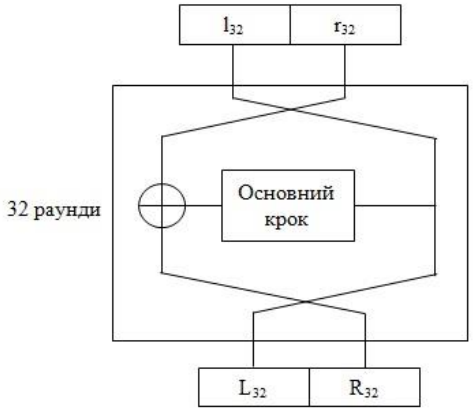

Рисунок 2.4 – Структура алгоритму ГОСТ 28147:2009

Ключі генеруються за рахунок розбивання 256-бітного ключа на вісім 32-бітових підключів. Оскільки алгоритм має 32 раунди, кожен підключ використовується в чотирьох раундах за схемою наведеною на рисунку 2.5.

Раунд	1	2	3	4	5	6	7	8
Підключ	1	2	3	4	5	6	7	8
Раунд	9	10	11	12	13	14	15	16
Підключ	1	2	3	4	5	6	7	8
Раунд	17	18	19	20	21	22	23	24
Підключ	1	2	3	4	5	6	7	8
Раунд	25	26	27	28	29	30	31	32
Підключ	8	7	6	5	4	3	2	1

Рисунок 2.5 – Схема використання підключів при шифруванні в ГОСТ 28147:2009

Тобто в раундах шифрування послідовно використовуються 32-бітові фрагменти K_1 ... K_8 вихідного 256-бітного ключа шифрування в наступному порядку: K_1, K_2, K_3, K_4, K_5, K_6, K_7, K_8, за винятком останніх 8 раундів. В раундах з 25-го по 31-й фрагменти використовуються в зворотному порядку.

Як правило, стійкість алгоритму визначається структурою S-блоків. Входом і виходом S-блоків є 4-бітні числа, тому кожен S-блок може бути представлений у вигляді рядка чисел від 0 до 15, розташованих в певній послідовності. Тоді порядковий номер числа буде вхідним значенням S-блоків, а число – вихідним значенням S- блоків.

Усі вісім S-блоків (табл. 2.1) можуть бути різними. Фактично, вони можуть бути додатковим ключовим матеріалом, але частіше є параметром схеми, загальним для певної групи користувачів.

Таблиця 2.1 – Рекомендовані S-блоки

Номер S-блоку	Значення															
1	4	10	9	2	13	8	0	14	6	11	1	12	7	15	5	3
2	14	11	4	12	6	13	15	10	2	3	8	1	0	7	5	9
3	5	8	1	13	10	3	4	2	14	15	12	7	6	0	9	11
4	7	13	10	1	0	8	9	15	14	4	6	12	11	2	5	3
5	6	12	7	1	5	15	13	8	4	10	9	14	0	3	11	2
6	4	11	10	0	7	2	1	13	3	6	8	5	9	12	15	14
7	13	11	4	1	3	15	5	9	0	10	14	7	6	8	2	12
8	1	15	13	0	5	7	10	4	9	2	3	14	6	11	8	12

Процедура дешифрування аналогічна процедурі шифрування, але з іншим порядком використання фрагментів ключа: в прямому порядку K_1 ... K_8 – у перших 8 раундах; в інших раундах – у зворотному порядку K_8... K_1 (рис. 2.6).

Раунд	1	2	3	4	5	6	7	8
Підключ	1	2	3	4	5	6	7	8
Раунд	9	10	11	12	13	14	15	16
Підключ	1	2	3	4	5	6	7	8
Раунд	17	18	19	20	21	22	23	24
Підключ	1	2	3	4	5	6	7	8
Раунд	25	26	27	28	29	30	31	32
Підключ	8	7	6	5	4	3	2	1

Рисунок 2.6 – Схема використання підключів при дешифруванні в ГОСТ 28147:2009

Така послідовність використання підключів при дешифруванні отримала назву *базовий цикл «32-Р».*

Алгоритм передбачає 4 режими роботи:

– режим простої заміни – є аналогом режиму ECB в DES;

– режим гамування – є аналогом режиму OFB в DES;

– режим гамування зі зворотним зв’язком, або режим гамування із зціпленням блоків – є аналогом режиму CFB в DES;

– режим обчислення імітовставки – є аналогом режиму CBC в DES.

Режим простої заміни приймає на вхід дані, розмір яких кратний 64-м бітам. Результатом шифрування є вхідний текст, перетворений блоками по 64 біта у випадку шифрування циклом «32-З», а в разі дешифрування – циклом «32-Р».

Режим гамування приймає на вхід дані будь-якого розміру, а також додатковий 64-бітовий параметр синхропосилки. В ході роботи синхропосилка перетвориться в циклі «32-З», результат ділиться на дві частини. Перша частина складається по модулю 232 з постійним значенням 101010116. Якщо друга частина дорівнює 232-1, то її значення не змінюється, інакше вона складається по модулю 232-1 з постійним значенням 101010416. Отримане об’єднанням обох перетворених частин значення, яке називають гамою шифру, надходить у цикл «32-З», його результат порозрядно складається по модулю 2 з 64-розрядним блоком вхідних даних. Якщо останній менше 64-х розрядів, то зайві розряди отриманого значення відкидаються. Отримане значення подається на вихід. Якщо ще є вхідні дані, то дія повторюється: складений з 32-розрядних частин блок перетвориться по частинах і так далі.

Режим гамування зі зворотним зв’язком також приймає на вхід дані будь-якого розміру і синхропосилку. Блок вхідних даних порозрядно сумується по модулю 2 з результатом перетворення в циклі «32-З» синхропосилки. Отримане значення подається на вихід. Значення синхропосилки замінюється в разі шифрування вихідним блоком, а в разі дешифрування – вхідним, тобто зашифрованим. Якщо останній блок вхідних даних менше 64 розрядів, то зайві розряди гами (виходу циклу «32-З») відкидаються. Якщо ще є

вхідні дані, то дія повторюється: з результату шифрування заміненого значення утворюється гамма шифру і т.п.

Режим вироблення імітовставки приймає на вхід дані, розмір яких становить не менше двох повних 64-розрядних блоків, а повертає 64-розрядний блок даних, що називається імітовставкою. Тимчасове 64-бітове значення встановлюється в 0, далі, поки є вхідні дані, воно поразрядно складається по модулю 2 з результатом виконання циклу «16-З», на вхід якого подається блок вхідних даних. Для базового циклу «16-З» двічі використовуються елементи ключа з першого по останній. Після закінчення вхідних даних тимчасове значення повертається як результат.

Нижче наведена низка переваг та недоліків характерних алгоритму ГОСТ 28147-2009.

Переваги:

– безперспективність силовий атаки (XSL-атаки в облік не беруться, так як їх ефективність на даний момент повністю не доведена).

– ефективність реалізації і відповідно висока швидкодія на сучасних ПК;

– наявність захисту від нав’язування помилкових даних (вироблення імітовставки);

– у режимі гамування всі елементи гами різні для реальних шифрованих масивів, отже, результат шифрування навіть двох однакових блоків в одному масиві даних буде різним;

– елементи гами виробляються однаковими 64-бітними блоками, але може використовуватися і частина такого блоку з розміром, рівним розміру шифрованого блоку.

Недоліки:

– не можливо визначити криптографічну стійкість алгоритму, не знаючи заздалегідь таблиці замін;

– реалізації алгоритму від різних виробників можуть використовувати різні таблиці замін, які можуть бути несумісні між собою;

– потенційна можливість (відсутність заборони в стандарті) використання таблиць заміни, в яких вузли не є перестановками може призвести до надзвичайного зниження стійкості шифру.

Протокол Діффі-Гелмана

Протокол Діффі-Геллмана – криптографічний протокол, що дозволяє двом і більш сторонам отримати загальний секретний ключ, використовуючи незахищений від прослуховування канал зв’язку. Отриманий ключ використовується для шифрування подальшого обміну за допомогою алгоритмів симетричного шифрування. Вирішальну

роль в цьому типі шифрування грає обмін шифрувальним ключем без можливості перехоплення зловмисником.

В алгоритмі Діффі-Геллмана симетричний сеансовий ключ не генерується і не розподіляється між сторонами. Алгоритм забезпечує формування одного й того ж секретного ключа двома сторонами, який можна використовувати для побудови сеансового ключа в симетричному алгоритмі. Дана процедура називається погодженням ключа: сторони погоджують ключ, який будуть використовувати. Її суть полягає в тому, що кожна зі сторін отримує секретний і відкритий ключ; об'єднання секретного ключа однієї із сторін з відкритим ключем іншої, забезпечує створення одного й того ж самого секретного ключа.

Процес алгоритму Діффі-Геллмана описується наступним чином:

Для початку сторони, А і В, домовляються використовувати кінцеве поле F_q і елемент $g \in F_q$, який породжує групу, що має великий порядок. Для простоти буде розглядатися поле, в якому число p є великим простим числом. Потім сторони А і В можуть знайти елемент g, який породжує групу F_p^*. Кожне число з інтервалу [1, p) можна представити у вигляді (2.2):

$$g^x (mod\ p), \tag{2.2}$$

де x – деяке число. Тепер числа p і q можна використовувати в якості загальних вихідних даних в основному варіанті протоколу обміну ключами Діффі-Геллмана.

Загальні вихідні дані протоколу обміну ключами Діффі-Геллмана:

(p, q): p – велике просте число;

g – породжує елемент групи F_p^*.

Результат:

– елемент групи F_p^*, розділений між користувачами А і В;

– користувач А генерує елемент $a \in U[1, p-1)$, обчислює число $g_a \leftarrow g^a (mod\ p)$ і відправляє його користувачу В;

– користувач В генерує елемент $b \in U[1, p-1)$, обчислює число $g_b \leftarrow g^b (mod\ p)$ і відправляє його користувачу А;

– сторона А обчислює значення $k \leftarrow g_b^a (mod\ p)$;

– сторона В обчислює значення $k \leftarrow g_a^b (mod\ p)$.

З розглянутого вище видно, що значення, яке обчислюється стороною А, виробляється по формулі (2.3), а значення, що обчислюється стороною В по формулі (2.4):

:

$$k = g^{ba}(mod\ p), \tag{2.3}$$

$$k = g^{ab}(mod\ p). \tag{2.4}$$

Опис протоколу Діффі-Геллмана слід доповнити наступними зауваженнями:

– просте число p слід вибирати так, щоб число p-1 мало достатньо великий простий множник p' (2.5):

$$p' > 2^{160}; \tag{2.5}$$

– число p не повинно бути породжуваним елементом групи F_p^*

Необхідно лише, щоб воно було породжуваним елементом її підгрупи, що має достатньо великий порядок, наприклад, підгрупи порядку p'. В цьому випадку користувачі А і В повинні перевірити умови (2.6):

$$g \neq 1 \text{ и } g^{p'} \equiv 1(mod\ p). \tag{2.6}$$

З цієї причини число p' має бути частиною загальних вихідних даних;

– сторона А (відповідно В) повинна перевірити умови (2.7):

$$g_b \neq 1 \text{ (відповідно } g_a \neq 1). \tag{2.7}$$

Ця умова гарантує, що для обраного нею ступеня, який належить інтервалу (1, p'), розділений ключ g^{ab} буде елементом підгрупи порядку p'групи F_p, тобто елементом достатньо великої підгрупи;

– після закінчення протоколу користувач А (а відповідно і В) повинен стерти свою ступінь a. Цим вони забезпечують завчасну секретність ключа g^{ab}.

Нижче наведена низка переваг та недоліків відносно протоколу Діффі-Геллмана.

Переваги:

– можливість будь-якій стороні змінювати власний секретний ключ без узгодження з іншою стороною і отримуючи при цьому кожен раз унікальний ключ шифрування.

Недоліки:

– відсутність взаємної автентифікації сторін.

Цифровий (електронний) підпис

Відповідно до Закону України «Про електронний цифровий підпис» [23], який визначає правовий статус ЕЦП, регулює відносини, що виникають при його використанні, і дає визначення терміну ЕЦП.

ЕЦП – це вид електронного підпису, призначений для забезпечення діяльності фізичних та юридичних осіб, яка здійснюється з використанням електронних документів. Формується даний вид підпису в результаті криптографічного перетворення набору електронних даних, який додається до цього набору або логічно з ним поєднується, і дає змогу підтвердити його цілісність та ідентифікувати особу, яка створила такий підпис. Електронний ЦП накладається за допомогою особистого ключа та перевіряється за допомогою відкритого ключа.

Електронний підпис – це дані в електронній формі, які додаються до інших електронних даних або логічно з ними пов’язані та призначені для гарантії того, що повідомлення було відправлено саме тим, хто називає себе відправником. Електронний підпис грає фундаментальну роль в автентифікації і авторизації.

