Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ДОПУСТИТИ ДО ЗАХИСТУ:
В.о. завідувача кафедри
кібербезпеки та захисту інформації
_____ Іван ПАРХОМЕНКО
«____» червня 2023 р.

ПОЯСНЮВАЛЬНА ЗАПИСКА

кваліфікаційної роботи

галузь знань 12 Інформаційні технології
(шифр і назва галузі знань)

спеціальність 125 Кібербезпека
(код і назва спеціальності)

освітній ступень бакалавр

освітня програма Кібербезпека
(назва освітньо-професійної програми)

на тему: Засоби та заходи захисту персональних даних у медичних інформаційних системах з використанням міжнародних стандартів

Виконавець: студентка IV курсу, групи КБ-41

_____ **Анна ГОЛУБНИЧА**
(підпис) (Ім'я ПРІЗВИЩЕ)

	Ім'я ПРІЗВИЩЕ	**Підпис**
Керівник	Сергій ДАКОВ	

Нормоконтроль	Олена БОГУСЛАВСЬКА	

Київ 2023

Міністерство освіти і науки України
Київський національний університет імені Тараса Шевченка

Факультет інформаційних технологій
Кафедра кібербезпеки та захисту інформації

ЗАТВЕРДЖЕНО:
В.о. завідувача кафедри кібербезпеки
та захисту інформації
_____ Сергій ТОЛЮПА
«24» жовтня 2022 р.

ЗАВДАННЯ
на виконання кваліфікаційної роботи

спеціальності 125 Кібербезпека
(код і назва спеціальності)

освітньої програми Кібербезпека
(назва освітньої програми)

Студентці **КБ-41** **Анні Русланівні Голубничій**
(група) (Прізвище Ім'я По батькові)

Тема кваліфікаційної роботи Засоби та заходи захисту персональних даних у медичних інформаційних системах з використанням міжнародних стандартів

1. ПІДСТАВИ ДЛЯ ПРОВЕДЕННЯ РОБОТИ

Тема кваліфікаційної роботи затверджена на засіданні кафедри кібербезпеки та захисту інформації протокол №3 від 20.10.2022 р.

2. ВИХІДНІ ДАНІ ДЛЯ ПРОВЕДЕННЯ РОБІТ

Медичні інформаційні системи, захист персональних даних

3. ЗМІСТ РОЗРАХУНКОВО-ПОЯСНЮВАЛЬНОЇ ЗАПИСКИ

Необхідно розглянути поняття персональних даних, зокрема у медичних інформаційних системах, проаналізувати загрози інформаційної безпеки, розглянути основоположні міжнародні стандарти, що стосуються захисту персональних даних в медичних інформаційних системах та розробити рекомендації щодо захисту персональних даних у медичних інформаційних системах з використанням міжнародних стандартів.

4. ВИМОГИ ДО РЕЗУЛЬТАТІВ ВИКОНАННЯ РОБОТИ

Практична цінність Розробка рекомендацій щодо захисту персональних даних у медичних інформаційних системах з використанням міжнародних стандартів.

5. ДАТА ВИДАЧІ ЗАВДАННЯ

Дата видачі завдання: 24 жовтня 2022 року

Завдання видав _____ (підпис) Сергій ДАКОВ (Ім'я, Прізвище)

Завдання прийняла до виконання _____ (підпис) Анна ГОЛУБНИЧА (Ім'я, ПРІЗВИЩЕ)

КАЛЕНДАРНИЙ ПЛАН

№ п/п	Найменування етапів робіт	Строки виконання робіт (початок-кінець)	Відмітка про виконання
1	Уточнення постановки задачі	24.10.2022 – 22.01.2023	*виконано*
2	Аналіз літератури	29.01.2023 – 11.02.2023	*виконано*
3	Обгрунтування вибору рішення	12.02.2023 – 15.02.2023	*виконано*
4	Концепція персональних даних	16.02.2023 – 04.03.2023	*виконано*
5	Аналіз проблем міжнародних стандартів захисту персональних даних у медичних інформаційних системах	05.03.2023 – 21.03.2023	*виконано*
6	Дослідження вразливостей та загроз	22.03.2023 – 08.04.2023	*виконано*
7	Вироблення рекомендацій щодо захисту персональних даних у медичних інформаційних системах	09.04.2023 – 10.05.2023	*виконано*
8	Оформлення пояснювальної записки	11.05.2023 – 27.05.2023	*виконано*
9	Підготовка до захисту кваліфікаційної роботи	28.05.2023 – 12.06.2023	*виконано*

Завдання видав _____ (підпис) Сергій ДАКОВ (Ім'я, ПРІЗВИЩЕ)

Завдання прийняла до виконання _____ (підпис) Анна ГОЛУБНИЧА (Ім'я, ПРІЗВИЩЕ)

Термін подання кваліфікаційної роботи до ЕК 12 червня 2023 року

РЕФЕРАТ

Пояснювальна записка: кваліфікаційна робота складається зі вступу, трьох розділів, загальних висновків, списку використаних джерел та додатків. Основний текст займає 61 сторінка. Список використаних джерел, має обсяг 2 сторінки, і складається з 15 найменувань. Крім того, робота містить 1 додаток, що займає 1 сторінку.

Об'єктом дослідження є процес захисту персональних даних у медичних інформаційних системах.

Метою роботи є розробка рекомендацій щодо захисту персональних даних у медичних інформаційних системах з використанням міжнародних стандартів задля підвищення безпеки та правомірності використання персональних даних в медичному секторі інформаційних систем.

Предметом дослідження є методи захисту персональних даних у медичних інформаційних системах з використанням міжнародних стандартів.

Методи дослідження використанні при підготовці кваліфікаційної роботи:

- аналіз наукової літератури;
- аналіз міжнародних стандартів;
- порівняння та метод теоретичного узагальнення;
- вивчення та узагальнення різних практик захисту.

В роботі розглянуто поняття персональних даних, зокрема персональних даних у медичних інформаційних системах.

Проаналізовано загрози інформаційної безпеки в медичних інформаційних системах.

Розглянуто основоположні міжнародні стандарти, що стосуються захисту персональних даних і медичних інформаційних системах.

Розроблено рекомендації щодо захисту персональних даних у медичних інформаційних системах з використанням міжнародних стандартів.

Практична цінність отриманих результатів полягає в розробці рекомендацій щодо захисту персональних даних у медичних інформаційних системах з використанням міжнародних стандартів.

Напрямки подальших досліджень: дослідження впливу новітніх технологій, таких як штучний інтелект і блокчейн, на захист персональних даних у медичних інформаційних системах, а також вивчення та впровадження більш розширених міжнародних стандартів і політик для покращення безпеки та конфіденційності медичної інформації.

Ключові слова: персональні дані, медичні інформаційні системи, стандартизація, загрози, кібербезпека, інформаційна безпека.

ПЕРЕЛІК УМОВНИХ ПОЗНАЧЕНЬ ТА СКОРОЧЕНЬ

2FA	–	Dual Factor Authentication
AES	–	Advanced Encryption Standard
CNPD	–	Commission Nationale pour la Protection des Données (Національна комісія з питань захисту інформації)
DPO	–	Data protection officer
ePHI	–	Electronic protected health information
GDPR	–	General Data Protection Regulation
HIPAA	–	Health Insurance Portability and Accountability Act
HTTPS	–	HyperText Transfer Protocol Secure
IDS	–	Intrusion Detection System
IPS	–	Intrusion Prevention System
IT	–	Information Technology
NIST	–	National Institute of Standards and Technology
RSA	–	абревіатура від прізвищ Rivest, Shamir та Adleman
VPN	–	Virtual Private Network
MIC	–	Медична інформаційна система

ЗМІСТ

ВСТУП

Актуальність. Сьогодні існує зростаюча потреби у забезпеченні конфіденційності та безпеки особистої медичної інформації. Сучасні медичні інформаційні системи збирають та обробляють великі обсяги персональних даних пацієнтів, включаючи медичну історію, діагнози, лікарські рецепти та іншу чутливу інформацію. Зростають вимоги щодо забезпечення високого рівня захисту цих даних від несанкціонованих осіб та недобросовісних зловмисників.

Медичні організації та провайдери охорони здоров'я знаходяться під постійним тиском забезпечити конфіденційність та цілісність персональних даних своїх пацієнтів. У зв'язку з цим, використання міжнародних стандартів у галузі захисту персональних даних, таких як GDPR в Європейському Союзі, стає необхідним елементом стратегії інформаційної безпеки. Враховуючи глобальну природу обміну медичною інформацією та міжнародні стандарти в цій сфері, дослідження засобів та заходів захисту персональних даних у медичних інформаційних системах з використанням міжнародних стандартів має велику практичну цінність для ефективного впровадження заходів із забезпечення безпеки та відповідності вимогам у цій області.

Тому метою роботи є розробка рекомендацій щодо захисту персональних даних у медичних інформаційних системах з використанням міжнародних стандартів задля підвищення безпеки та правомірності використання персональних даних в медичному секторі інформаційних систем.

Для досягнення визначеної мети необхідно вирішити наступні завдання:

- розглянути поняття персональних даних, зокрема персональних даних у медичних інформаційних системах;
- розглянути основоположні міжнародні стандарти, що стосуються захисту персональних даних і медичних інформаційних системах;
- розробити рекомендації щодо захисту персональних даних у медичних інформаційних системах з використанням міжнародних стандартів.