Система ЦП припускає, що кожен користувач мережі має свій особистий ключ (зберігається в таємниці), який використовується для формування підпису, а також відповідний цьому особистому ключу відкритий ключ, відомий решті користувачів мережі і призначений для перевірки підпису. ЦП обчислюється на основі особистого ключа відправника інформації й власне інформаційних бітів документу (файлу). Спосіб обчислення ЦП гарантує, що знання відкритого ключа не може призвести до підробки підпису.

Алгоритм ДСТУ 4145-2002

ДСТУ 4145-2002 «Інформаційні технології. Криптографічний захист інформації. ЦП, що ґрунтується на еліптичних кривих. Формування, та перевірка» – національний стандарт України, що описує алгоритми формування та перевірки ЕЦП. Криптографічна стійкість ЦП базується на складності задачі дискретного логарифмування в циклічній підгрупі групи точок еліптичної кривої.

До системних параметрів ЦП належать:

– параметри основного поля (2.8);

$$GF(2^m), \tag{2.8}$$

де m – степінь основного поля – непарне просте число;

– коефіцієнти еліптичної кривої виду (2.9);

$$y^2 + xy = x^3 + Ax^2 + B, \tag{2.9}$$

де $A, B \in GF(2^m)$, $B \neq 0,\ A \in \{0,1\}$;

– базова точка еліптичної кривої P, що породжує підгрупу E_n групи E;

– порядок базової точки n (просте число);

– довжина $L(n)$ представлення числа n у двійковому виді;

– ідентифікатор iH геш-функції, яка застосовується в мережі;

– довжина ЦП L_D (довжина блоку даних, що містить ЦП).

Реалізація співвідношень, що задають операції в групі E кривої над $GF(2^m)$, суттєво відрізняються від реалізації співвідношень для простого поля $GF(p)$ характеристики $p>3$.

Наявність полінома (2.10):

$$f(t) = t^m + f_{m-1}t^{m-1} + \cdots + f_0,\ f_i \in GF(2),\ i = 0, \dots,\ m-1\ , \tag{2.10}$$

необхідна для виконання модульних операцій виду $a(t)(mod\ f(t))$ над двійковими векторами коефіцієнтів поліномів розмірності m – елементами $GF(2^m)$.

Всі поліноми $f(t)$, що рекомендовані у стандарті, мають три, або п’ять ненульових коефіцієнтів і вибрані з урахуванням оптимізації обчислень.

Для множення точки $P \neq O$ на велике ціле число, як зауважено у стандарті, можна використовувати способи, цілком аналогічні тим, що застосуються для піднесення цілого числа до ступеня k.

Наприклад, якщо (2.11) – двійкове зображення числа k, то точку $Q = kP$ можна обчислити наступним чином:

$$k = \sum_{t=0}^{t-1} k_i\, 2^i, \tag{2.11}$$

– присвоїти Q значення O;

– для i від t-1 до 0 присвоїти (2.12), якщо $k_i = 0$, інакше, якщо $k_i = 1$, обчислити (2.13):

$$Q \coloneqq 2Q, \tag{2.12}$$

$$Q \coloneqq 2Q + P. \tag{2.13}$$

Однією з особливостей ДСТУ 4145-2002 є можливість застосовувати довільні геш-функції *H(T)* повідомлення *T* з довжиною геш-коду $L_H \geq 160$.

Вони розрізняються значенням ідентифікатора *iH*. Геш-функції функції, однак, мають узгоджуватися з уповноваженим органом. Значення геш-кодів розширяється зліва нулями, або частина значущих розрядів зліва відкидається так, щоб довжина геш-коду дорівнювала 256.

За замовчуванням, без узгодження, а також без ідентифікатора, дозволяється використовувати геш-функцію, встановлену ГОСТ 34.311-95. Таким чином, ДСТУ 4145-2002 залежить від ГОСТ 28147-89 за рахунок геш-функції, хоча й не так жорстко, як ГОСТ 34.310-95.

Інша особливість полягає у запису ЦП (2.14), а не *D=r,s*, який представляється, як двійковий рядок *D* довжини (2.15).

$$D = s, r, \tag{2.14}$$

$$L_D \geq 2L(n). \tag{2.15}$$

До того ж, необхідно, щоб $L_D = 0(mod\ 16)$. Таким чином, довжина L_D може бути надмірною.

Для запису ЦП L_D поле розбивається на дві половини у молодших розрядах лівої половини розміщується *S*, аналогічно, у правій половині розміщується *r*. Позиції зайвих бітів заповнюються нулями.

Особистий (секретний) ключ *d* ЦП обчислюють таким чином:

– за визначеною процедурою, обчислюють випадкове ціле число *d*;

– якщо $d \neq 0$, то d обирають як особистий ключ ЦП, інакше, переходять до попереднього кроку.

Відкритий ключ ЦП обчислюють, як точку еліптичної кривої виду (2.16):

$$Q = -dP, \tag{2.16}$$

де *P* – базова точка еліптичної кривої.

Важливою особливістю алгоритму ДСТУ 4145-2002 є те, що в ньому встановлено обов'язкову для використання схему криптографічного генератора псевдовипадкових чисел.

Алгоритм механізму ЦП ДСТУ 4145-2002:

Основними процедурами алгоритма ЦП, що встановлений ДСТУ 4145-2002 є обчислення передпідпису, обчислення підпису, та перевірка ЦП.

Обчислення передпідпису полягає у виборі першої координати секретної, випадково вибраної точки з орбіти точки P. Вхідні дані до цієї процедури: загальні параметри ЦП. Результат – рандомізатор e та цифровий передпідпис F_e, що відповідає рандомізатору – секретному випадковому лишку за модулем n,

де $0 < e < n$, $F_e \in GF(2^m)$.

Алгоритм обчислення ЦП:

– вибір рандомізатора e на основі криптографічного генератора псевдовипадкових чисел;

– обчислення точки еліптичної кривої (2.17):

$$R = eP = (x_R, y_R), \tag{2.17}$$

– перевірка значення координати x_R (якщо $x_R = 0$, то повторити процедуру з вибору рандомізатора);

– інакше приймають (2.18):

$$F_e = x_R. \tag{2.18}$$

ЦП обчислюється на основі повідомлення, та передпідпису (допускається підготовка масиву передпідписів заздалегідь).

Вхідні дані алгоритму ЦП:

– загальні параметри ЦП;

– особистий ключ ЦП d;

– повідомлення T довжини $L_t > 0$;

– функція гешування $H(T)$, з довжиною геш-коду L_H та ідентифікатором iH;

– довжина ЦП L_D, що вибирається для групи користувачів.

Результат виконання алгоритму: ЦП D повідомлення T і підписане повідомлення у вигляді (iH, T, D).

Для обчислення ЦП виконують наступні дії:

– перевіряється коректність загальних параметрів, ключів, та виконання умов і обмежень, щодо значень проміжних величин, відповідно до процедур, визначених стандартом;

– за повідомленням *T* обчислюють геш-код *H(T)*;

– геш-код *H(T)* перетворюють на елемент основного поля h за встановленою стандартом процедурою і, якщо $h=0$, то приймають $h=1$;

– вибирають рандомізатор e;

– обчислюють ЦП F_e;

– обчислюють елемент основного поля (2.19);

$$y = hF_e \tag{2.19}$$

– за встановленою стандартом процедурою, елемент основного поля y перетворюють на ціле число r (якщо $r=0$, то переходять до вибору нового рандомізатора);

– обчислюють ціле число (2.20), (якщо s=0, то переходять до вибору нового рандомізатора):

$$s = (e + dr) mod\ n, \tag{2.20}$$

– пару цілих чисел (r, s) перетворюють на ЦП D довжини L_D як описано вище.

Результат виконання алгоритму – підписане повідомлення (iH, T, D).

Для перевірки ЦП використовуються:

– загальні параметри ЦП;

– відкритий ключ ЦП Q;

– підписане повідомлення (iH, T, D) довжини (2.21);

$$L = L(iH) + L_T + L_D, \tag{2.21}$$

– функція гешування H.

В результаті виконання алгоритму приймається рішення «підпис дійсний» або «підпис недійсний».

Для перевірки ЦП виконують наступні дії:

– перевіряють коректність загальних параметрів, ключів, та виконання умов і обмежень щодо значень проміжних величин, відповідно до процедур визначених стандартом;

– якщо ідентифікатор геш-функції *iH* у групі користувачів не використовується, то видають «підпис недійсний» і перевірка закінчується;

– виходячи з *iH* (або за промовчанням) визначають L_H;

– перевіряють умови $L_D \geq 2L(n), \quad L_D = 0(mod\ 16)$, якщо хоч одна з них не виконується, вважається, що підпис недійсний і перевірка закінчується;

– перевіряють наявність тексту повідомлення та його довжину (2.22), у випадку відсутності тексту, або при $L_T \leq 0$ – «підпис недійсний» і перевірка закінчується;

$$L_T = L - L_D - L(iH), \tag{2.22}$$

– за повідомленням *T* обчислюють геш-код *H(T)*;

– за встановленою стандартом процедурою, геш-код *H(T)* перетворюють на елемент основного поля *h* (якщо *h=0*, то приймають *h=1*);

– з ЦП *D* вибирають пару цілих чисел (*r*, *s*);

– якщо умова $0 < r < n$, або умова $0 < s < n$ не виконана, то видають «підпис недійсний» і перевірка закінчується;

– обчислюють точку еліптичної кривої (2.23);

$$R = sP + rQ,\ R = (x_R, y_R), \tag{2.23}$$

– обчислюють елемент основного поля (2.24);

$$y = hx_R, \tag{2.24}$$

– за встановленою стандартом процедурою, елемент основного поля *y* перетворюють на ціле число $\widetilde{r}$;

– якщо $r = \widetilde{r}$, то видають повідомлення видають «підпис дійсний», інакше, видають повідомлення видають «підпис недійсний».

Коректність ЦП випливає з порівняння (2.25) і співвідношення (2.26).

$$s = (e + dr) mod\ n_i, \tag{2.25}$$

$$Q = -dP. \tag{2.26}$$

Відповідно, $R = sP + rQ = (e + rd)P - rdP = eP + rdP - rdP = eP$.

Таким чином, при істинному підписі, координата x_R точки $R = (x_R, y_R)$ дорівнює F_e. Тому $y = hx_R = hF_e$ і після перетворення елемента y на ціле число $\widetilde{r}$, має виконуватися рівність $r = \widetilde{r}$, що й доводить коректність алгоритму перевірки ЦП.

Криптографічна стійкість ЦП основана на складності задачі дискретного логарифмування (2.27 – 2.28) в циклічній підгрупі групи точок еліптичної кривої.

$$R = eP, \tag{2.27}$$

$$Q = -dP. \tag{2.28}$$

Криптографічний генератор випадкових послідовностей

В ДСТУ 4145-2002 встановлено процедуру генерації випадкових двійкових послідовностей.

Генератор повинен використовуватися для отримання випадкових цілих чисел, випадкових елементів основного поля і випадкових точок еліптичних кривих, необхідних для побудови загальних параметрів ЦП, обчислення ЦП, а також для побудови відкритих і особистих ключів ЦП. За один цикл роботи генератор видає один випадковий біт.

Як криптографічне перетворення в генераторі застосовується алгоритм ГОСТ 28147:2009 у режимі простої заміни. Ключі перетворення повинні відповідати вимогам цього стандарту. Умови отримання й використання особистого ключа повинні унеможливлювати доступ до нього, або його частини, модифікацію, підміну, або знищення.

Ключі, що використовується в генераторі випадкових послідовностей, використовувати для інших цілей заборонено.

Генератор функціонує наступним чином:

Позначимо через $E_k(.)$ шифрування двійкового рядка довжиною 64 біти алгоритмом ГОСТ 28147-89 в режимі простої заміни на ключі *k*. Нехай *s, D, I, x* – двійкові рядки довжиною 64 двійкові розряди. Перед застосуванням задають початковий стан генератора випадкових послідовностей.

Встановлення початкового стану генератора випадкових послідовностей:

– задають початкове значення *s* генератора. Для цього використовують фізичне джерело випадковості. Як таке джерело можна використовувати, наприклад, квантові

ефекти в напівпровідниках (шумові діоди і т. п.), сигнал від мікрофонного входу з відключеним мікрофоном, часові інтервали між натисканнями на клавіші клавіатури, часові інтервали між натисканнями на клавіші миші. Початковий стан генератора є таємним. Умови отримання початкового стану генератора повинні унеможливлювати доступ до нього або його частини, модифікацію, підміну, або знищення;

– задають значення двійкового рядка *D*. Для цього використовують поточне значення дати і часу з точністю 64 двійкових розрядів;

– обчислюють двійковий рядок (2.29).

$$I = E_k(D). \tag{2.29}$$

Криптографічні геш-функції

В цілому під геширування розуміють перетворення вхідних даних довільної довжини в вихідний бітовий рядок фіксованої довжини. Найчастіше геш-функції застосовують в процесі автентифікації користувача (в БД зазвичай зберігається геш-пароль замість самого пароля) і для обчислення контрольних сум файлів, пакетів даних. Криптографічна геш-функція – особливо значимий базовий елемент, який застосовується в багатьох криптографічних протоколах і алгоритмах. Геш-функція вилучає дані довільного обсягу, кодує їх і відправляє рядок, розмір якого має строго встановлену довжину. Інформація, отримана для шифрування, найчастіше, називається «повідомленням», а рядок з генерованим геш-значенням – «дайджестом».

Використання геш-функцій поширене при організації обміну документами, що містять ЕЦП. Геширується в даному випадку файл, який підписується, для того щоб його одержувач міг упевнитися в тому, що він справжній. Хоча формально геш-функція не входить в структуру електронного ключа, вона може фіксуватися у флеш-пам’яті АЗ, за допомогою яких підписуються документи.

Гешування не є безпосередньо компонентом ЕЦП, однак дозволяє досить ефективно оптимізувати алгоритми задіяння електронного підпису. Так, шифруватися може, власне, тільки геш, а не сам текст повідомлення. В результаті швидкість обробки файлів значно зростає, одночасно стає можливим забезпечувати більш ефективні механізми захисту ЕЦП, так як акцент в обчислювальних операціях в цьому випадку буде ставитися не на обробці вихідних даних, а на забезпеченні криптографічного стійкості підпису.

На сьогоднішній день, неможливо зламати систему, яка використовує у своїй роботі геш-функцію високої криптографічної стійкості, так як для цього потрібно буде

залучати колосальні обчислювальні потужності і витрачати величезну кількість часу на вирішення завдань. З появою кожного нового дайджесту система отримує додатковий захист, який зводить нанівець усі зусилля, сконцентровані в хакерській атаці.

Алгоритм гешування ГОСТ 34.311-95

ГОСТ 34.311-95 «Інформаційна технологія. Криптографічний захист інформації. Функція гешування» – стандарт, який визначає алгоритм і процедуру обчислення геш-функції для будь-якої послідовності двійкових символів, які застосовуються в криптографічних методах обробки і захисту інформації, в тому числі для реалізації процедур ЕЦП при передачі, обробці, та зберіганні інформації в автоматизованих системах.

Процедура обчислення геш-функції:

Початковими даними для обчислення геш-функції є повідомлення $M^* \in B^*$, та вектор ініціалізації (стартовий вектор) $H^* \in V_{256}$,

де $M \in B^*$ – частина послідовності $M^* \in B^*$, що ще не була задіяна у попередніх ітераціях;

$H^* \in V_{256}$ – поточне значення геш-коду;

$\sum \in V_{256}$ – поточне значення контрольної суми;

$L \in V_{256}$ – лічильник (у бітах) поточної довжини вже обробленої у попередніх ітераціях частини повідомлення.

Алгоритм складається з трьох етапів. Основний етап – це етап 3, який використовується у більшості операцій. На кожній такий ітерації обчислюється проміжний геш-код, для чого обробляються останні 256 бітів $M_S \in V_{256}$ послідовності M, що розглядається, як $M = M_P||M_S$. Після обробки блок M_S з послідовності M забирається.

Етап 1. Присвоєння початкових значень:

$$M \coloneqq M^*, \tag{2.30}$$

$$H \coloneqq H^*, \tag{2.31}$$

$$\sum : = 0^{256}, \tag{2.32}$$

$$L \coloneqq 0^{256}. \tag{2.33}$$

Етап 2:

Перевірити умову (2.34). При позитивному результаті перейти на етап 3, інакше, провести заключні обчислення, що приведені нижче:

$$|M| > 256, \tag{2.34}$$

– переобчислити довжину обробленої послідовності (2.35);

$$L := < L + |M| >_{256}, \tag{2.35}$$

– доповнити короткий блок нулями зліва (2.36);

$$M` := 0^{256-|M|}||M, \tag{2.36}$$

– обчислити праві 256 бітів звичайної суми двох великих чисел (2.37);

$$\sum := \sum \oplus` M`, \tag{2.37}$$

– перше змішування проміжного геш-коду (2.38);

$$H := k(M`, H), \tag{2.38}$$

– друге змішування проміжного геш-коду (2.39);

$$H := k(L, H), \tag{2.39}$$

– останнє змішування проміжного геш-коду (2.40);

$$H := k(\sum, H), \tag{2.40}$$

Кінець алгоритму, результат (2.41):

$$h(M^*) = H. \tag{2.41}$$

Етап 3:

Вибрати крайнє праве підслово M_S довжини 256 бітів з повідомлення $M = M_P||M_S$ та виконати наступну послідовність обчислень.

– змішування проміжного геш-коду з блоком повідомлення (2.42);

$$H := k(M_S, H), \tag{2.42}$$

– обчислити нову довжину обробленої послідовності (2.43);

$$L :=< L + 256 >_{256}, \tag{2.43}$$

– обчислити праві 256 бітів звичайної суми двох великих чисел (2.44);

$$\sum := \sum \oplus M_S, \tag{2.44}$$

– відкинути праві 256 бітів послідовності M та перейти на етап 2 (2.45).

$$M := M_P. \tag{2.45}$$

2.3 Запропонована технологія підвищення захисту ПДн в МІС

Для підвищення захисту ПДн та медичних ПДн в МІС, пропонується застосувати:

– подвійний прохід мережевого трафіку через функцію шифрування/ дешифрування;

– передачу даної функції від апаратного шифратора – центральному процесору комп'ютера на якому встановлено АРМ клієнта в МІС;

– вилучити апаратний шифратор зі схеми (рис. 1.1).

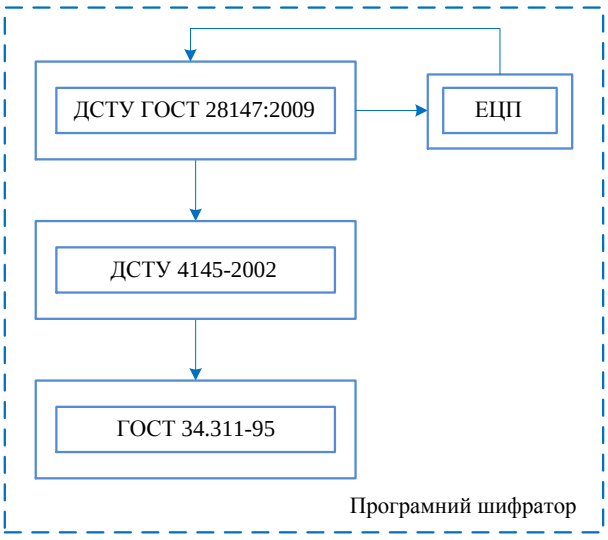

Рисунок 2.7 – Схема подвійного проходу функцій шифрування/дешифрування на програмному шифраторі

Введемо деякі обмеження та умови щодо застосування такої технології:

– подвійний прохід функцій шифрування/дешифрування на процесорі комп’ютера клієнта, повинен реалізовуватися за той же проміжок часу, що і на апаратному шифраторі;

– функція шифрування/дешифрування, яка буде виконуватися на процесорі, повинна використовувати не більше 10% ресурсів даного пристрою, щоб не впливати на його обчислювальні можливості;

– якщо перші дві умови буде підтверджено розрахунками, тоді доцільно вилучити апаратний шифратор/дешифратор концептуальної схеми.

2.4 Висновки до другого розділу

У другому розділі магістерської роботи розглянуто сучасні методи та засоби організації захисту ПДн в МІС, їх класифікація, переваги та недоліки. Проаналізовано найбільш поширені програмні, апаратні та криптографічні підходи до забезпечення безпеки і цілісності конфіденційної інформації. У рамках програмного захисту даних, описано операційне і прикладне середовище функціонування, антивірусні засоби захисту, симетричні/асиметричні алгоритми шифрування, визначення алгоритмічних мов, модулей, принципів їх роботи і взаємодії, методів автентифікації.

Зважаючи на сучасний досвід вирішення проблематики, приклади (аналоги) побудови МІС і ґрунтовний аналіз методів, засобів та шляхів забезпечення ІБ, запропоноване рішення щодо підвищення рівня захисту ПДн та медичних ПДн в МІС. В даній концепції, ІБ забезпечується апаратно-програмними засобами, що володіють чинним позитивним експертним висновком ДССЗЗІ України. Конфіденційність медичної інформації забезпечується бібліотеками криптографічних перетворень:

– шифрування/дешифрування даних згідно алгоритму ДСТУ ГОСТ 28147-2009;

– створення та перевірка ЕЦП згідно алгоритму ДСТУ 4145-2002;

– розрахунок геш-функцій здійснюється відповідно алгоритму ГОСТ 34.311-95;

– формування спільного секрету за протоколом Діффі-Гелмана ДСТУ ISO/IEC 15946-3;

– генерація ключової пари: особистого та відкритого ключа для протоколу Діффі-Гелмана ДСТУ ISO/IEC 15946-3;

– генерація випадкових двійкових послідовностей згідно алгоритму А ДСТУ 4145-2002.

Таким чином, враховуючи вищезазначене запропоноване рішення з метою вибору оптимального варіанта системи захисту інформації, виникає необхідність в практичному дослідженні та оцінці його ефективності.

3 ПРАКТИЧНЕ ДОСЛІДЖЕННЯ ЕФЕКТИВНОСТІ ЗАПРОПОНОВАНОГО МЕТОДА ПІДВИЩЕННЯ ЗАХИСТУ ПДН В МІС

3.1 Розроблене комплексне рішення побудови МІС на основі запропонованої технології підвищення захисту ПДн

Клієнт системи є лікар, медичний персонал, адміністратор медичної системи, та інші співробітники ЛПЗ, які мають можливість роботи з МІС. Права доступу і функції чітко регламентуються (для різних груп користувачів) і керуються адміністратором медичної системи. Для взаємодії з системою суб'єкт повинен підтвердити свою особистість, пройшовши автентифікацію використовуючи систему логування і парольної авторизації в сукупності з ЕЦП.

Комутатор третього рівня виконує управління фізичним розмежуванням доступу до медичної системи.

Шифратор/Дешифратор забезпечує підвищення рівня захисту трафіку, який циркулює між клієнтом та сервером в МІС. В запропонованій архітектурі даний вид пристрою реалізується на процесорі (AMD Ryzen 5 2200G4/ ядра) клієнта МІС.

Сервер є софтовую машиною до складу якої входять ОС, віртуальні машини на які встановлено Сервер БД та Клієнтський додаток.

АЗ – це різні технічні пристрої та системи, призначені для захисту інформації від розголошення, витоку і НСД.

Використання АЗ захисту інформації дозволяє вирішувати наступні завдання:

- виявлення каналів витоку інформації на різних об'єктах і в приміщеннях;
- локалізація каналів витоку інформації;
- пошук і виявлення засобів промислового шпигунства;
- протидія НСД до джерел конфіденційної інформації.

Одним з різновидів АЗ захисту інформації, який входить до складу розробленої комплексної моделі є комутатор.

Комутатор належить до ряду технічних засобів захисту інформації, наявність яких в КСЗІ є обов'язковою. Даний пристрій забезпечує з'єднання вузлів комп'ютерної мережі для організації єдиної системи доступу користувачів до програмних, технічних та інформаційних ресурсів. Комутатор передає дані лише безпосередньо отримувачу. Це підвищує продуктивність і безпеку мережі, позбавляючи інші сегменти мережі від необхідності обробляти дані, які їм не призначалися.

Комутатор третього рівня – пристрій для локальної обчислювальної мережі. Даний комутатор розбиває трафік в локальній мережі між існуючими сегментами. Зазвичай він використовується на рівні розподілу в ієрархічній моделі мережі.

Комутатор третього рівня, як і звичайний комутатор, захоплює усі кадри своїми портами незалежно від їх MAC-адрес, однак порти комутатора третього рівня мають і власні MAC-адреси. Якщо захоплений кадр спрямований на MAC-адресу будь-якого комп'ютера в мережі, то пакет комутується. Якщо захоплений кадр спрямований на MAC-адресу порту комутатора, то пакет маршрутизується. Комутатор третього рівня може підтримувати динамічні протоколи маршрутизації, такі як RIP або OSPF, а може покладатися на статичне завдання маршрутів, або на отримання таблиці маршрутизації від іншого маршрутизатора.