Об'єктом дослідження в даній роботі є процес захисту персональних даних у медичних інформаційних системах.

Предметом дослідження в даній роботі є методи захисту персональних даних у медичних інформаційних системах з використанням міжнародних стандартів.

Методи дослідження використанні при підготовці кваліфікаційної роботи:

- аналіз наукової літератури;
- аналіз міжнародних стандартів;
- порівняння та метод теоретичного узагальнення;
- вивчення та узагальнення різних практик захисту.

РОЗДІЛ 1
ПОНЯТТЯ ПЕРСОНАЛЬНИХ ДАНИХ ТА ЇХ ЗАХИСТУ В МЕДИЧНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ

Сучасна епоха цифрових технологій і зростаюча кількість електронної інформації ставлять перед нами нові виклики щодо захисту особистих даних. Особливо важливою є проблема захисту персональних даних в медичних інформаційних системах, де ми маємо справу з найбільш конфіденційною та чутливою інформацією про пацієнтів.

В контексті розвитку МІС, де електронні медичні записи та інші електронні дані стають основою для надання якісної медичної допомоги, виникає потреба у забезпеченні конфіденційності, цілісності та доступності цих даних. Особливу увагу слід звернути на те, що медична інформація містить найбільш приватну та особисту інформацію про пацієнтів, що вимагає надзвичайної обережності та захисту від несанкціонованого доступу.

У цьому розділі будуть розглянуті ключові поняття, пов'язані з персональними даними, вимоги законодавства та стандартів, що стосуються захисту даних в МІС, а також найбільш поширені загрози та виклики, які стоять перед організаціями охорони здоров'я в контексті захисту персональних даних. Крім того, будуть розглянуті сучасні методи та технології, які можуть бути використані для забезпечення високого рівня захисту персональних даних в МІС.

Розуміння поняття персональних даних та впровадження ефективних заходів їх захисту в МІС є важливим завданням для забезпечення конфіденційності пацієнтів, довіри громадськості та відповідності вимогам законодавства.

1.1 Визначення поняття персональних даних

У цьому підрозділі буде розглянуто важливе поняття персональних даних, яке є основою для розуміння проблематики захисту і конфіденційності інформації в

медичних інформаційних системах. Розуміння і правильна інтерпретація персональних даних має вирішальне значення для розробки та впровадження ефективних механізмів захисту особистої інформації пацієнтів.

1.1.1 Загальне визначення персональних даних

Згідно із Законом України «Про захист персональних даних» [1], персональні дані – це «відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована». До персональних даних можуть входити:

- ім'я та прізвище особи;
- адреса проживання або роботи;
- електронна адреса;
- номер телефону;
- паспортні дані (серія та номер паспорта);
- інформація про медичний стан та історію хвороб;
- біометричні дані (відбитки пальців, обличчя тощо);
- інші ідентифікаційні дані (номер соціального страхування, номер водійського посвідчення тощо).

У МІС також можуть міститися більш деталізовані дані, такі як історії хвороб, результати тестів, знімки з рентгенівських апаратів та інші медичні дані, які також вважаються персональними даними.

Оскільки персональні дані можуть містити конфіденційну інформацію про людей, їх збір, зберігання, обробка та передача потребує особливого уваги та захисту, що стосується особливо МІС.

Власником персональних даних є особа, на яку вони поширюються. Це може бути будь-яка фізична особа, яка ідентифікується або може бути ідентифікована за допомогою цих даних. Наприклад, пацієнт, який надав медичну інформацію своєму лікарю, є власником цієї інформації.

Однак, іноді можуть бути випадки, коли інша особа, наприклад, опікун або представник, може діяти в якості власника персональних даних від імені іншої особи,

якщо це передбачено законом або даними особами була надана належна згода. Також, власником персональних даних може виступати компанія або організація, якщо ці дані стосуються їх клієнтів, співробітників або інших зацікавлених осіб.

Незалежно від того, хто є власником персональних даних, важливо, щоб вони були захищені від несанкціонованого доступу та використання, що є однією з основних метою захисту персональних даних у МІС.

1.1.2 Персональні дані у медичних інформаційних системах

Також, маємо знати, що, згідно з ст. 32 Конституції України [2] «Ніхто не може зазнавати втручання в його особисте і сімейне життя, крім випадків, передбачених Конституцією України. Не допускається збирання, зберігання, використання та поширення конфіденційної інформації про особу без її згоди, крім випадків, визначених законом, і лише в інтересах національної безпеки, економічного добробуту та прав людини.». З цього випливає, що права людини щодо захисту її персональних даних, які прописані в Конституції, закріплені Законом України «Про захист персональних даних», котрий «регулює правові відносини, пов’язані із захистом і обробкою персональних даних, і спрямований на захист основоположних прав і свобод людини і громадянина, зокрема права на невтручання в особисте життя, у зв’язку з обробкою персональних даних.» [1].

Тобто, персональні дані в медицині - це будь-яка інформація, яка відноситься до конкретної людини і є асоційована з її здоров'ям, медичною історією, діагнозами, лікуванням та іншими медичними даними. Ці дані включають ім'я, адресу, дату народження, стать, контактну інформацію, а також більш конфіденційну інформацію, таку як результати тестів, інформація про ліки, стан здоров'я та інші медичні дані.

До МІС також можуть входити дані про медичні заклади, лікарів та медичний персонал. Наприклад, це можуть бути дані про кваліфікацію лікарів, їхню робочу історію та інші дані, які можуть бути корисними для ведення медичної документації та організації медичної допомоги.

1.1.3 Законодавство щодо захисту персональних даних у медичних інформаційних системах

Важливо зберігати персональні дані в медицині в безпеці та забезпечувати доступ до них тільки медичним фахівцям, які займаються лікуванням пацієнта. Для цього, на рівні законодавства, в багатьох країнах, включаючи Україну, існують спеціальні закони, які регулюють збір, обробку та збереження персональних даних в медицині. Прикладом служить, згаданий раніше, Закон України «Про захист персональних даних» [1], а також Закон України «Про захист інформації в інформаційно-комунікаційних системах» [3] тощо. Закони вимагають, щоб лікарі та медичні установи забезпечували конфіденційність та захист персональних даних своїх пацієнтів.

Законодавство про захист персональних даних в загальному розглядає правила та норми, які встановлені для забезпечення конфіденційності та безпеки персональних даних у будь-якій сфері діяльності. У більшості країн це законодавство базується на загальних принципах, таких як:

- прозорість - особа повинна бути повністю інформована про те, які дані збираються, як вони використовуються та з ким можуть бути поділені;
- призначення - персональні дані повинні збиратися лише для конкретної та чітко визначеної цілі, і не можуть бути використані для іншої мети без попередньої згоди власника даних;
- мінімізація - повинні збиратися лише ті персональні дані, які необхідні для досягнення визначеної мети;
- точність - персональні дані повинні бути точними та актуальними, і, якщо необхідно, повинні бути виправлені або оновлені;
- обмеження збереження - персональні дані повинні зберігатися лише на той час, що необхідний для досягнення визначеної мети;
- безпека - персональні дані повинні бути захищені від несанкціонованого доступу, втрати, знищення чи пошкодження;

– відповідальність - власник даних повинен мати можливість контролювати та змінювати свої персональні дані, а також знати, до кого звертатися в разі порушення їх захисту.

У кожній країні законодавство може мати свої особливості та відрізнятися від інших країн, проте загальні принципи захисту персональних даних залишаються важливим аспектом безпеки інформації в МІС.

1.1.4 Ризики пов'язані з недостатнім захистом персональних даних у медичних інформаційних системах

Недостатній захист персональних даних у медичній галузі може призвести до різних негативних наслідків, серед яких:

1. порушення приватності пацієнта - викрадення або витік інформації, зокрема, можуть бути розкриті дані про стан здоров'я, результати лікування, наслідки тестування тощо;
2. ризик шахрайства та крадіжки особистої інформації - зловмисники можуть скористатися персональними даними для шахрайства або крадіжки ідентифікаційних даних;
3. ризик порушення медичної етики - якщо медичний працівник розголошує конфіденційну інформацію про своїх пацієнтів;
4. втрата довіри пацієнтів до медичної установи - недостатній захист персональних даних може негативно вплинути на ділову репутацію лікарів та/або медичної установи;
5. порушення законодавства - порушення законодавства, що регулює захист персональних даних, включаючи медичну інформацію, може призвести до штрафів або інших правових наслідків для медичної установи або лікаря;
6. ризик фінансових втрат - якщо конфіденційна інформація про пацієнтів потрапляє в руки зловмисників, це може призвести до крадіжки грошей або кредитних карток, особливо якщо ці дані включають інформацію про страхування і фінансовий стан пацієнта;

7. ризик порушення інтелектуальної власності - якщо конкуренти отримують доступ до конфіденційної інформації про методи лікування або розробки нових медичних препаратів, це може призвести до порушення прав на інтелектуальну власність та втрати конкурентної переваги;

8. ризик порушення прав людини - якщо конфіденційна інформація про пацієнтів стає доступною громадськості, це може призвести до стигматизації або дискримінації пацієнтів за їхнім станом здоров'я.

Так як, порушення конфіденційності може мати серйозні наслідки для пацієнтів та медичних закладів, захист персональних даних в медичній галузі є надзвичайно важливим питанням. Нижче розглянуті можливі наслідки для пацієнтів у разі порушення конфіденційності їхніх персональних даних у МІС. До їх переліку входять:

1. ризик ідентифікації - це особливо стосується тих пацієнтів, які, наприклад, мають унікальні характеристики, такі як рідкісні захворювання або стан після трансплантації органів;

2. психологічні наслідки - порушення конфіденційності медичної інформації може викликати стрес та тривогу у пацієнтів, особливо, якщо інформація стосується їхнього стану здоров'я або результатів досліджень;

3. втрата довіри - пацієнти можуть втратити довіру до медичних працівників та медичної системи загалом після порушення конфіденційності їхніх медичних даних, що може призвести до відмови від медичних процедур та послуг, і у наслідку загрожувати їхньому здоров'ю;

4. фінансові наслідки - якщо зловмисники отримають доступ до медичних даних, то це може призвести до фінансових наслідків для пацієнтів.

1.1.5 Важливість захисту персональних даних у медичних інформаційних системах

Належний захист персональних даних у медичній галузі також може допомогти збільшити довіру пацієнтів до медичних працівників і систем охорони здоров'я в

цілому. Якщо люди знають, що їхні дані належним чином захищені, вони можуть бути більш схильні ділитися своєю медичною інформацією і шукати медичну допомогу без страху, що їхні дані будуть використані недоречно. Крім того, належний захист персональних даних може зменшити ризики порушення медичної етики, зменшити витрати на повідомлення про порушення і запобігти законодавчим та репутаційним наслідкам, пов'язаним з порушенням конфіденційності медичних даних. Загалом, належний захист персональних даних може покращити якість медичних послуг і зробити систему охорони здоров'я більш ефективною і надійною.

Належний захист персональних даних у медичній галузі має наступні переваги:

- забезпечення конфіденційності даних пацієнтів;
- покращення якості медичних послуг;
- ефективне управління медичною інформацією;
- підвищення довіри пацієнтів.

Для зберігання та обробки персональних даних в медицині використовуються МІС, які забезпечують високий рівень захисту та конфіденційності цих даних. Крім того, для захисту персональних даних в медицині можуть використовуватися різні методи та технології, такі як шифрування даних, автентифікація та авторизація користувачів, захист від вірусів та інших шкідливих програм, а також збереження даних в безпечному місці.

Медичні установи використовують МІС задля забезпечення максимального рівня захисту персональних даних. Адже будь-який інший вид взаємодії між лікарем та пацієнтом онлайн не може гарантувати безпеку особистої інформації. Як приклад можна навести безкоштовні месенджери або файлообмінники.

1.2 Опис особливостей персональних даних у медичних інформаційних системах

Далі будуть розглянуті особливості персональних даних, які використовуються в МІС. Розуміння цих особливостей є критичним для визначення вимог захисту та конфіденційності медичної інформації.

Буде розглянуто різні типи персональних даних, які входять до складу медичної інформації, включаючи особисті дані пацієнтів, медичні записи, дослідження та інші клінічні дані. Також буде звернута увага на особливості зберігання та обробки цих даних з огляду на їх чутливість та конфіденційність.

1.2.1 Типи персональних даних у медичних інформаційних системах

Для подальшого дослідження медичних інформаційних систем важливо розуміти, які типи персональних даних можуть бути збережені у цих системах. Отже, ось деякі з них:

– ідентифікаційні дані - ім'я, прізвище, адреса, номери телефонів та інша особиста інформація, що дозволяє ідентифікувати конкретну особу;

– дані про стан здоров'я - ці дані можуть включати інформацію про діагноз, лікування, результати лабораторних досліджень, історію хвороби та інші медичні дані;

– інформація про страхування - це можуть бути дані про медичне страхування, інші деталі страхування та оплати медичних послуг;

– дані про здоровий спосіб життя - це можуть бути дані про звички щодо харчування, фізичної активності, вживання алкоголю та інших звичок, які впливають на здоров'я;

– дані про генетичний код - у деяких випадках медичні інформаційні системи можуть містити генетичні дані пацієнта, які дозволяють оцінити ризик розвитку певних захворювань;

– дані про ментальне здоров'я - це можуть бути дані про стан психічного здоров'я, лікування, діагноз та інші медичні дані, що стосуються психічного здоров'я пацієнта;

– інші дані - до цієї категорії можуть входити будь-які інші персональні дані, які не входять до вищезазначених категорій, але все ж є важливими для збереження у медичних інформаційних системах.

1.2.2 Особливості обробки персональних даних у медичних інформаційних системах

Збір та реєстрація персональних даних є ключовим процесом у МІС. Для збору персональних даних у МІС використовуються різні методи, включаючи:

1. Електронний внесок даних. За допомогою електронної реєстрації можна збирати дані про пацієнтів, такі як особисту інформацію, медичну історію, результати тестів, діагнози та інші медичні дані.

2. Автоматична ідентифікація. Іноді у МІС використовуються технології автоматичної ідентифікації для збору даних про пацієнтів. Наприклад, використовуючи браслети з RFID-чипами, що видаються пацієнтам, медичні фахівці можуть відстежувати рух пацієнта в лікарні та отримувати доступ до його медичної інформації.

3. Ручне введення даних. В деяких випадках медичні працівники вводять дані вручну в систему. Це може бути корисним у випадках, коли інші методи недоступні, або коли потрібно внести додаткову інформацію, яка не може бути зібрана автоматично.

Після збору персональних даних, їх реєструють в МІС. У реєстрі зазвичай зберігаються інформація про пацієнтів, їх медичну історію, результати тестів, діагнози та інші медичні дані. Реєстр має бути добре організованим та захищеним, щоб забезпечити безпеку та конфіденційність даних.

Зберігання та забезпечення конфіденційності персональних даних так само є важливим питанням у МІС. Це потрібно для того, щоб уникнути порушення конфіденційності, витоку або втрати цінної медичної інформації.

Для забезпечення конфіденційності персональних даних, МІС повинні мати ефективні механізми контролю доступу до інформації. Це означає, що тільки особи з дозволом можуть отримувати доступ до конфіденційної інформації. Також повинні бути встановлені механізми автентифікації, що дозволяють визначити, хто саме здійснює доступ до інформації.

Крім того, МІС повинні бути обладнані механізмами забезпечення цілісності даних, щоб уникнути їх втрати або пошкодження. Для цього можуть використовуватися різні методи, включаючи резервне копіювання даних на зовнішні носії, архівування даних, використання мережевих засобів безпеки, таких як файєрволи та антивіруси, тощо.

Також, МІС повинні використовувати шифрування даних, щоб уникнути їх незаконного доступу та витоку. Шифрування може бути виконане на різних рівнях, від окремих файлів до всієї системи.

Для забезпечення конфіденційності персональних даних в МІС, також важливо забезпечити надійність фізичного захисту інформаційних ресурсів. Наприклад, серверні бази даних повинні бути захищені від несанкціонованого доступу, втрати даних та вірусних атак. Для цього використовуються різні технології захисту, такі як шифрування даних, резервне копіювання, антивірусне програмне забезпечення та багато іншого.

Необхідно також зазначити, що важливо дотримуватися законодавства та медичної етики щодо зберігання та обробки персональних даних пацієнтів. Законодавство може визначати терміни зберігання даних, вимоги до їх зберігання та використання, а також критерії для знищення даних.

Загалом, належне зберігання та забезпечення конфіденційності персональних даних у медичній галузі є необхідною умовою для забезпечення безпеки та довіри пацієнтів, а також дотримання етичних та законодавчих норм.

Тепер поговоримо про обмін персональними даними між медичними закладами та органами державної влади. Ця частина медичної галузі дозволяє робити більш об'єктивні та точні діагнози, а також планувати та проводити ефективні лікування. Проте, збір та обмін персональними даними можуть стати об'єктом кібератак, які можуть привести до витоку конфіденційної інформації про пацієнтів. Це може викликати серйозні наслідки, такі як порушення приватності пацієнтів, ідентифікаційна крадіжка, шахрайство та інші види кіберзлочинності.

Органи державної влади також можуть мати доступ до персональних даних через різноманітні бази даних та системи, які є у медичній галузі. Це може бути

необхідно для ведення статистики, планування медичної допомоги на рівні країни та інших цілей, які пов'язані зі здоров'ям громадян. Однак, важливо, щоб органи державної влади не мали необмеженого доступу до персональних даних пацієнтів, а лише отримували обмежену інформацію, необхідну для виконання своїх завдань.

Ще хотілося би зачепити тему використання персональних даних у наукових дослідженнях. Це може бути корисним для розвитку нових методів лікування та профілактики різних захворювань. Однак, збір та обробка персональних даних повинні здійснюватись з дотриманням вимог конфіденційності та захисту особистої інформації.

Перед тим, як здійснити дослідження, необхідно отримати згоду пацієнта на використання його персональних даних у наукових цілях. Це повинно бути зроблено на підставі чіткої та доступної інформації про цілі та обсяг використання даних, терміни їх зберігання, можливі наслідки для пацієнта, а також про можливість відмовитись від участі в дослідженні.