В МІС найбільш доцільним в плані технічної реалізації є використання комутатору третього рівня. Це пояснюється тим, що дані засоби мають безліч технічних новинок, завдяки яким мережа легка в адмініструванні, зручна в налаштуванні, а також присутня можливість з'єднатися з сервером та вихід в Internet по стандарту Gigabit Ethernet IEEE 802.3 1000BaseT.

Firewall

При роботі в глобальних мережах загального користування, зокрема в Internet, крім традиційних способів антивірусного захисту даних в ІС, стає актуальним контроль усього вхідного і вихідного мережевого трафіку. Це може бути здійснено шляхом інтеграції такого компонента, як firewall (міжмережевий екран, брандмауер), покликаного контролювати доступ до інформації з боку користувачів зовнішніх мереж.

Firewall уможливлює фільтрацію вхідного і вихідного трафіку, що йде через систему. Брандмауер використовує один, або більше наборів «правил» для перевірки мережевих пакетів при їх вході, або виході через мережеве з'єднання, він або дозволяє проходження трафіку, або блокує його. Крім того, мережеві екрани, як правило, володіють великим набором налаштувань. Проходження трафіку на мережевому екрані можна налаштовувати по службам, IP-адресам відправника і одержувача, по ідентифікаторам користувачів, які роблять запит на службу. Firewall дозволяє здійснювати централізоване управління безпекою. В одній конфігурації адміністратор може налаштувати дозволений вхідний трафік для усіх внутрішніх систем організації. Це не позбавляє від необхідності в оновленні та налаштуванні систем, але дозволяє знизити ймовірність неправильного конфігурування однієї, або декількох систем, в результаті чого ці системи можуть піддатися атакам на некоректно налаштовану службу.

Іншими словами, firewall захищає комп'ютерні мережі, або конкретні вузли від НСД, злому хакерами ззовні, і блокує підозрілі ресурси.

Для корпоративної мережі ЛПЗ дані функціональні можливості брандмауерів дуже важливі, оскільки зловмисники можуть проникнути в мережу, зашифрувати, пошкодити, або навіть знищити дані.

Брандмауер може бути апаратним, програмним, або змішаного типу. В КСЗІ, як правило використовується третій тип. На даний момент, перелік ДССЗЗІ України налічує декілька моделей сертифікованого апаратного рішення «Check Point Security Management», що відносяться до класу «міжмережевий екран».

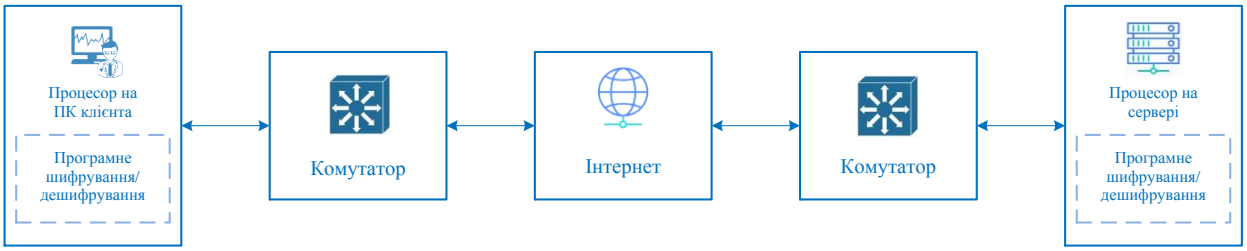

Рисунок 3.1 – Розроблене комплексне апаратно-програмне рішення побудови МІС в ЛПЗ

3.2 Вимоги до апаратних та програмних засобів для комплексного рішення

Нижче наведено мінімальні, та рекомендовані вимоги до апаратних і програмних складових, що застосовуються у комплексному рішенні (табл. 3.1 – 3.2).

Таблиця 3.1 – Вимоги до АЗ комплексного рішення

АЗ			
АРМ адміністраторів/ клієнтів	**Назва**	**Мінімальні характеристики**	**Рекомендовано**
	Процесор	2 ядра/2-3 ГГц Intel або симулятор AMD	4 ядра/AMD Ryzen 5 2200G
	Оперативна пам'ять	DDR4; 4 ГБ	DDR4; 8 ГБ (в одному слоті)
	Жорсткий диск	500 ГБ 7200 rpm SATA 3	SSD 240 ГБ
	Порт	2x USB 2.0, 2x USB 3.0; 1 VGA; 1 RJ-45; 10/100/1000 ГбЕ	2xUSB 2.0, 2xUSB 3.0; 1 VGA; 1 RJ-45; 10/100/1000 ГбЕ
Монітор	Розширення	FHD (1920x1080 @ 60 Hz)	FHD (1920 x 1080 @ 60 Hz)
	Порт	VGA	VGA
Фізичний сервер	Процесор	x86 / x64-сумісні автоматизовані системи з такими мінімальними (min) та основними характеристиками: 1x ЦП Intel Xeon E5-2600 v4 min - 8 ядер; min - 2,2 ГГц	x86 / x64-сумісні автоматизовані системи з такими min та opt основними характеристиками: 1x ЦП Intel Xeon E5-2600 v4 min - 8 ядер; min - 2,2 ГГц

Продовження таблиці 3.1 – Вимоги до АЗ комплексного рішення

АЗ			
	Назва	**Мінімальні характеристики**	**Рекомендовано**
Фізичний сервер	Оперативна пам’ять	DDR4, 32 ГБ, DIMM, 2133 Гц	DDR4, 32 ГБ, DIMM, 2133 Гц
	Швидке сховище	1x (-SSD) в RAID 10 для ОС	2x (250 МБ - SSD) в RAID 10 для ОС
	Звичайне сховище	1x (1 ТБ, жорсткий диск, min 10 КБ) в RAID 10	4x (1 ТБ, жорсткий диск, min 10 КБ) в RAID 10
	Система зберігання даних (сховище backup)	1x Removable HDD Min 1 ТБ SSD	1x Removable HDD Min 1 ТБ SSD
Засіб КЗІ	Засоби КЗІ, які мають позитивний експертний висновок за результатами державної експертизи в сфері криптографічного захисту інформації.		
Шифратор / дешифратор	-	ІІТ IP-шифратор Канал-201	ІІТ IP-шифратор Канал-201
Комутатор (третього рівня)	-	TP-Link T1600G-28TS або його аналог	TP-Link T1600G-28TS або його аналог
Джерело безперебійного живлення	Має потужність ні менш ніж 900 Вт та спроможне забезпечити роботу, з максимальною потужністю, на протязі ні менш ніж 10 хвилини.		

Таблиця 3.2 – Вимоги до програмних забезпечення комплексного рішення

Апаратне забезпечення			
АРМ адміністраторів/ клієнтів	**Назва**	**Мінімальні характеристики**	**Рекомендовано**
	ОС	ОС MS Windows 10 (Professional) або Ubuntu*Pack 18.04	ОС MS Windows 10 (Professional) або Ubuntu*Pack 18.04
	Антивірусний засіб захисту інформації	ESET або Avast Premium Security - програмні продукти антивірусного захисту інформації, які мають позитивний експертний висновок за результатами державної експертизи в сфері технічного захисту інформації.	ESET або Avast Premium Security - програмні продукти антивірусного захисту інформації, які мають позитивний експертний висновок за результатами державної експертизи в сфері технічного захисту інформації.
	Офісний пакет додатків	MS Office 2016 Pro	MS Office 2016 Pro
	СКБД	MS SQL Server 2019	MS SQL Server 2019
Засіб КЗІ	Бібліотеки криптографічних перетворень, які мають позитивний експертний висновок за результатами державної експертизи в сфері криптографічного захисту інформації: ДСТУ ГОСТ 28147-2009; ДСТУ 4145-2002; А ДСТУ 4145-2002; протоколом Діффі-Гелмана; ГОСТ 34.311-95.		
Шифратор/ дешифратор	-		
Комутатор (третього рівня)	-		
Джерело безперебійного живлення	-		

3.3 Критерії оцінки системи захисту ПДн

При формуванні критеріїв оцінки ефективності того, чи іншого комплексного рішення, необхідно враховувати, що дана система функціонує в ЛПЗ і оперує таким видом даних, як ПДн та медичні ПДн, тому вимоги до цих систем декілька відрізняються.

Критерії оцінки ефективності МІС:

1) захищеність системи;
2) обов'язкова наявність сертифікованих ДССЗЗІ засобів;
3) вартість системи;
4) трудомісткість впровадження та обслуговування системи;
5) швидкість передачі, шифрування/дешифрування даних;
6) надійність системи в цілому (при використанні тих, чи інших засобів захисту інформації).

На основі цих критерій робиться висновок про відповідність чинному законодавству запропонованого комплексного рішення, та його складових, та можливість сертифікації ДССЗЗІ.

3.4 Методика порівняння сучасних засобів захисту інформації, які використовуються в побудові КСЗІ при впровадженні в МІС

За останні роки, значно підвищилась продуктивність сучасних процесорів. З появою нових інструкцій, розробники середовищ для програмування, додали до своїх бібліотек нові функції, які забезпечили більш ефективніше написання програмного коду. Технології багато поточного програмування, дозволяють більш ефективніше використовувати багатоядерні процесори, які вже давно стали нормою, і застосовуються в сучасній техніці. Використання більш потужних процесорів, дозволяє перенести більшу частину обчислювальних задач з окремих апаратних пристроїв до центрального процесору. Таким чином, збільшується функціональність пристроїв і підвищується швидкість обробки даних. Враховуючи вищезазначене, такі досягнення ІТ надають можливість перенести частину задач, які вирішували окремі АЗ у програмний код, який буде виконуватися центральним процесором. Програмні застосунки розроблені з урахуванням особливостей функціонування центрального процесора зможуть замінити такі окремні апаратні засоби, як шифратори/дешифратори мережевого трафіку. Ці засоби, як правило використовуються в побудові КСЗІ. Якщо припустити, що задачу шифрування/дешифрування мережевого трафіку можливо перенести до програмного коду, який буде

виконуватися процесором комп'ютера клієнта МІС таким чином, щоб виконання цієї задачі не заважало роботі цього комп'ютера, то це дало б можливість не використовувати АЗ шифрування/дешифрування і зменшило вартість побудови КСЗІ, що спростило використання таких систем у подальшому.

Для того, щоб підтвердити чи спростувати цей факт, необхідно зробити обчислення, що до навантаження задачі шифрування/дешифрування мережевого трафіку сучасним процесором, який використовується комп'ютером клієнта та порівняти отримані результати з роботою апаратного шифратора.

3.5 Дані для експериментів

Як було зазначено раніше, процесор клієнта повинен виділяти на задачі шифрування/дешифрування мережевого трафіку не більше 10% своїх ресурсів, щоб не заважати роботі системних програм, які використовуються. Для порівняльного аналізу в якості досліджуваного процесору обрано AMD Ryzen 5 2200G, який є рекомендованим для використання на комп'ютері клієнта МІС.

Таблиця 3.3 – Характеристика досліджуваних апаратних компонентів процесора комп'ютера на якому працює АРМ клієнта

Характеристика процесора комп'ютера АРМ клієнта			
Назва			
Процесор	4 ядра /AMD Ryzen 5 2200G	$F_{такт}$	3,5 ГГц
		$T_{такт}$	0,25 ГГц
Оперативна пам'ять	DDR4-2666	$F_{такт}$	1333 МГц
		$F_{дата}$	2666 МГц
		$T_{такт}$	0,94 нс
		$T_{дата}$	0,47 нс
	Таймінг	Латентність CAS	15
		Затримка RAS to CAS	15
		Час зарядки RAS	15

В якості досліджуваного апаратного шифратора/дешифратора використовується ІІТ IP-шифратор «Канал-201», який є чиним, і входить до переліку сертифікованих засобів ДССЗЗІ України.

Таблиця 3.2 – Характеристики шифратора/дешифратора для практичного порівняння

Характеристика шифратора			
Назва			
Шифратор	ІІТ IP-шифратор «Канал-201»	2 x Ethernet 10/100/1000	
		Швидкість шифрування (обробки IP-пакетів)	125 Мбіт/с

Зважаючи на вищенаведену інформацію та функціональні можливості пристрою, можна зробити висновок, що навантаження на процесор шифратора буде близько 90% а 10% піде на вирішення інших службових задач.

Для початку треба розрахувати максимальну швидкість передачі даних з використанням ресурсів ПК клієнта, скориставшись формулою 3.1.

$$\text{ШПД}_{max} = F_{\text{дата}} \times \text{розрядність} = 2666 \text{ МГц} * 64 = 17064 \text{ Мбайт/с}. \quad (3.1)$$

Час отримання даних

З регістрів і кеша, дані можуть бути надані протягом робочого такту (регістри, кеш 1-го рівня), або із затримкою в декілька тактів процесора для кеша 2-го і 3-го рівня.