Дані повинні бути анонімізовані перед їх використанням в дослідженні. Також слід забезпечити безпеку зберігання даних та захист їх від несанкціонованого доступу.

Важливою умовою використання персональних даних у наукових дослідженнях є дотримання етичних норм та принципів, які гарантують повагу до прав та гідності людини.

1.3 Розгляд сучасних методів захисту персональних даних

Тут будуть розглянуті сучасні методи захисту персональних даних, що застосовуються у МІС. Забезпечення безпеки та конфіденційності цих даних є надзвичайно важливим завданням у контексті зберігання та обробки медичної інформації.

Будуть розглянуті сучасні підходи та технології, що використовуються для захисту персональних даних у МІС, включаючи шифрування, контроль доступу, аудит та моніторинг, а також заходи для захисту від витоку даних та кібератак.

1.3.1 Вступ до технічних аспектів захисту персональних даних в МІС

Вступ до технічних аспектів захисту персональних даних в МІС передбачає розгляд різних аспектів безпеки, включаючи фізичний захист обладнання та мережі. Фізичний захист є одним із важливих елементів загальної стратегії безпеки даних.

Фізичний захист обладнання та мережі передбачає застосування різноманітних заходів для запобігання несанкціонованому фізичному доступу до серверних приміщень та мережевого обладнання. Основна мета полягає в забезпеченні безпеки фізичного середовища, в якому розміщені МІС.

Деякі важливі аспекти фізичного захисту включають:

– контроль доступу - установлення механізмів контролю доступу до серверних приміщень, таких як електронні картки, біометричні системи, PIN-коди та інші методи ідентифікації користувачів; це дозволяє обмежити доступ лише авторизованим особам;

– фізична охорона - забезпечення присутності фізичних охоронців або систем відеоспостереження для контролю та нагляду за серверними приміщеннями;

– захист обладнання - забезпечення фізичної безпеки серверів, маршрутизаторів, комутаторів та іншого мережевого обладнання, наприклад, шляхом розміщення їх у спеціальних місцях або кабінетах з обмеженим доступом;

– запобігання пожежам та стихійним лихам - встановлення систем автоматичного виявлення пожежі, пожежних тривог та систем аварійного відключення, а також резервного живлення для забезпечення безперебійної роботи систем у разі виникнення непередбачених ситуацій;

– резервне копіювання даних - регулярне створення резервних копій даних та їх зберігання у безпечному фізичному місці, що дозволяє відновити дані у разі їх втрати або пошкодження.

Ці заходи фізичного захисту спрямовані на забезпечення безпеки самого обладнання та мережі, а також на запобігання можливості несанкціонованого доступу

до них. Це є важливим кроком у створенні надійної і безпечної інфраструктури для зберігання та обробки персональних даних в МІС.

Логічний захист даних у базах даних та системах відіграє важливу роль у захисті персональних даних у медичній галузі. Цей аспект безпеки включає ряд технологічних та організаційних заходів, спрямованих на забезпечення конфіденційності, цілісності та доступності даних.

Основні підпункти логічного захисту даних у базах даних та системах включають:

1. Автентифікація та авторизація. Реалізація механізмів автентифікації, які перевіряють ідентичність користувачів перед наданням доступу до бази даних або системи. Авторизація встановлює рівні доступу та права користувачів для забезпечення обмеженого доступу до конфіденційної інформації.

2. Шифрування даних. Використання шифрування для захисту конфіденційної інформації у базі даних та під час передачі даних між системами. Шифрування дозволяє перетворити дані у незрозумілу форму, яку можуть прочитати лише авторизовані особи з використанням правильного ключа.

3. Запобігання вразливостям. Використання заходів безпеки, таких як регулярні оновлення програмного забезпечення, патчів та відстежування вразливостей, для запобігання несанкціонованому доступу до баз даних та систем. Це включає такі заходи, як файєрволи, системи виявлення вторгнень (IDS) та системи захисту від вторгнень (IPS).

4. Аудит та моніторинг. Застосування механізмів аудиту та моніторингу для виявлення потенційних загроз та несанкціонованих дій щодо персональних даних у базі даних та системі. Це дозволяє виявляти вторгнення, аномальну активність та ведення слідування за доступом до даних.

5. Резервне копіювання та відновлення даних. Регулярне створення резервних копій баз даних та систем, а також розробка планів відновлення даних у разі втрати або пошкодження. Це гарантує, що в разі непередбачених ситуацій, таких як технічні збої або кібератаки, дані можуть бути відновлені і використовувані з мінімальними затримками.

6. Управління правами доступу. Встановлення контролю над правами доступу до баз даних та систем шляхом призначення різних рівнів доступу для різних користувачів або груп користувачів. Це забезпечує обмеження доступу лише до необхідної інформації для здійснення робочих обов'язків.

Ці підпункти логічного захисту даних спільно створюють надійну систему захисту персональних даних у базах даних та системах. Комбінація технічних та організаційних заходів забезпечує високий рівень безпеки і довіри до обробки та зберігання персональних даних в МІС.

Аудит доступу до персональних даних також є важливою складовою частиною захисту і контролю над використанням цих даних у МІС. Він дозволяє відстежувати, контролювати та аналізувати активності користувачів, які мають доступ до персональних медичних даних. Головна мета аудиту доступу полягає у виявленні потенційних загроз безпеці даних, виявленні вразливостей та недоліків у системі, а також забезпеченні відповідності законодавству і регуляторним вимогам.

Складові аудиту доступу до персональних даних у МІС можуть включати:

1. Ведення журналу подій. Це включає запис і зберігання історії подій, таких як входи, виходи, зміни в базі даних, виконання запитів тощо. Інформація про ці події може бути використана для виявлення потенційних вторгнень або неправомірного використання даних.

2. Моніторинг користувачів. Система може включати механізми, що дозволяють стежити за активністю користувачів, включаючи перегляд, редагування, видалення та інші дії з персональними даними. Це дозволяє виявити незвичайну або підозрілу активність та вжити відповідних заходів безпеки.

3. Аналіз аномалій. Застосування алгоритмів аналізу даних та машинного навчання для виявлення аномальної активності або відхилень від звичайних моделей поведінки користувачів. Це може допомогти виявити недоліки у системі або підозрілу діяльність, яка може вказувати на можливий витік або незаконне використання персональних даних.

4. Контроль доступу. Реалізація механізмів контролю доступу до персональних даних шляхом встановлення правил і обмежень щодо того, які користувачі мають

доступ до яких даних. Це включає надання привілеїв доступу згідно з ролями та обов'язками користувачів, а також використання механізмів автентифікації та авторизації.

5. Перевірка відповідності. Періодична оцінка системи з точки зору відповідності вимогам законодавства, стандартам безпеки та внутрішнім політикам організації. Це забезпечує, що система захисту персональних даних у медичній галузі відповідає вимогам і є ефективною у запобіганні порушень безпеки.

Аудит доступу до персональних даних у МІС допомагає виявляти потенційні загрози та вразливості, запобігаючи неправомірному використанню і витоку даних. Це дозволяє забезпечити високий рівень безпеки та довіри до обробки та зберігання персональних даних у медичній галузі.

Захист даних під час їх транспортування між серверами є ще одним аспектом безпеки персональних даних у МІС. Пункти, які можна розглянути в контексті захисту даних під час їх транспортування, включають:

1. Шифрування даних. Використання шифрування є одним з найефективніших способів захисту даних під час їх транспортування. Дані шифруються перед їх передачею з одного сервера на інший, що забезпечує конфіденційність та недоступність для несанкціонованих осіб. Симетричне та асиметричне шифрування є основними методами шифрування, які можуть бути використані в медичній галузі.

2. Використання захищених каналів зв'язку. Для транспортування даних важливо використовувати захищені канали зв'язку, такі як протокол HTTPS. Цей протокол забезпечує шифрування даних, а також автентифікацію сервера, що дозволяє уникнути проблем зі зловживанням та перехопленням даних під час їх передачі.

3. Використання віртуальних приватних мереж (VPN). VPN забезпечує захищене з'єднання між серверами за допомогою шифрування трафіку. Це дозволяє забезпечити конфіденційність та цілісність даних під час їх транспортування через незахищені мережі, такі як Інтернет.

4. Автентифікація та авторизація. Забезпечення правильної автентифікації та авторизації під час передачі даних між серверами є важливим аспектом захисту.

Застосування механізмів автентифікації, таких як сертифікати, та контроль доступу до даних допомагає переконатися, що тільки авторизовані користувачі мають доступ до персональних даних.

5. Моніторинг та журналювання. Реалізація системи моніторингу та журналювання під час транспортування даних дозволяє виявляти та реагувати на будь-які аномальні або недозволені активності. Це допомагає вчасно виявляти можливі загрози та інциденти безпеки та забезпечувати високий рівень захисту персональних даних.

Застосування цих пунктів дозволяє забезпечити ефективний захист персональних даних під час їх транспортування між серверами в МІС.

1.3.2 Автентифікація користувачів у медичних інформаційних системах

Автентифікація користувачів є важливим етапом захисту персональних даних у медичній галузі. Для цього використовуються паролі та логіни, які є основними методами перевірки ідентифікації користувача.

Пароль є конфіденційним кодом, який використовується для підтвердження ідентичності користувача. Він може бути унікальним для кожного користувача або спільним для групи користувачів зі спеціальним рівнем доступу. Важливо, щоб паролі були достатньо складними, містили комбінацію букв, цифр та спеціальних символів, щоб ускладнити їх перехоплення або вгадування.

Логін, у свою чергу, є ідентифікаційним ім'ям користувача, яке використовується разом з паролем для доступу до системи. Він може бути унікальним для кожного користувача або використовуватися в спільному порядку для групи користувачів.

Для підвищення безпеки автентифікації, рекомендується використовувати додаткові методи, такі як двофакторна автентифікація. Цей підхід вимагає введення додаткового коду або використання фізичного пристрою, наприклад, мобільного телефону або токена, разом з паролем та логіном для підтвердження ідентичності користувача.

Важливо також забезпечити безпечне зберігання паролів та логінів у МІС, використовуючи механізми шифрування та захисту даних. Регулярна зміна паролів і використання сильних автентифікаційних методів сприяють підвищенню безпеки та запобіганню несанкціонованому доступу до медичних даних.

Двофакторна автентифікація (2FA) є одним із сучасних методів підвищення безпеки при доступі до МІС. Вона використовується як додатковий шар захисту, крім пароля та логіна, і забезпечує більш високий рівень ідентифікації користувача.

Принцип роботи 2FA полягає у використанні двох незалежних факторів для підтвердження ідентичності. Зазвичай це комбінація чогось, що користувач знає (наприклад, пароль) і чогось, що він має (наприклад, фізичний пристрій або мобільний телефон). Підтвердження може відбуватись через введення додаткового одноразового коду, використання біометричних даних (відбиток пальця, обличчя) або отримання спеціального підтверджувального повідомлення.

Переваги використання двофакторної автентифікації включають:

– підвищена безпека - 2FA робить процес автентифікації більш надійним, оскільки для доступу потрібно мати не тільки пароль, а й додатковий фактор, що ускладнює несанкціонований доступ;

– захист від крадіжки паролів - навіть якщо пароль втрачено чи скомпрометовано, без додаткового фактора зловмисник не зможе отримати доступ до системи;

– зручність та доступність - багато МІС підтримують 2FA і надають різні методи підтвердження, що робить його доступним для багатьох користувачів;

– сумісність з мобільними пристроями - мобільні телефони часто використовуються в ролі другого фактора, оскільки багато людей мають їх постійно при собі.

Загалом, використання двофакторної автентифікації є ефективним способом забезпечення безпеки при доступі до МІС та захисту персональних даних. Враховуючи ріст кіберзагроз та важливість збереження конфіденційності медичної інформації, 2FA стає необхідною складовою частиною захисних заходів.

Біометрична автентифікація є одним з передових методів захисту та ідентифікації в медичній галузі. Вона базується на унікальних фізичних або поведінкових характеристиках особи для підтвердження її ідентичності. Замість використання паролів або карток доступу, біометрична автентифікація використовує такі фактори, як відбиток пальця, розпізнавання обличчя, структура очного дна, голосовий або письмовий підпис та інші унікальні біометричні ознаки.

Один з основних переваг використання біометричної автентифікації полягає в високому рівні точності та надійності ідентифікації. Унікальність біометричних ознак дозволяє з високою ймовірністю встановити особу та запобігти несанкціонованому доступу до МІС.

Додатковою перевагою є зручність використання біометричних ознак. Користувачам не потрібно запам'ятовувати паролі або носити з собою картки доступу. Вони можуть швидко та зручно автентифікуватись, просто використовуючи свої фізичні характеристики.

В медичній галузі біометрична автентифікація використовується для доступу до МІС, контролю доступу до медичних закладів, автентифікації медичного персоналу та багатьох інших сценаріїв. Вона дозволяє підвищити рівень безпеки та забезпечити точну ідентифікацію пацієнтів та медичного персоналу.

Проте, при використанні біометричних ознак необхідно враховувати певні виклики та обмеження. Наприклад, можлива нестабільність результатів через зміни фізичних характеристик, проблеми зі сумісністю різних систем біометричної автентифікації, а також потенційні проблеми з приватністю та захистом персональних даних.

У всіх випадках використання біометричної автентифікації важливо дотримуватись відповідних стандартів та протоколів безпеки, щоб забезпечити захист персональних даних та запобігти можливим загрозам.

1.3.3 Захист даних у мобільних додатках для медичної сфери

Обробка персональних даних у мобільних додатках має певні ризики, які варто враховувати. Одним з найбільших ризиків є можливість несанкціонованого доступу до цих даних. Мобільні додатки можуть бути більш вразливими до кібератак та зловмисного програмного забезпечення, особливо якщо не виконуються відповідні заходи безпеки.

Інший ризик пов'язаний зі збором та використанням персональних даних у мобільних додатках без належної згоди або з неадекватними цілями. Деякі додатки можуть збирати більше інформації, ніж необхідно для їх функціонування, і використовувати її з комерційною метою або неправомірно передавати третім сторонам.

Крім того, недостатня безпека під час передачі даних між мобільними додатками та серверами може призвести до витоку чутливої інформації. Несанкціоновані особи можуть перехоплювати трафік і отримувати доступ до персональних даних, таких як медична інформація, контактні дані або фінансові дані.

Також, важливим ризиком є неправильне зберігання та обробка персональних даних у мобільних додатках. Якщо не вживаються належні заходи безпеки, такі як шифрування даних або використання безпечних протоколів передачі, існує загроза несанкціонованого доступу до цих даних з боку хакерів або зловмисників.

Захист персональних даних у мобільних додатках можна забезпечити шляхом реалізації різноманітних заходів безпеки. Одним з таких заходів є використання сильних і унікальних паролів для доступу до додатку. Крім того, можна впровадити двофакторну автентифікацію, яка вимагатиме додатковий підтверджуючий елемент, такий як СМС-код або відбиток пальця.

Інші заходи безпеки включають використання шифрування для захисту переданих даних, яке дозволить унеможливити їх прочитання незаконними особами. Рекомендується використовувати безпечні протоколи передачі даних для забезпечення захищеного каналу зв'язку.

Також важливо враховувати апаратні можливості пристрою, які допоможуть забезпечити безпеку. Наприклад, використання датчиків біометричної ідентифікації, таких як сканер відбитків пальців або розпізнавання обличчя, може забезпечити додатковий рівень автентифікації.

Для запобігання несанкціонованому доступу до даних, можна використовувати механізми контролю доступу, які обмежать права користувачів і дозволять доступ до персональних даних тільки необхідним особам. Також варто забезпечити безпечне зберігання даних на пристрої, наприклад, шляхом використання шифрованих сховищ або схем шифрування, що дозволяють зберігати дані в зашифрованому вигляді.

Нарешті, регулярне оновлення мобільного додатку та його компонентів допоможе забезпечити виправлення виявлених безпекових уразливостей і зменшити ризик несанкціонованого доступу до даних.

Ці заходи безпеки сприятимуть забезпеченню високого рівня захисту персональних даних у мобільних додатках та зменшенню ризику їх неправомірного використання.

1.3.4 Огляд сучасних підходів до захисту персональних даних у медичній галузі

Огляд заходів безпеки та методів захисту персональних даних у медичній галузі включає різноманітні підходи та технології. Починаючи з фізичного захисту обладнання та мережі, досягнення безпеки передбачають застосування фізичних обмежень, таких як контроль доступу до серверних приміщень та фізичний моніторинг обладнання.

У логічному захисті даних використовуються різні методи, зокрема шифрування, яке забезпечує конфіденційність даних шляхом перетворення їх у зашифрований формат. Крім того, для забезпечення цілісності та автентичності даних застосовуються механізми контролю цілісності та цифрові підписи.

Одним з найефективніших методів захисту є використання біометричних технологій, таких як сканер відбитків пальців або розпізнавання обличчя. Вони забезпечують унікальну ідентифікацію особи на основі її фізичних характеристик.

Для запобігання несанкціонованому доступу та забезпечення автентифікації користувачів використовуються різні методи, включаючи використання паролів, логінів та двофакторної автентифікації. Це дозволяє переконатися в тому, що тільки уповноважені особи мають доступ до персональних даних.

Захист персональних даних також можна забезпечити за допомогою технологій блокчейн, які забезпечують розподілену та недоступну для змін базу даних. Це дозволяє забезпечити недоступність даних для незаконних змін та зловживань.

Крім того, важливо регулярно оновлювати програмне забезпечення та застосовувати механізми виявлення та запобігання кібератак. Це включає в себе встановлення міцних брандмауерів, систем виявлення вторгнень та антивірусного програмного забезпечення.

Загалом, використання цих заходів безпеки та методів захисту дозволяє забезпечити високий рівень захисту персональних даних у медичній галузі та зменшити ризики їх неправомірного використання.

Огляд сучасних технологій та рішень, що використовуються для захисту персональних даних у медичній галузі, включає широкий спектр інноваційних підходів.

Одним із них є використання алгоритмів шифрування, які забезпечують конфіденційність даних шляхом перетворення їх у зашифрований формат. Симетричне та асиметричне шифрування використовуються для захисту даних під час їх зберігання та передачі.