У випадку з ОП ситуація інакша:

– час вибору рядка становить: 15 clk × 0,94 нс = 14 нс

– час до отримання даних з команди вибору стовпця: 15 clk × 0,94 нс = 14 нс

– час закриття рядка: 15 clk × 0,94 нс = 14 нс

З цього можна зробити висновок, що час між командою, яка запитує дані з ячейки пам’яті (у разі якщо до кешу не потрапили) може змінюватися:

14 нс – дані уже знаходяться у вибраному рядку;

28 нс – дані знаходяться в іншому рядку за умови, що попередній рядок вже закритий (блок в стані «idle»);

42-50 нс – дані знаходяться в іншому рядку, при цьому поточний рядок потребує закриття.

Кількість операцій, які може виконати вищезазначений процесор за цей час становить від 56 (14 нс) до 200 (50 нс зміна рядка). Також, окремо варто відзначити, що до часу між командою вибору стовпця і отриманням усього пакету даних додається і затримка завантаження рядка кешу: 8 біт пакету × 0,47 нс = 3,76 нс.

Для ситуації коли дані будуть доступні «програмі» тільки після завантаження рядку кешу, можна отримати ще до 15-ти пропущених тактів.

Повністю позбавитися від впливу пропускної здатності пам'яті можливо тільки в операціях послідовного звернення до пам'яті, в разі довільного доступу збільшується час обробки з 4-10 нс (послідовний доступ) до 60-120 нс (зміна рядків), що дає різницю в швидкості обробки в 12-15 разів.

Швидкість обробки даних

Для обраного модуля пікова пропускна здатність – 17064 Мбайт/с, що з частотою в 3,6 ГГц дає можливість обробляти за такт 32-х бітні слова (17064 Мб / 3600 МГц = 4,74 байт на такт). У зв'язку з цим накладаються наступні обмеження:

– без планування завантаження кешу, процесор буде змушений простоювати (чим вище частота, тим довше ядро простує);

– в циклах «читання – модифікація – запис» швидкість обробки знижується в два рази;

– багатоядерні процесори розділять між ядрами пропускну здатність шини пам'яті, а при виникненні ситуації з конкуруючими запитами (вироджених випадок), продуктивність роботи пам'яті може погіршитися в «200 разів (зміна рядків) * X ядер».

Тепер можна розрахувати:

$$\frac{\text{Пікова пропускна здатність}}{\text{кількість ядер}} = \frac{17064\ \text{Мбайт}/c}{4\ \text{ядра}} = 4266\ \text{Мбайт/с}$$ – на ядро в оптимальному випадку;

$$\frac{\text{Пікова пропускна здатність}}{\text{кількість ядер}} = \frac{17064\ \text{Мбайт}/c}{4\ \text{ядра} \times 200\ \text{пропущених операцій}} = 21{,}73\ \text{Мбайт/с}$$ – на ядро для виродженого випадку.

В даному практичному досліджені, для отримання об'єктивних результатів необхідно, шляхом введення обмеження на кількість ресурсів, які будуть виділятися на вирішення задачі шифрування/дешифрування, а саме – 10% обчислювальної потужності процесору, відповідно максимальна (пікова) швидкість шифрування/дешифрування складає (3.4):

$$4266\ \text{Мбайт/с} \times 10\% = 42{,}66\ \text{Мбайт/с} \quad (3.4)$$

Для виродженого випадку (3.5):

$$21{,}73\ \text{Мбайт/с} \times 10\% = 2{,}173\ \text{Мбайт/с} \quad (3.5)$$

Таким чином можна розрахувати швидкість обробки шифрування/дешифрування при половинному навантаженні (3.6):

$$4266\ \text{Мбайт/с} \times 5\% = 21{,}33\ \text{Мбайт/с} \quad (3.6)$$

Шифратор «Канал-201», згідно з паспортом здатний мати продуктивність до 125 Мбіт/с або 15,63 Мбайт/с.

Таблиця 3.3 – Результати розрахунків швидкості операцій шифрування/дешифрування на процесорі комп'ютера клієнта та на апаратному шифраторі

Характеристика процесора і шифратора			
Назва	**Модель**	**Кількість ресурсів пристрою під операцію**	**Швидкість шифрування**
Процесор	4 ядра /AMD Ryzen 5 2200G	10%	42,66 Мбайт/с
		5%	21,33 Мбайт/с
Апаратний шифратор	ІІТ IP-шифратор «Канал-201»	90%	15,63 Мбайт/с

Таким чином, результати розрахунків підтверджують, що сучасні процесори в змозі без особливого навантаження виконувати обчислювальні задачі деяких окремих апаратних пристроїв. В даному випадку, процесор AMD Ryzen 5 2200G, який рекомендовано для використання на комп'ютері клієнта МІС, може без зайвих зусиль, а саме використовуючи лише 5% своїх обчислювальних потужностей виконувати задачі по шифруванню / дешифруванню мережевого трафіку, які на сьогоднішній день покладені на апаратний шифратор ІІТ IP-шифратор «Канал-201», який використовується в побудові КСЗІ при впровадженні МІС.

Виходячи з того, що накладалися обмеження у вигляді 10% на функції шифрування/дешифрування, а розрахунки підтверджують, що 5 % ресурсів цілком достатньо для цих задач, і що інші 5 %, які не буде задіяно можна буде використовувати на будь-які інші потреби. Цих 5% буде достатньо для другого проходу функції шифрування/дешифрування.

3.6 Висновки до третього розділу

В третьому розділі магістерської роботи запропонована технологія підвищення захисту ПДн. Проведено практичне дослідження та відповідні розрахунки ефективності розробленого комплексного рішення з використанням запропонованої технології.

Отримані результати наглядно демонструють, що швидкість функцій шифрування/дешифрування, які виконані на процесорі комп'ютера клієнта системи з накладанням обмеження щодо використання 10% системних ресурсів, в 2,5 рази більша ніж швидкість виконання тих самих задач на апаратному шифраторі.

Враховуючи це, використання в якості шифрування/дешифрування процесора, який рекомендується для застосування на комп'ютері клієнта МІС, дає можливості щодо:

– підвищення швидкодії функцій шифрування/дешифрування;

– зменшення вартості обладнання, що використовується при побудові КСЗІ тому що ринкова ціна апаратного ІІТ IP-шифратора «Канал-201» складає 1000 USD, в той час, як вартість процесора AMD Ryzen 5 2200G складає 100 USD;

– запровадження такої технології при побудови КСЗІ для МІС.

4 ОХОРОНА ПРАЦІ ТА БЕЗПЕКА В НАДЗВИЧАЙНИХ СИТУАЦІЯХ

В даному розділі проведено аналіз потенційних небезпечних та шкідливих виробничих факторів, причин пожеж. Розглянуті заходи, які дозволяють забезпечити гігієну праці і виробничу санітарію. На підставі аналізу розроблені заходи з техніки безпеки та рекомендації з пожежної профілактики.

Завданням даної магістерської роботи було підвищення захисту персональних даних в медичних інформаційних системах, і як результат було досліджено методи, підходи, технології на основі яких розроблено комплекс апаратно-програмних рішень у відповідності до вимог нормативно-правової бази. Так як в процесі проектування виконувалось у побутових умовах, то аналіз потенційно небезпечних і шкідливих виробничих чинників виконується для персонального комп'ютера, на якому розробляється система.

4.1 Загальні питання з охорони праці

Умови праці на робочому місці, безпека технологічних процесів, машин, механізмів, устаткування та інших засобів виробництва, стан засобів колективного та індивідуального захисту, що використовуються працівником, а також санітарно-побутові умови повинні відповідати вимогам нормативних актів про охорону праці. В законі України «Про охорону праці» [24] визначається, що охорона праці – це система правових, соціально-економічних, організаційно-технічних, санітарно-гігієнічних і лікувально-профілактичних заходів та засобів, спрямованих на збереження життя, здоров'я і працездатності людини у процесі трудової діяльності.

4.2 Правові та організаційні основи охорони праці

Основним організаційним напрямом у здійсненні управління в сфері охорони праці є усвідомлення пріоритету безпеки праці і підвищення соціальної відповідальності держави, і особистої відповідальності працівників.

Державна політика в галузі охорони праці визначається відповідно до Конституції України Верховною Радою України і спрямована на створення належних, безпечних і здорових умов праці, запобігання нещасним випадкам та професійним захворюванням. Відповідно до статті 3 Закону України «Про охорону праці» [24] (далі – Закону) законодавство про охорону праці складається з Закону, Кодексу законів про працю

України [25], Закону України «Про загальнообов'язкове державне соціальне страхування від нещасного випадку на виробництві та професійного захворювання, які спричинили втрату працездатності» [26], та прийнятих відповідно до них нормативно-правових актів, норм міжнародного договору (ратифіковані Конвенції і Рекомендації МОТ, директиви Європейської Ради).

Користувачі персональних комп'ютерів, для яких ця робота є головною, підлягають медичним оглядам: попереднім – під час влаштування на роботу і періодичним – протягом професійної діяльності раз на два роки. Жінок з часу встановлення вагітності та в період годування дитини грудьми до роботи з ПК не допускають.

Наявні трудові відносини між працівниками і роботодавцями в Україні за темою дипломного проекту регулюються Кодексом законів про працю України, відповідно до якого права працюючої людини на охорону праці охороняються всебічно та норми охорони праці неухильно інтегровані до правил внутрішнього розпорядку організації/підприємства.

4.3 Аналіз стану умов праці

Робота над проектуванням та розробка навчального додатку проходить в побутовому приміщенні. Для даної роботи достатньо однієї людини, для якої надано робоче місце зі стаціонарним комп'ютером.

4.3.1 Вимоги до приміщення

Геометричні розміри приміщення зазначені у таблиці 4.1

Таблиця 4.1 – Розміри робочого місця

Параметр	Значення
Довжина, м	5
Ширина, м	3
Висота, м	2,5
Площа, $м^2$	15
Об'єм, $м^3$	37,5

Згідно до санітарних норм мікроклімату виробничих приміщень [27] розмір площі для одного робочого місця оператора персонального комп'ютера має бути не менше 6 м^2, а об'єм – не менше 20 м^3. Отже, дане приміщення цілком відповідає зазначеним нормам.

4.3.2 Вимоги до організації робочого місця

При порівнянні відповідності характеристик робочого місця нормативним основні вимоги до організації робочого місця [28] (табл. 4.2) і відповідними фактичними значеннями для робочого місця, констатуємо повну відповідність.

Таблиця 4.2 – Характеристика робочого місця

Найменування параметра	Фактичне значення	Нормативне значення
Висота робочої поверхні, мм	750	680 ÷800
Висота простору для ніг, мм	730	не менше 600
Ширина простору для ніг, мм	660	не менше 500
Глибина простору для ніг, мм	700	не менше 650
Висота поверхні сидіння, мм	470	400 ÷500
Ширина сидіння, мм	400	не менше 400
Глибин сидіння, мм	400	не менше 400
Висота поверхні спинки, мм	600	не менше 300
Ширина опорної поверхні спинки, мм	500	не менше 380
Радіус кривини спинки в горизонтальній площині, мм	400	400
Відстань від очей до екрану дисплея, мм	800	700÷800

Приміщення кабінету знаходиться на другому поверсі чотирьох поверхової будівлі і має об'єм 37,5 м^3, площу – 15 м^2. У цьому кабінеті обладнано одне робоче місце, яке укомплектовано одним персональним комп'ютером.

Температура в приміщенні протягом року коливається у межах 18 –24°С, відносна вологість – близько 50%. Система вентилювання приміщення – природна, а опалення – централізоване.

4.3.3 Навантаження та напруженість процесу праці

За фізичним навантаженням робота відноситься до категорії легкі роботи (Ia), її виконують сидячи з періодичним ходінням. Щодо характеру організування виконання дипломної роботи, то він підпадає під нав'язаний режим, оскільки певні розділи роботи необхідно виконати у встановлені конкретні терміни. За ступенем нервово-психічної напруги виконання роботи можна віднести до II – III ступеня і кваліфікувати як помірно напружений – напружений за умови успішного виконання поставлених завдань.

Найбільшому ризику виникнення різноманітних порушень піддаються: органи зору, м'язово скелетна система, нервово-психічна діяльність, репродуктивна функція у жінок.

Роботу за дипломним проектом визнано, таку, що займає 50% часу робочого дня та за восьмигодинної робочої зміни рекомендовано встановити додаткові регламентовані перерви тривалістю 15 хв через кожну годину роботи [28].

4.4 Виробнича санітарія

На підставі аналізу небезпечних та шкідливих факторів при виробництві (експлуатації), пожежної безпеки можуть бути надалі вирішені питання необхідності забезпечення працюючих достатньою кількістю освітлення, вентиляції повітря, організації заземлення, тощо.