Також, розповсюджені методи автентифікації, такі як використання паролів, логінів та двофакторної автентифікації. Ці методи дозволяють переконатися в тому, що тільки уповноважені користувачі мають доступ до персональних даних.

Використання біометричних технологій, таких як сканер відбитків пальців або розпізнавання обличчя, стає все більш поширеним в медичній галузі. Ці технології дозволяють ідентифікувати особу на основі її унікальних фізичних характеристик.

Важливим аспектом захисту персональних даних є використання блокчейн технологій. Блокчейн забезпечує розподілену та недоступну для змін базу даних, що дозволяє забезпечити безпеку та недоступність даних для несанкціонованого доступу.

Крім того, використання систем виявлення та запобігання кібератак є необхідним для захисту персональних даних. Ці системи виявляють незвичну активність та атаки на інформаційні системи, що дозволяє своєчасно реагувати та запобігати можливим порушенням безпеки даних.

Усі ці технології та рішення спрямовані на підвищення безпеки та конфіденційності персональних даних у медичній галузі та зменшення ризиків їх неправомірного використання.

Аналіз ефективності заходів безпеки та підходів до захисту персональних даних у медичній галузі виконується з метою оцінки їх ефективності, виявлення потенційних слабких місць та вдосконалення заходів безпеки.

Один з аспектів аналізу полягає у перевірці відповідності застосованих заходів безпеки вимогам нормативно-правових актів, таких як законодавство про захист персональних даних. Це включає перевірку наявності та дотримання політик безпеки, процедур автентифікації, шифрування даних, контролю доступу та інших заходів.

Також проводиться аналіз ефективності застосованих технологій та рішень. Це включає перевірку їх надійності, швидкодії, масштабованості та відповідності специфічним потребам медичної галузі.

Оцінка ризиків пов'язаних з обробкою персональних даних також важлива частина аналізу. Виявлення потенційних загроз та ідентифікація вразливостей дозволяють прийняти необхідні заходи для зменшення ризиків витоку або неправомірного використання даних.

Поряд з технічними аспектами, аналіз включає оцінку організаційних процедур та політик безпеки. Це охоплює перевірку наявності систем управління безпекою, процедур надання доступу до даних, навчання персоналу з питань безпеки та інших важливих аспектів.

Загальний аналіз ефективності заходів безпеки та підходів до захисту персональних даних допомагає виявити слабкі місця та розробити план подальших покращень. Він сприяє підвищенню рівня безпеки даних у медичній галузі та забезпеченню високого рівня конфіденційності та захисту персональних даних пацієнтів.

Висновок до першого розділу

У даному розділі кваліфікаційної роботи було розглянуто поняття персональних даних та їх захисту в медичних інформаційних системах. Було розглянуто важливі аспекти, пов'язані з персональними даними, включаючи їхню визначеність та специфіку в контексті медичної сфери.

Також було висвітлено значення захисту персональних даних у медичних інформаційних системах. Зазначено, що забезпечення конфіденційності, цілісності та доступності персональних даних є критично важливим завданням у медичному секторі. Надійний захист персональних даних не лише забезпечує дотримання законодавства та вимог регуляторних органів, але й сприяє збереженню довіри пацієнтів та забезпеченню ефективної роботи медичних інформаційних систем.

У процесі вивчення теми були проаналізовані ключові проблеми та загрози, пов'язані з безпекою персональних даних у медичних інформаційних системах. Виявлено, що недостатній рівень захисту може призвести до несанкціонованого доступу до медичних даних, порушення конфіденційності та порушення правил обробки персональних даних.

Загалом, розділ "Поняття персональних даних та їх захисту в медичних інформаційних системах" підкреслює необхідність вдосконалення заходів безпеки для забезпечення надійного захисту персональних даних у медичному секторі. Дотримання міжнародних стандартів та рекомендацій, висунутих у даній роботі, сприятиме підвищенню безпеки та правомірності використання персональних даних, забезпечуючи важливу основу для подальшого розвитку медичних інформаційних систем.

РОЗДІЛ 2
МІЖНАРОДНІ СТАНДАРТИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ У МЕДИЧНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ

У цьому розділі будуть розглянуті нам основні орієнтири та регуляторні вимоги, які спрямовані на забезпечення конфіденційності, цілісності та доступності цих даних. Дотримання таких стандартів є критичним для захисту персональних даних в медичній галузі, зменшення ризиків витоку та неправомірного використання цих даних та забезпечення високого рівня довіри до медичних інформаційних систем. Для досягнення цих цілей використовуються різноманітні стандарти, включаючи загальний регламент з захисту даних, HIPAA та інші. У подальшому огляді будуть детальніше розглянуті ці стандарти та їх роль у захисті персональних даних у медичній галузі.

2.1 Огляд міжнародних стандартів та нормативних документів

Міжнародні стандарти захисту персональних даних у медичних інформаційних системах включають:

1. GDPR (General Data Protection Regulation) - цей європейський стандарт встановлює правила та обов'язки щодо збору, обробки та зберігання персональних даних, включаючи медичні дані;
2. HIPAA (Health Insurance Portability and Accountability Act) - цей американський закон встановлює правила та стандарти безпеки для зберігання та передачі медичних інформаційних даних;

Ці стандарти і регуляторні вимоги спрямовані на забезпечення конфіденційності, цілісності та доступності персональних даних в медичних інформаційних системах, а також на зменшення ризиків витоку та неправомірного використання цих даних. Дотримання цих стандартів є важливим кроком для забезпечення високого рівня захисту персональних даних у медичній галузі.

2.1.1 GDPR (General Data Protection Regulation)

Загальний регламент про захист даних (GDPR - General Data Protection Regulation) є важливим міжнародним стандартом, що регулює захист персональних даних в Європейському Союзі. GDPR набув чинності в 2018 році і має на меті забезпечити високий рівень захисту приватності та контролю над персональними даними громадян.

GDPR встановлює ряд принципів та вимог, які стосуються збирання, обробки та зберігання персональних даних. Він надає права особам, чиї дані обробляються, зокрема право на доступ до власних даних, право на виправлення неточностей, право на видалення даних та інші. Також GDPR вимагає, щоб організації, які обробляють персональні дані, приймали відповідні технічні та організаційні заходи для забезпечення безпеки цих даних.

Одним з ключових аспектів GDPR є вимога отримати згоду від особи на обробку її персональних даних. Це означає, що організації повинні ясно пояснити, які дані збираються, з якою метою вони використовуються і кому можуть бути передані. Особа має право відкликати свою згоду в будь-який час.

GDPR також встановлює вимоги щодо повідомлення про порушення безпеки даних. Якщо сталося порушення, яке може призвести до ризику для прав та свобод осіб, організація повинна повідомити компетентний державний орган і осіб, чиї дані були порушені.

Цей регламент має значний вплив на медичну галузь, оскільки медичні організації збирають і обробляють великі обсяги персональних даних пацієнтів. Дотримання вимог GDPR є обов'язковим для медичних установ, які працюють з даними пацієнтів з Європейського Союзу, незалежно від їх місцезнаходження.

В цілому, GDPR встановлює стандарти захисту приватності та персональних даних, які важливі для забезпечення довіри до медичних інформаційних систем та забезпечення прав та свобод осіб, чиї дані обробляються.

Українські медичні підприємства, які надають послуги або товари резидентам ЄС, або здійснюють моніторинг поведінки осіб, що знаходяться в ЄС, автоматично потрапляють під дію Загального регламенту про захист даних (GDPR). Висока якість медичних послуг та привабливі ціни привертають багато іноземних пацієнтів, зокрема в галузі медичного туризму в Україні. Лідерами в цій галузі є стоматологія, офтальмологія, репродукція, неврологія, кардіологія, клітинна терапія та реабілітація.

GDPR надає контролюючим органам країн-членів ЄС можливість накладати санкції на українські медичні установи навіть поза межами ЄС. Це означає, що виконання GDPR стає обов'язковим.

Регламент вносить суттєві зміни у збір, обробку, володіння та передачу даних про здоров'я. Тепер пацієнти повинні надати свою згоду на використання таких даних та можуть її відкликати або навіть вимагати видалення. Це є нововведеннм, оскільки в інших країнах, наприклад, в США, було поширене зберігання медичних даних безстроково. GDPR дає громадянам ЄС право звертатися до медичних закладів з проханням видалити їхні медичні записи у певних обставинах, і таке прохання не можуть відхилити.

Галузь охорони здоров'я стикається з трьома типами особистих даних, які особливо важливі з точки зору GDPR. Це дані про стан здоров'я, генетичні дані та біометричні дані. Дані про стан здоров'я включають будь-яку інформацію про фізичне або психічне здоров'я людини, включаючи інформацію про надану допомогу. Генетичні дані виявляють деталі фізіології або здоров'я пацієнта, включаючи результати лабораторних досліджень. Біометричні дані пов'язані з фізичними або поведінковими характеристиками людини, такими як обличчя, відбитки пальців або риси ходи, які можуть використовуватися для ідентифікації особи. Варто підкреслити, що GDPR встановлює високі стандарти щодо інформованої згоди пацієнта, яка повинна включати типи персональних даних, що збираються, пояснення, як вони будуть використовуватися (інформація про можливі ризики повинна бути надана "зрозумілою та доступною мовою"), а також можливість підтвердження або відмови пацієнта.