4.4.1 Аналіз небезпечних та шкідливих факторів при розробці виробу

Роботу, пов'язану з ЕОП з ВДТ, у тому числі на тих, які мають робочі місця, обладнані ЕОМ з ВДТ і ПП, виконують із забезпеченням виконання [29], які встановлюють вимоги безпеки до обладнання робочих місць, до роботи із застосуванням ЕОМ з ВДТ і ПП. Переважно роботи за проектами виконують у кабінетах чи інших приміщеннях, де використовують різноманітне електрообладнання, зокрема ПК та периферійні пристрої.

- робоча напруга U = +220В ± 5%;
- робочий струм I = 2А;
- споживана потужність P = 350 Вт.

Робоче місце має відповідати вимогам Державних санітарних правил і норм роботи з візуальними дисплейними терміналами електронно-обчислювальних машин,

затверджених постановою Головного державного санітарного лікаря України від 10.12.98 N 7 [28].

Аналіз небезпечних та шкідливих виробничих факторів виконується у табличній формі (табл. 4.3).

Таблиця 4.3 – Аналіз небезпечних і шкідливих виробничих факторів

Небезпечні і шкідливі виробничі фактори	Джерела факторів (види робіт)	Кількісна оцінка	Нормативні документи
1	2	3	А
Фізичні			
- підвищений рівень напруги електричної мережі, замикання якої може відбутися через тіло людини	-//-	4	ДСТУ Б А.3.2-13:2011 [30]
- недостатність природного світла	порушення умов праці (вимог до приміщень)	2	ДБН В.2.5-28:2015 [31]
- недостатнє освітлення робочої зони	порушення гігієнічних параметрів виробничого середовища	3	ДБН В.2.5-28:2015 [31]
Психофізіологічні:			
- нервово-психічна перевантаження (розумове, перенапруження аналізаторів-зорових)	- пошук інформації для постановки теми; - пошук та аналіз аналогів і літератури; - пошук наявних технологій, моделювання та аналіз алгоритмів; - виконання роботи за темою диплома, тестування; - оформлення роботи	4	НПАОП 0.00-7.15-18 [29] ДСанПіН 3.3.2.007-98 [28]
- фізичні (статичне – сидіння)	порушення умов праці (організації місця праці- сидіння користувача,) та організації робочого часу - безперервна робота)	2	НПАОП 0.00-7.15-18 [29] ДСанПіН 3.3.2.007-98 [28]

4.4.2 Пожежна безпека

Небезпека розвитку пожежі на обчислювальному центрі обумовлюється застосуванням розгалужених систем електроживлення ЕОМ, вентиляції і кондиціювання. Небезпека загоряння пов’язана з особливістю комп’ютерів – із значною кількістю щільно розташованих на монтажній платі і блоках електронних вузлів і схем, електричних і комутаційних кабелів, резисторів, конденсаторів, напівпровідникових діодів і транзисторів. Надійна робота окремих елементів і мікросхем в цілому забезпечується тільки в певних інтервалах температури, вологості і при заданих електричних параметрах. При відхиленні реальних умов експлуатації від розрахункових можуть виникнути пожежонебезпечні ситуації.

Потенційними джерелами запалювання можуть бути:

– іскри і дуги короткого замикання;

– електрична іскра при замиканні і розмиканні ланцюгів;

– перегріви від тривалого перевантаження;

– відкритий вогонь і продукти горіння;

– наявність речовин, нагрітих вище за температуру самозаймання,

– розрядна статична електрика.

Причинами можливого загоряння і пожежі можуть бути:

– несправність електроустановки;

– конструктивні недоліки устаткування;

– коротке замикання в електричних мережах;

– запалювання горючих матеріалів, що знаходяться в безпосередній близькості від електроустановки.

Продуктами згорання, що виділяються на пожежі, є: окис вуглецю; сірчистий газ; окис азоту; синильна кислота; акромін; фосген; хлор та ін. При горінні пластмас, окрім звичних продуктів згорання, виділяються різні продукти термічного розкладання: хлорангідридні кислоти, формальдегіди, хлористий водень, фосген, синильна кислота, аміак, фенол, ацетон, стирол.

4.4.3 Електробезпека

На робочому місці виконуються наступні вимоги електробезпеки: ПК, периферійні пристрої та устаткування для обслуговування, електропроводи і кабелі за виконанням та ступенем захисту відповідають класу зони за правилами улаштування електроустановок, мають апаратуру захисту від струму короткого замикання та інших аварійних режимів. Лінія електромережі для живлення ПК, периферійних пристроїв і устаткування для обслуговування, виконана як окрема групова три- провідна мережа, шляхом прокладання фазового, нульового робочого та нульового захисного провідників. Електромережа штепсельних розеток для живлення персональних ПК, укладено по підлозі поруч зі стінами відповідно до затвердженого плану розміщення обладнання та технічних характеристик обладнання.

4.5 Гігієнічні вимоги до параметрів виробничого середовища

4.5.1 Освітлення

Світло є природною умовою існування людини. Воно впливає на стан вищих психічних функцій і фізіологічні процеси в організмі. Хороше освітлення діє тонізуюче,

створює гарний настрій, покращує протікання основних процесів вищої нервової діяльності.

У проекті, що розробляється, передбачається використовувати суміщене освітлення. У світлий час доби використовуватиметься природне освітлення приміщення через віконні отвори, в решту часу використовуватиметься штучне освітлення. Штучне освітлення створюється газорозрядними лампами.

У приміщенні, де розташовані ЕОМ передбачається природне бічне освітлення, рівень якого відповідає [31]. Джерелом природного освітлення є сонячне світло. Регулярно повинен проводитися контроль освітленості, який підтверджує, що рівень освітленості задовольняє ДБН і для даного приміщення в світлий час доби достатньо природного освітлення.

Розрахунок освітлення.

Для виробничих та адміністративних приміщень світловий коефіцієнт приймається не менше – 1/8, в побутових – 1/10:

$$S_b = \left(\frac{1}{5} \div \frac{1}{10}\right) \times S_n \,, \tag{4.1}$$

де S_b – площа віконних прорізів, м^2;

S_n – площа підлоги, м^2.

S_n = a · b = 5·3 = 15 м^2,

S = 1/10 · 15 = 1,5 м^2.

Приймаємо 1 вікно площею S = 1,5 м^2.

Розрахунок штучного освітлення виробляється по коефіцієнтах використання світлового потоку, яким визначається потік, необхідний для створення заданої освітленості при загальному рівномірному освітленні. Розрахунок кількості світильників n виробляється по формулі (4.2):

$$n = \frac{E \cdot S \cdot Z \cdot K}{F \cdot U \cdot M} \tag{4.2}$$

де E – нормована освітленість робочої поверхні, визначається нормами – 300 лк;

S – освітлювана площа, м^2; S = 15 м^2;

Z – поправочний коефіцієнт світильника (1,1 для люмінесцентних ламп);

K – коефіцієнт запасу, що враховує зниження освітленості в процесі експлуатації – 1,5;

U – коефіцієнт використання, залежний від типу світильника, показника індексу приміщення і т.п. – 0,575

M – число люмінесцентних ламп в світильнику – 3;

F – світловий потік лампи – 5200лм (для ЛБ-80-7).

Підставивши числові значення у формулу (4.2), отримуємо:

$$n = \frac{300 \times 15 \times 1.1 \times 1.5}{5200 \times 0.54 \times 3} = 0{,}8 \approx 1 \qquad (4.2)$$

Приймаємо освітлювальну установку, яка складається з 1-го світильника, які складаються з трьох люмінесцентних ламп загальною потужністю 80 Вт, напругою – 220 В.

4.5.2 Вентилювання

У приміщенні, де знаходяться ЕОМ, повітрообмін реалізується за допомогою природної організованої вентиляції. Цей метод забезпечує приплив потрібної кількості свіжого повітря, що визначається в СНіП.

4.6 Заходи з організації виробничого середовища та попередження виникнення надзвичайних ситуацій

Відповідно до санітарно-гігієнічних нормативів та правил експлуатації обладнання наводимо приклади деяких заходів безпеки.

1) Заходи безпеки під час експлуатації персонального комп'ютера та периферійних пристроїв передбачають:

– правильне організування місця праці та дотримання оптимальних режимів праці та відпочинку під час роботи з ПК;

– експлуатацію сертифікованого обладнання;

– дотримання заходів електробезпеки;

– забезпечення оптимальних параметрів мікроклімату;

– забезпечення раціонального освітлення місця праці (освітленість робочого місця не перевищувала 2/3 нормальної освітленості приміщення);

– облаштовуючи приміщення для роботи з ПК, потрібно передбачити припливно-витяжну вентиляцію або кондиціювання повітря:

а) якщо об’єм приміщення 20 м^3, то потрібно подати не менш як 30 м^3/год повітря;

б) якщо об’єм приміщення у межах від 20 до 40 м^3, то потрібно подати не менш як 20 м^3/рік повітря;

в) якщо об’єм приміщення становить понад 40 м^3, допускається природна вентиляція, у випадку, коли немає виділення шкідливих речовин.

– зниження рівня шуму та вібрації:

а) у джерелі виникнення, шляхом застосування раціональних конструкцій, нових матеріалів і технологічних процесів;

б) звукоізолювання устаткування за допомогою глушників, резонаторів, кожухів, захисних конструкцій, оздоблення стін, стелі, підлоги тощо;

в) використання засобів індивідуального захисту.

2) Заходи безпеки під час експлуатації інших електричних приладів передбачають дотримання таких правил:

– постійно стежити за справним станом електромережі, розподільних щитків, вимикачів, штепсельних розеток, лампових патронів, а також мережевих кабелів живлення, за допомогою яких електроприлади під’єднують до електромережі;

– постійно стежити за справністю ізоляції електромережі та мережевих кабелів, не допускаючи їхньої експлуатації з пошкодженою ізоляцією;

– не тягнути за мережевий кабель, щоб витягти вилку з розетки;

– не закривати меблями, різноманітним інвентарем вимикачі, штепсельні розетки;

– не підключати одночасно декілька потужних електропристроїв до однієї розетки, що може викликати надмірне нагрівання провідників, руйнування їхньої ізоляції, розплавлення і загоряння полімерних матеріалів;

– не залишати включені електроприлади без нагляду;

– не допускати потрапляння всередину електроприладів крізь вентиляційні отвори рідин або металевих предметів, а також не закривати їх та підтримувати в належній чистоті, щоб уникнути перегрівання та займання приладу;

– не ставити на електроприлади матеріали, які можуть під дією теплоти, що виділяється, загорітися (канцелярські товари, сувенірну продукцію тощо).

4.7 Екологія

Діяльність за темою магістерської роботи, а саме: розробка методики удосконалення захисту комп'ютерної мережі в процесі її виконання впливає на навколишнє природнє середовище і регламентується нормами діючого законодавства: Законом України «Про охорону навколишнього природного середовища» [32], Законом України «Про забезпечення санітарного та епідемічного благополуччя населення» [33], Законом України «Про відходи» [34].

В процесі діяльності користувача виникають процеси поводження з відходами ІТ галузі. Нижче надано перелік відходів, що утворюються в процесі роботи:

- відпрацьовані люмінесцентні лампи – I клас небезпеки;
- змінні носії інформації – IV клас небезпеки;
- макулатура – IV клас небезпеки;
- побутові відходи – IV клас небезпеки.

4.8 Висновки до четвертого розділу

В четвертому розділі магістерської роботи виконаний аналіз потенційних небезпек при роботі із засобами обчислювальної техніки, на підставі якого розроблено заходи з техніки безпеки, заходи, що забезпечують виробничу санітарію та гігієну праці, розрахунки природного та штучного освітлень, рекомендації з пожежної профілактики, які підтверджені відповідними розрахунками. Також розглянуто вплив роботи на навколишнє середовище та процеси поводження з відходами ІТ галузі.

ВИСНОВКИ

В атестаційній дипломній роботі було проведено аналіз сучасних методів, засобів, та шляхів підвищення захисту ПДн в МІС, які є обов'язковими в побудові КСЗІ.

Розроблено комплексне апаратно-програмне рішення побудови МІС в ЛПЗ на основі запропонованої технології, яка дозволяє підвищити рівень захисту ПДн в МІС, шляхом збільшення циклів шифрування даних і зменшення вартості обладнання при проектуванні та побудові КСЗІ.

У першому розділі досліджено предметну галузь, описано законодавчу основу інформатизації медичної сфери і впровадження МІС в роботу ЛПЗ. Окремо проаналізовано і детально розглянуто аспекти та практику правового регулювання захисту ПДн та медичних ПДн в МІС. Зроблено ґрунтовний аналіз найбільш популярніших і лідируючих на ринку рішень МІС. Надано концептуальну модель побудови МІС в ЛПЗ.