GDPR розрізняє дві особи, відповідальні за обробку персональних даних: контролера і процесора. Контролером називається особа або орган, що визначає цілі та способи обробки персональних даних. Процесором є особа або орган, що здійснює обробку персональних даних відповідно до вказівок контролера. Наприклад, лікарня, що збирає інформацію, виступає контролером, а власник програмного продукту, де зберігаються та обробляються дані, а також медичні працівники, що вносять дані в електронну систему, виступають процесорами даних.

Контролер і процесор несуть спільну відповідальність за дотримання GDPR і зобов'язані повідомляти контролюючі органи та суб'єкти даних про будь-які порушення (наприклад, витік, несанкціонований доступ) щодо персональних даних протягом 72 годин з моменту виявлення порушення.

GDPR набув чинності в травні 2018 року, а вже восени того ж року відбувся один з перших прецедентів: португальський наглядовий орган (CNPD) оштрафував місцеву клініку на загальну суму 400 тисяч євро за незаконний доступ працівників клініки до персональних даних пацієнтів за допомогою фальшивих облікових записів.

Таким чином, українським медичним установам неминуче потрібно дотримуватися вимог GDPR у найближчому майбутньому. Вони повинні бути готові до більш жорстких вимог і високих стандартів щодо захисту чутливої категорії персональних даних, зокрема інформації про здоров'я. [4]

2.1.2 HIPAA (Health Insurance Portability and Accountability Act)

Закон про переносимість та відповідальність за страхування здоров'я (HIPAA) є важливим законодавством у Сполучених Штатах, яке регулює захист персональних медичних даних. HIPAA було прийнято у 1996 році з метою забезпечення конфіденційності, цілісності та доступності медичної інформації пацієнтів.

HIPAA вперше встановив всебічний захист конфіденційності інформації про фізичний та психічний стан пацієнтів на федеральному рівні. Ці правила були розроблені з метою забезпечення суворої юридичної захищеності інформації про стан

здоров'я пацієнтів, не втручаючись при цьому у план лікування, роботу медичних установ або якість надання медичних послуг.

HIPAA встановлює стандарти для обробки та зберігання персональних медичних даних в електронному вигляді (ePHI) та встановлює вимоги щодо захисту цих даних. Закон надає пацієнтам право контролювати свої медичні дані, включаючи доступ до них, виправлення неточностей та обмеження доступу до них третіх осіб.

Організації, які працюють з персональними медичними даними, повинні виконувати низку вимог HIPAA, включаючи розробку політик та процедур безпеки, забезпечення обмеженого доступу до даних, шифрування електронної передачі даних, ведення аудиту та ін.

Особлива увага приділяється захисту електронних медичних записів та забезпеченню безпеки електронних комунікацій в медичних установах. HIPAA також встановлює вимоги щодо повідомлення про порушення безпеки даних та покарання за невиконання вимог законодавства.

Закон HIPAA має на меті забезпечити конфіденційність та захист персональних медичних даних пацієнтів, а також сприяти впровадженню електронної обробки медичної інформації з метою покращення якості та ефективності медичних послуг.

Дотримання вимог HIPAA включає набір правил, які постачальники медичних послуг повинні дотримуватися, щоб забезпечити конфіденційність, цілісність та доступність інформації про пацієнтів. Правила HIPAA охоплюють різні аспекти, включаючи конфіденційність, безпеку та повідомлення про порушення. Постачальники медичних послуг повинні впроваджувати відповідні адміністративні, фізичні та технічні заходи для захисту інформації пацієнтів від несанкціонованого доступу, використання та розголошення. Невиконання норм HIPAA може призвести до серйозних наслідків, включаючи штрафи та судові позови. [5]

HIPAA ґрунтується на двох основних принципах:

- принцип приватності, який захищає конфіденційні дані;
- принцип безпеки, який вимагає вжиття посилення заходів безпеки.

Існує список, в який включаються навіть найменші порушення HIPAA, відомий як "стіна сорому". Цей список веде Відділ громадянських справ Міністерства охорони

здоров'я та соціальних служб США. У ньому вказуються імена постачальників медичних послуг, тип порушення та кількість постраждалих пацієнтів.

Проте, це питання стосується не лише сорому, а й наслідків невідповідності HIPAA. За порушення встановлені штрафи, що залежать від рівня порушення і можуть становити від 100 до 50 000 доларів США за кожне випадок порушення. Максимальний річний штраф становить 1,5 мільйона доларів. Крім того, можуть бути порушені кримінальні справи, що можуть призвести до ув'язнення.

2.2 Опис застосування міжнародних стандартів у практиці

Однією з ключових складових ефективної системи захисту є використання міжнародних стандартів, які сприяють створенню єдиного фреймворку та розробці практичних рекомендацій для забезпечення конфіденційності, цілісності та доступності персональних даних.

Далі буде проведений огляд застосування міжнародних стандартів у практиці захисту персональних даних у практиці. Розглянемо основні стандарти, які знаходять широке використання, включаючи GDPR (Загальний регламент з охорони даних), HIPAA (Health Insurance Portability and Accountability Act) та інші. Описані будуть приклади їхнього впровадження в різних сферах, зокрема в медичних інформаційних системах, з метою підвищення рівня захисту особистих даних та забезпечення відповідності національному та міжнародному законодавству.

2.2.1 GDPR (General Data Protection Regulation)

GDPR є одним з найважливіших правових актів в сфері захисту персональних даних. Він застосовується в широкому масштабі до 27 країн Європейського Союзу та 3 країн Європейської Економічної Зони. Проте, його вплив не обмежується лише юрисдикцією ЄС та ЄЕЗ.

Навіть компанії, зареєстровані за межами ЄС або ЄЕЗ, повинні дотримуватись вимог GDPR, якщо вони збирають, обробляють або зберігають персональні дані

громадян ЄС. Це означає, що якщо ваша компанія пропонує товари або послуги людям, що знаходяться в ЄС, або займається моніторингом їх поведінки, вона підпадає під обов'язки та вимоги GDPR, незалежно від юридичної адреси.

GDPR встановлює широкий спектр прав та обов'язків для компаній, що опрацьовують персональні дані. Вони повинні забезпечувати належний рівень захисту даних, включаючи їх конфіденційність, цілісність та доступність. Компанії повинні мати чіткі політики щодо збирання та використання персональних даних, а також забезпечувати згоду осіб, чиї дані обробляються. Вони також повинні інформувати про можливі порушення безпеки даних та приймати заходи для їх запобігання.

Оскільки GDPR має широкий міжнародний вплив, компанії з усього світу повинні бути свідомими своїх зобов'язань та забезпечити відповідність з цим законодавством, якщо вони займаються діяльністю, яка потрапляє під його сферу застосування. [6]

Відповідно до вимог GDPR, українські володільці даних можуть підпадати під його юрисдикцію в різних випадках. Передбачені критерії дозволяють визначити, чи поширюються вимоги GDPR на конкретну організацію чи компанію. Ці критерії включають такі ситуації:

- організація/компанія зареєстрована на території ЄС і здійснює обробку персональних даних в рамках своєї діяльності;
- організація/компанія зареєстрована в Україні, але пропонує товари або послуги громадянам, що проживають у ЄС;
- в організації працюють громадяни ЄС;
- організація проводить маркетингові та інші дослідження, які стосуються громадян з ЄС.

Якщо хоча б один із цих критеріїв відповідає діяльності володільця даних, то за міжнародним правом він зобов'язаний діяти відповідно до вимог Регламенту.

В Україні в даний час активно обговорюється необхідність реформ у сфері захисту персональних даних. Згідно з Угодою про асоціацію з ЄС, наша країна зобов'язана забезпечити високий рівень захисту персональних даних відповідно до

міжнародних стандартів. Покращення законодавства є одним з аспектів цих реформ, але також необхідно будувати систему контролю та підвищувати спроможність всіх суб'єктів, які займаються обробкою даних, забезпечувати належний рівень захисту. Наприклад, країни ЄС перед прийняттям GDPR вклали багато зусиль у те, щоб громадяни, державні органи, муніципалітети та бізнес-спільнота розуміли норми нового законодавства, пов'язані з обробкою даних, кібербезпекою та електронною комунікацією, і були ознайомлені з практичними аспектами впровадження та ризиками, пов'язаними з невиконанням цих положень. [7]

Санкції за порушення або серйозне недотримання цього закону є значними і можуть становити до 4% від обороту компанії або до 20 мільйонів євро, залежно від того, яке значення більше.

Положення GDPR поширюються на всі компанії без жодних винятків, проте особливу увагу потрібно приділити компаніям, які займаються діяльністю в галузі IT-технологій та здійснюють її через глобальну мережу Інтернет. Це пов'язано з тим, що їхній бізнес в більшій мірі використовує персональні дані, ніж у будь-яких інших компаній. [8]

2.2.2 HIPAA (Health Insurance Portability and Accountability Act)

На жаль, в Україні відсутнє законодавче положення, яке б регулювало збір та обробку медичних даних пацієнтів. В даний час медичні заклади та страхові компанії використовують загальні норми Закону України "Про захист персональних даних", а також Закон України "Про захист населення від інфекційних хвороб" та Закон України "Про державні фінансові гарантії медичного обслуговування населення".