У другому розділі проведено аналіз програмних, апаратних, та криптографічних підходів до забезпечення безпеки і цілісності конфіденційної інформації, які сертифіковані ДССЗЗІ, і входять до складу КСЗІ, а саме: алгоритм шифрування/дешифрування ДСТУ ГОСТ 28147-2009; алгоритм створення та перевірки ЕЦП ДСТУ 4145-2002; алгоритм розрахунку геш-функцій ГОСТ 34.311-95; протокол Діффі-Гелмана; алгоритм генерації випадкових двійкових послідовностей А ДСТУ 4145-2002. Запропоновано технологію підвищення захисту ПДн в МІС, яка дозволяє збільшити швидкодію функцій шифрування/дешифрування, шляхом подвійного проходу мережевого трафіку через функцію, перерозподілити дану функцію від апаратного шифратора – центральному процесору комп'ютера клієнта в МІС і вилучити апаратний шифратор зі схеми КСЗІ.

В третьому розділі сформовано комплексний підхід до забезпечення захисту ПДн та медичних ПДн з урахуванням виявлених недоліків. Проведено практичне дослідження та відповідні розрахунки ефективності розробленого комплексного рішення з використанням запропонованої технології. Отримані результати наглядно показали, що швидкість функцій шифрування/дешифрування, які виконані на процесорі комп'ютера клієнта системи з накладанням обмеження щодо використання 10% системних ресурсів, в 2,5 рази більша, ніж швидкість виконання тих самих задач на апаратному шифраторі.

В четвертому розділі виконано аналіз потенційних небезпек при роботі з засобами обчислювальної техніки, на підставі якого розроблено заходи з техніки безпеки, заходи, що забезпечують виробничу санітарію та гігієну праці, розрахунки природного та штучного освітлень, рекомендації з пожежної профілактики, які підтверджені відповідними розрахунками. Також розглянуто вплив роботи на навколишнє середовище та процеси поводження з відходами в ІТ галузі.

ПЕРЕЛІК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Указ Президента України «Про Положення про технічний захист інформації в Україні» [Електронний ресурс]. – 1999. – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/term/1229/99.

2. Постанова КМУ № 411 «Деякі питання електронної системи охорони здоров'я» [Електронний ресурс]. – 2018. – Режим доступу до ресурсу: https://www.kmu.gov.ua/ua/npas/deyaki-pitannya-elektronnoyi-sistemi-ohoroni-zdorovya.

3. Закон України «Про захист персональних даних» [Електронний ресурс]. – 2010. – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/2297-17.

4. Закон України «Основи законодавства України про охорону здоров'я» [Електронний ресурс]. – 1993. – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/2801-12.

5. Закон України «Про захист інформації в інформаційно-телекомунікаційних системах» [Електронний ресурс]. – 1994. – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80.

6. Евсеев С. П. Защита персональных данных / С. П. Евсеев, Э. А. Линд, О. Г. Король, О. М. Носик // Системи обробки інформації. – 2012. – №4(1). – С. 108–117. http://nbuv.gov.ua/UJRN/soi_2012_1_4_27.

7. Гольдберг Д. Л. Основные аспекты обеспечения защищенности персональных данных в медицинских информационных системах / Д. Л. Гольдберг, П. Е. Григорьев, А. В. Оленчук // Биотехносфера. – 2016. – № 2 (44) – С. 12–16.

8. Истратова Е. Е. Особенности защиты персональных данных в медицинских информационных системах / Е. Е. Истратова, А. П. Молчанов [Електронний ресурс] – Режим доступу до ресурсу: http://ngmu.ru/cozo/mos/article/abauthors.php?id=1969.

9. Гулиев Я. И. Основные аспекты разработки медицинских информационных систем / Я. И. Гулиев. // нау.-практ. журнал «Врач и информационные технологии» – 2014. – № 5. – С. 10–19.

10. Гулиев Я. И. Обеспечение информационной безопасности в медицинских организациях / Я. И. Гулиев, А. А. Цветков. // нау.-практ. жур. «Врач и информационные технологии». – 2016. – №6. – С. 49–62.

11. Гарифьянов Д. М. Защита персональных данных в медицинских информационных системах / Д. М. Гарифьянов, И. Х. Вахитов. // Молодежный научный форум XI Студенческой международной научно-практической конференции. – 2018. – № 10. – С. 8–17.

12. Гулиев Я. И. Подход к оценке экономической эффективности медицинских информационных систем / Я. И. Гулиев, И. Ф. Гулиева, Е. В. Рюмина, В.Л. Малых, О.А.Фохт, Э.Ф. Тавлыбаева, А. Ю. Вахрина // Врач и информационные технологии. – 2012. – № 6. – С. 15–25.

13. Yao-Chang Yu, To-Yeh Huang, Ting-Wei Hou Forward Secure Digital Signature for Electronic Medical Records / Journal of Medical Systems. – 2012. – № 36 (2), P. 399–406.

14. Lisiak-Felic D. Selected aspects of information security management in entities performing medical activity / D. Lisiak-Felic, P. Nowak, M. Szmit // Economic and Social Development: 34th International Scientific Conference on Economic and Social Development – XVIII International Social Congress. – 2018. – P. 51–60.

15. Офіційний сайт МІС «Доктор ЕЛЕКС» [Електронний ресурс]. – Режим доступу до ресурсу: https://doctor.eleks.com/.

16. Офіційний сайт МІС «EMCiMED» [Електронний ресурс]. – Режим доступу до ресурсу: https://www.mcmed.ua/ua.

17. Офіційний сайт МІС «МедІнфоСервіс» [Електронний ресурс]. – Режим доступу до ресурсу: https://www.infomed.ck.ua/.

18. Офіційний сайт МІС «e-Life» [Електронний ресурс]. – Режим доступу до ресурсу: https://e-life.com.ua/ru/.

19. Закон України Про внесення змін до Закону «Про захист персональних даних» [Електронний ресурс]. – 2012. – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/5491-17.

20. Наказ МОЗ України «Про затвердження Порядку вибору лікаря, який надає первинну медичну допомогу, та форми декларації про вибір лікаря, який надає первинну медичну допомогу» [Електронний ресурс]. – 2018. – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/z0347-18.

21. Перелік засобів технічного захисту інформації, дозволених для забезпечення технічного захисту державних інформаційних ресурсів та інформації, вимога щодо захисту якої встановлена законом [Електронний ресурс].– 2020. – Режим доступу до ресурсу:http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article?showHidden=1&art_id=288071&cat_id=44795.

22. Наказ ДССЗЗІ «Про затвердження Технічних специфікацій форматів криптографічних повідомлень» [Електронний ресурс]. – 2009. – Режим доступу до ресурсу:http://www.dsszzi.gov.ua/dsszzi/control/uk/publish/article;jsessionid=468F492EF9A0CE701DA6D01448AF7F38?art_id=78884&cat_id=38837.

23. Закон України «Про електронний цифровий підпис» [Електронний ресурс]. – 2003. – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/852-15.

24. Закон України «Про охорону праці». Вводиться в дію Постановою ВР № 2695-XII від 14.10.92 р., ВВР, 1992, № 49, ст.669. [Електронний ресурс]. – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/2694-12.

25. Кодекс законів про працю України. Затверджується Законом № 322-VIII від 10.12.71 ВВР, 1971. [Електронний ресурс]. – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/322-08.

26. Закон України «Про загальнообов'язкове державне соціальне страхування від нещасного випадку на виробництві та професійного захворювання, які спричинили втрату працездатності». Наказ від 21 грудня 2000 року № 2180-III. [Електронний ресурс]. – Режим доступу до ресурсу: https://dnaop.com/html/2065/doc-zakon-ukrajini-pro-zagalynoobovjazkove-derzhavnesocialyne-strahuvannya-vid-neshhasnogo-vipadku-na-virobnictvi-ta-profesijnogo-z.

27. ДСН 3.3.6.042-99 «Санітарні норми мікроклімату виробничих приміщень». Постанова N 42 від 01.12.99. [Електронний ресурс]. – Режим доступу до ресурсу: https://zakon.rada.gov.ua/rada/show/va042282-99.

28. ДСанПіН 3.3.2.007-98 «Державні санітарні правила і норми. Гігієнічні вимоги до організації роботи з візуальними дисплейними терміналами електронно-обчислювальних машин». Затверджено Постановою Головного державного санітарного лікаря України від 10 грудня 1998 р. № 7. [Електронний ресурс]. – Режим доступу до ресурсу: https://zakon.rada.gov.ua/rada/show/v0007282-98.

29. НПАОП 0.00-7.15-18 «Вимоги щодо безпеки та захисту здоров'я працівників під час роботи з екранними пристроями». Зареєстровано в Міністерстві юстиції України 25 квітня 2018 р. за № 508/31960. [Електронний ресурс]. – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/z0508-18.

30. ДСТУ Б А.3.2-13:2011 «Система стандартів безпеки праці. Будівництво. Електробезпечність». Наказ Мінрегіону України від 29.12.2011 року № 405. [Електронний ресурс]. – Режим доступу до ресурсу: http://ksv.do.am/GOST/DSTY_ALL/DSTY4/dsty_b_a.3.2-13-2011.pdf.

31. ДБН В.2.5-28:2018 «Природне і штучне освітлення». [Електронний ресурс]. – Режим доступу до ресурсу: http://www.minregion.gov.ua/wp-content/uploads/2018/12/V2528-1.pdf.

32. Закон України «Про охорону навколишнього природного середовища». Вводиться в дію Постановою ВР № 1268-XII від 26.06.91, ВВР, 1991, № 41, ст.547.

[Електронний ресурс]. – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/1264-12.

33. Закон України «Про забезпечення санітарного та епідемічного благополуччя населення». Вводиться в дію Постановою ВР № 4005-XII від 24.02.94, ВВР, 1994, № 27, ст.219. [Електронний ресурс]. – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/4004-12.

34. ДСТУ 3911-99 (ГОСТ 17.9.0.1-99). «Охорона природи. Поводження з відходами. Виявлення відходів та подання інформаційних даних про відходи. Загальні вимоги». Відомості Верховної Ради України (ВВР), 1998, № 36-37, ст.242. [Електронний ресурс]. – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/187/98-вр.

35. Устинов О. В. Персональні дані в системі охорони здоров'я: аналіз законодавства [Електронний ресурс] / О. В. Устинов, С. В. Вахненко // Український медичний журнал.. – 2019. – Режим доступу до ресурсу: https://www.umj.com.ua/article/135215/personalni-dani-v-sistemi-ohoroni-zdorov-ya-analiz-zakonodavstva.

36. Державний стандарт України. ДСТУ ISO/IEC 15946-3:2006 «Інформаційні технології. Методи захисту. Криптографічні методи, що ґрунтуються на еліптичних кривих. Частина 3. Встановлення ключів» (ISO/IEC 15946-3: 2002, IDT). [Електронний ресурс]. – 2006. – Режим доступу до ресурсу: http://online.budstandart.com/ru/catalog/doc-page?id_doc=53520.

37. Наказ № 739 «Про затвердження Вимог до форматів криптографічних повідомлень» [Електронний ресурс]. – 2012. – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/z0108-13.

38. Наказ № 1236/5/453 «Про затвердження вимог до форматів, структури та протоколів, що реалізуються у надійних засобах електронного цифрового підпису» [Електронний ресурс]. – 2012. – Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/z1398-12.

39. Офіційний сайт «eZdorovya» [Електронний ресурс] – Режим доступу до ресурсу: https://ehealth.gov.ua/.

40. Тарнавський Ю. А. Технології захисту інформації / Ю. А. Тарнавський. – Київ: НТУУ «КПІ», 2014. – 162 с. – (електронне мережне навчальне видання).

41. Stefanos Gritzalis Enhancing Privacy and Data Protection in Electronic / Medical Environments. – 2004 – № 28 (6) – pp 535–547.

42. Thomas C. Rindfleisch Confidentiality, Information Technology, and Health Care / Communications of the ACM. – 1997. – №40. – P. 92–100.

43. Столбов А. Б. Об организации обработки персональных данных в медицинских учреждениях / науч.-практ. журнал «Менеджер здравоохранения». – 2008. – №4. – С. 29–32.

44. Ubuntu*Pack 18.04 експертний висновок ДССЗЗІ України. [Електронний ресурс] – Режим доступу до ресурсу: https://linux.org.ua/index.php?topic=11456.0.

45. Черемушкин А.В. Криптографические протоколы. Основные свойства и уязвимости. - М.: Изд. дом «Академия». – 2009. – С. 272.

46. Khovratovich D., Nikolic I. Rotational Cryptanalysis of ARX // Proc. Fast Software Encryption-10. - Lect. Notes in Comp. Sci. – 2010. – Vol. 6147. – P. 333-346.

Додаток А
Електрона презентація

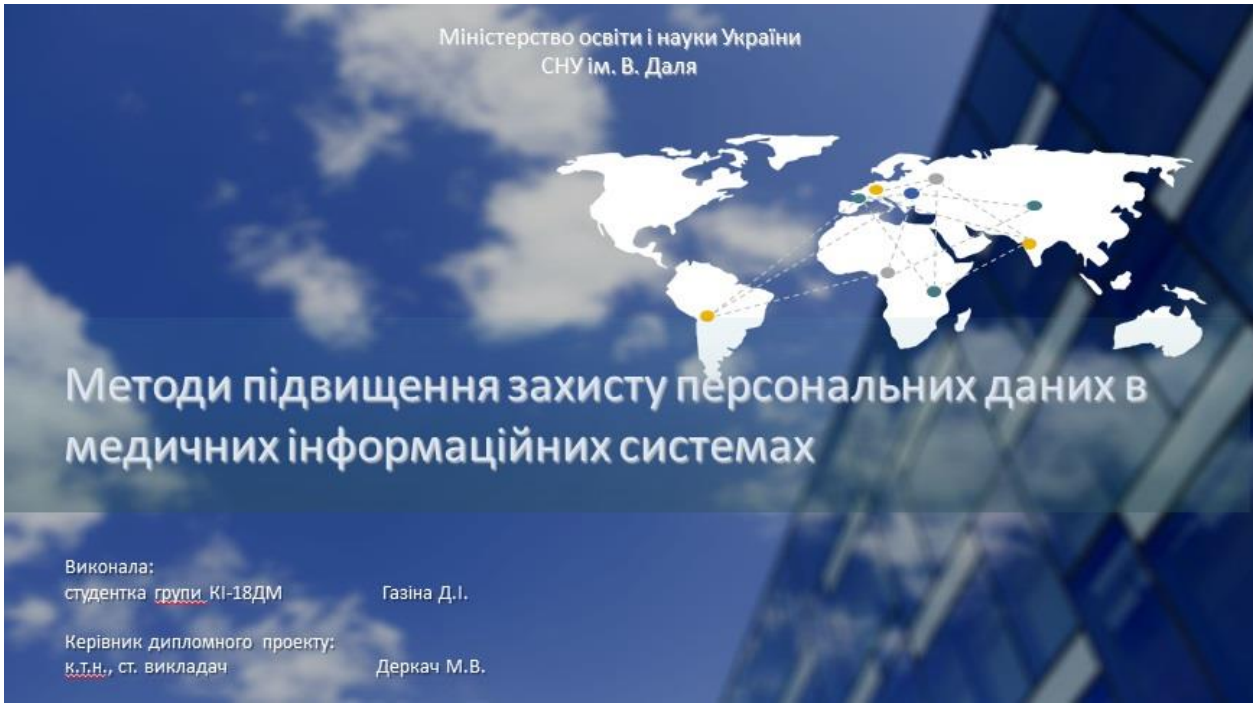

Рисунок А.1 – Слайд №1

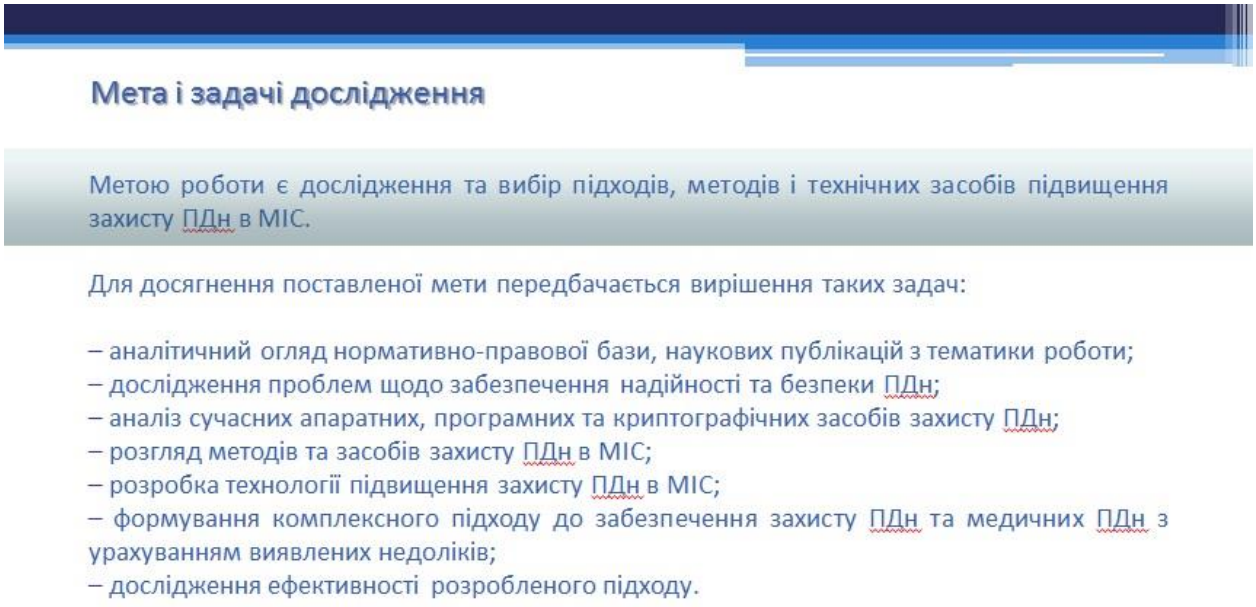

Рисунок А.1 – Слайд №2

Об'єкт дослідження – комплекс апаратно-програмних засобів захисту ПДн в МІС.

Предмет дослідження – медичні ПДн в МІС.

Методи дослідження визначалися специфікою вирішуваних завдань і поставленою метою. В роботі використовувалися методи криптографічного захисту інформації, апаратні і програмні засоби побудови КСЗІ, проектування інформаційної системи.

Рисунок А.1 – Слайд №3

Аналіз предметної області

– впровадження медичної реформи;
– необхідність використання медичних інформаційних систем (МІС);
– МІС повинна мати сертифікацію функціоналу від Міністерства охорони здоров'я (МОЗ).

Рисунок А.1 – Слайд №4

Аналіз предметної області

МІС обробляє персональні дані (ПДн) та медичні ПДн, тому потрібна побудова Комплексної Системи Захисту Інформації (КСЗІ), згідно чинного законодавства, а саме:
– побудова КСЗІ лише згідно концептуальної схеми;
– використання лише тих програмних, апаратних та криптографічних засобів захисту, що є в переліку затвердженому Державною службою Спеціального Зв'язку та Захисту Інформації України (ДССЗЗІ);
– сертифікація системи в цілому на конкретному об'єкті впровадження.

Концептуальна схема побудови КЗСІ, що впроваджується станом на теперішній час

Рисунок А.1 – Слайд №5

Засоби та алгоритми криптографічного захисту, які повинні використовувати КСЗІ

– шифрування/дешифрування даних згідно алгоритму ДСТУ ГОСТ 28147-2009;
– створення та перевірка ЕЦП згідно алгоритму ДСТУ 4145-2002;
– розрахунок геш-функцій здійснюється відповідно алгоритму ГОСТ 34.311-95;
– формування спільного секрету за протоколом Діффі-Гелмана ДСТУ ISO/IEC 15946-3;
– генерація ключової пари: особистого та відкритого ключа для протоколу Діффі-Гелмана ДСТУ ISO/IEC 15946-3;
– генерація випадкових двійкових послідовностей згідно алгоритму А ДСТУ 4145-2002.

Рисунок А.1 – Слайд №6

Технологія підвищення захисту ПДн та медичних в МІС

– подвійний прохід мережевого трафіку через функцію шифрування/дешифрування;
– передача даної функції від апаратного шифратора – центральному процесору комп'ютера на якому встановлено АРМ клієнта в МІС;
– вилучення апаратного шифратора із концептуальної схеми.

Обмеження щодо застосування такої технології:

– подвійний прохід функцій шифрування/дешифрування на процесорі комп'ютера клієнта, повинен реалізовуватися за той же проміжок часу, що і на апаратному шифраторі;
– функція шифрування/дешифрування, яка буде виконуватися на процесорі, повинна використовувати не більше 10% ресурсів даного пристрою, щоб не впливати на його обчислювальні можливості;
– якщо перші дві умови буде підтверджено розрахунками, тоді доцільно вилучити апаратний шифратор/дешифратор концептуальної схеми.

Рисунок А.1 – Слайд №7

Характеристики досліджуваних апаратних засобів

Характеристика шифратора			
Назва			
Шифратор	ІІТ IP-шифратор «Канал-201»	2 x Ethernet 10/100/1000	
		Швидкість шифрування (обробки IP-пакетів)	125 Мбіт/с

Характеристика процесора комп'ютера АРМ клієнта			
Назва			
Процесор	4 ядра / AMD Ryzen 5 2200G	$F_{такт}$	3,5 ГГц
		$T_{такт}$	0,25 ГГц
Оперативна пам'ять	DDR4-2666	$F_{такт}$	1333 МГц
		$F_{дата}$	2666 МГц
		$T_{такт}$	0,94 нс
		$T_{дата}$	0,47 нс
	Таймінг	Латентність CAS	15
		Затримка RAS to CAS	15
		Час зарядки RAS	15

Рисунок А.1 – Слайд №8

Розрахунки

Швидкість обробки даних:

$$\frac{\text{Пікова пропускна здатність}}{\text{кількість ядер}} = \frac{17064\ \text{Мбайт/с}}{4\ \text{ядра}} = 4266\ \text{Мбайт/с} - \text{на ядро в оптимальному випадку;}$$

$$\frac{\text{Пікова пропускна здатність}}{\text{кількість ядер}} = \frac{17064\ \text{Мбайт/с}}{4\ \text{ядра} \times 200\ \text{пропущених операцій}} = 21{,}73\ \text{Мбайт/с} - \text{на ядро для вироджeного випадку.}$$

Максимальна (пікова) швидкість шифрування/дешифрування:

$$4266\ \text{Мбайт/с} \times 10\% = 42{,}66\ \text{Мбайт/с}$$

Швидкість обробки шифрування/дешифрування при половинному навантаженні:

$$4266\ \text{Мбайт/с} \times 5\% = 21{,}33\ \text{Мбайт/с}$$

Рисунок А.1 – Слайд №9

Результати розрахунків

Результати розрахунків швидкості операцій шифрування/дешифрування на процесорі комп'ютера клієнта та на апаратному шифраторі

Характеристика процесора і шифратора			
Назва	**Модель**	**Кількість ресурсів пристрою під операцію**	**Швидкість шифрування**
Процесор	4 ядра/AMD Ryzen 5 2200G	10%	42,66 Мбайт/с
		5%	21,33 Мбайт/с
Апаратний шифратор	ІІТ IP-шифратор «Канал-201»	90%	15,63 Мбайт/с

Рисунок А.1 – Слайд №10

Розроблене комплексне апаратно-програмне рішення побудови МІС

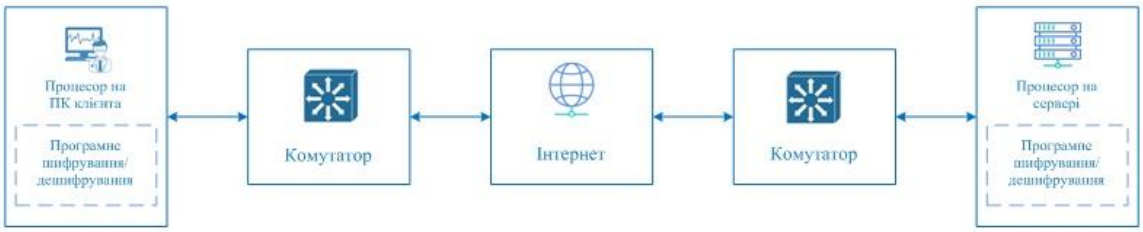

Рисунок А.1 – Слайд №11

Висновки

Отримані результати наглядно демонструють, що:

– швидкість функцій шифрування/дешифрування, які виконані на процесорі комп'ютера клієнта з використанням 10% системних ресурсів, в 2,5 рази більша ніж швидкість виконання тих самих задач на апаратному шифраторі;

– використання в якості шифрування/дешифрування процесора, який рекомендується для застосування на комп'ютері клієнта МІС, дає можливість підвищити швидкодію і зменшити вартість обладнання для КСЗІ. Ринкова ціна апаратного ІІТ IP-шифратора «Канал-201» складає 1000 USD, в той час вартість процесора AMD Ryzen 5 2200G складає 100 USD.

– розрахунки підтверджують, що 5 % ресурсів цілком достатньо для виконання функцій шифрування/дешифрування;

– 5 % ресурсів, які не буде задіяно достатньо для другого проходу функції шифрування/дешифрування.

Рисунок А.1 – Слайд №12