Проте ця законодавча база є недостатньою, оскільки вона не враховує специфіку медичних даних. У зв'язку з численними законодавчими прогалинами, захист цієї категорії даних в Україні залишається неефективним. Тому є доцільним розробити окремий нормативно-правовий акт, який б на законодавчому рівні врегулював збір, обробку, розкриття та передачу інформації про стан здоров'я особи, за аналогією з HIPAA в США. [9]

Висновок до другого розділу

У даному розділі кваліфікаційної роботи було детально розглянуто міжнародні стандарти, які регулюють захист персональних даних у медичних інформаційних системах. Зокрема, було проаналізовано HIPAA (Health Insurance Portability and Accountability Act) та GDPR (General Data Protection Regulation) як ключові стандарти, які встановлюють вимоги та принципи захисту персональних даних у медичному секторі.

Зазначено, що обидва стандарти надають важливі вказівки та вимоги щодо безпеки та конфіденційності персональних даних, а також визначають права осіб, чиї дані обробляються в медичних інформаційних системах. HIPAA спрямований на забезпечення безпеки медичних даних в Сполучених Штатах, тоді як GDPR є регуляторним актом Європейського Союзу, що стосується захисту персональних даних у всіх секторах, включаючи медичний.

Виявлено, що обидва стандарти вимагають від організацій, які займаються обробкою персональних даних в медичних інформаційних системах, впроваджувати ряд технічних та організаційних заходів для забезпечення захисту цих даних. Серед таких заходів відзначаються контроль доступу, шифрування, аудит, політики безпеки, навчання персоналу та проведення аудиторських перевірок.

У розділі також було проаналізовано переваги впровадження міжнародних стандартів у медичних інформаційних системах. Зазначено, що дотримання цих стандартів сприяє підвищенню безпеки та конфіденційності персональних даних, забезпечуючи довіру пацієнтів та зменшуючи ризик порушення законодавства щодо захисту даних. Крім того, впровадження міжнародних стандартів сприяє гармонізації підходів до захисту персональних даних у медичних системах на міжнародному рівні.

Отже, впровадження міжнародних стандартів захисту персональних даних у медичних інформаційних системах є критично важливим кроком для забезпечення безпеки, конфіденційності та правомірності обробки цих даних. Рекомендується, щоб медичні організації і компанії, які працюють з медичними даними, дотримувалися встановлених стандартів та впроваджували необхідні технічні та організаційні заходи для ефективного захисту персональних даних та забезпечення довіри пацієнтів і виконання вимог законодавства.

РОЗДІЛ 3
ЗАСОБИ ТА ЗАХОДИ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ У МЕДИЧНИХ ІНФОРМАЦІЙНИХ СИСТЕМАХ

Захист персональних даних у медичних інформаційних системах є надзвичайно важливим аспектом сучасного медичного сектору. З огляду на збільшення обсягів цифрової обробки та зберігання медичної інформації, необхідність забезпечення конфіденційності, цілісності та доступності персональних даних стає надзвичайно актуальною.

Розділ "Засоби та заходи захисту персональних даних у медичних інформаційних системах" присвячений детальному аналізу різноманітних інструментів та заходів, які можуть бути використані для ефективного захисту персональних даних у медичному середовищі. Цей розділ розгляне важливі аспекти безпеки даних, включаючи шифрування, контроль доступу, аудит та моніторинг, фізичну безпеку, освіту персоналу та інші важливі практики.

Метою даного розділу є дослідження сучасних технологій та підходів до захисту персональних даних у медичних інформаційних системах, а також надання рекомендацій та пропозицій для вдосконалення захисту даних у медичному секторі України.

Цей розділ є важливим доповненням до загального розуміння проблематики захисту персональних даних у медичному секторі та сприятиме покращенню безпеки даних, забезпечуючи довіру та конфіденційність медичної інформації.

3.1 Шифрування даних

Шифрування даних є одним з найефективніших та розповсюджених засобів захисту персональних даних у медичних інформаційних системах. Воно дозволяє перетворити медичну інформацію на незрозумілу форму для сторонніх осіб, залишаючи доступ до неї лише авторизованим користувачам.

Вимоги щодо шифрування правил безпеки HIPAA полягають у «впровадженні механізму шифрування та дешифрування ePHI», щоб дозволити доступ лише тим особам або програмним забезпеченням, яким надано права доступу [11], а також «запровадити механізм шифрування ePHI, коли це буде вважатися доцільним», щоб захистити від неавторизованого доступу до ePHI, який передається через мережу електронного зв'язку [11].

Одна з рекомендацій щодо застосування шифрування полягає у використанні сильних алгоритмів шифрування, таких як AES або RSA. Ці алгоритми забезпечують високий рівень безпеки та надійності шифрування.

Стандарти шифрування в рамках HIPAA є мінімальними рекомендаціями NIST для захисту ePHI під час зберігання та передачі. На сьогоднішній день, 128-бітне шифрування AES вважається абсолютним мінімумом. Також організаціям рекомендується впроваджувати більш потужні рішення, що підтримують 192-бітне та 256-бітне шифрування AES, з метою забезпечення вищого рівня безпеки. [10]

Додатковою рекомендацією є шифрування не лише самої медичної інформації, а й всіх засобів зберігання даних, таких як сервери, бази даних, переносні пристрої. Це дозволить запобігти несанкціонованому доступу до даних навіть у випадку фізичного злому або втрати пристроїв.

При реалізації шифрування необхідно також враховувати вимоги до ключів шифрування. Рекомендується використовувати довгі та випадкові ключі, які складаються з комбінації букв, цифр і символів. Регулярна зміна ключів та їх безпечне зберігання є також важливими аспектами шифрування даних.

Застосування шифрування даних у медичних інформаційних системах допоможе забезпечити конфіденційність, цілісність та доступність персональних даних, запобігаючи їх незаконному використанню чи розголошенню. Це є важливою складовою частиною ефективної системи захисту персональних даних у медичній сфері.

3.2 Контроль доступу

Контроль доступу є важливим засобом забезпечення безпеки та конфіденційності персональних даних у медичних інформаційних системах. Він забезпечує, що лише авторизовані користувачі мають доступ до цих даних, утримуючи незаконний доступ поза межами.

Правило безпеки HIPAA визначає доступ у [12] як «здатність або засоби, необхідні для читання, запису, зміни або передачі даних/інформації або іншим чином використовувати будь-який системний ресурс.» Контроль доступу надає користувачам права та/або привілеї для доступу та виконання функцій за допомогою інформаційних систем, програм, програм або файлів. Контроль доступу повинен надавати авторизованим користувачам доступ до мінімально необхідної інформації, необхідної для виконання службових функцій. Права та/або привілеї мають надаватися авторизованим користувачам на основі набору правил доступу, які суб'єкт зобов'язаний запроваджувати відповідно до [13], стандарту керування доступом до інформації відповідно до розділу закону про Адміністративні гарантії.

Отже, рекомендація полягає у встановленні рівнів доступу для різних типів користувачів в системі. Це означає, що кожному користувачеві буде призначено певні привілеї доступу, залежно від його ролі та обов'язків. Наприклад, лікарі можуть мати повний доступ до медичних записів пацієнтів, тоді як адміністративний персонал має обмежений доступ лише до необхідної інформації.

Згідно з [11], наявно чотири специфікації реалізації пов'язані зі стандартом контролю доступу.

1. Унікальна ідентифікація користувача (обов'язково).

У специфікації для впровадження унікальної ідентифікації користувача зазначено, що особа повинна мати унікальне ім'я або номер для ідентифікації. Ідентифікація користувача полягає у способі розпізнавання конкретної особи в системі за допомогою ім'я або номера. Унікальний ідентифікатор користувача дозволяє відстежувати активність користувача при вході в систему і допомагає

встановити відповідальність за виконання функцій, пов'язаних з обробкою захищеної електронної медичної інформації.

Правила не встановлюють однозначного формату ідентифікації користувача. Кожна організація повинна розробити власну стратегію ідентифікації, враховуючи свою робочу силу і операції. Деякі організації можуть використовувати ім'я співробітника або його варіацію (наприклад, jsmith), тоді як інші можуть застосовувати випадкові числа та символи. Важливо забезпечити, щоб випадково призначений ідентифікатор був складним для вгадування неавторизованими користувачами, але при цьому не був важким для запам'ятовування авторизованими користувачами та розпізнавання керівництвом. Незалежно від формату, ідентифікатор користувача не потребує запам'ятовування іншими особами, окрім самого користувача, на відміну від електронної адреси.

Приклади запитань для організацій для розгляду:

- Чи кожен співробітник має унікальний ідентифікатор користувача?
- Який поточний формат використовується для унікальної ідентифікації користувача?
- Чи можна використовувати унікальний ідентифікатор користувача для відстеження активності користувача в інформаційних системах, які містять ePHI?

2. Процедура екстреного доступу (обов’язково).

Організація, що підпадає під цю специфікацію, повинна встановити процедури отримання електронної захищеної інформації про здоров'я під час надзвичайних ситуацій. Ці процедури є задокументованими інструкціями та практиками для отримання доступу до необхідної захищеної електронної медичної інформації (ePHI) під час надзвичайних ситуацій. Засоби контролю доступу можуть значно відрізнятися від звичайних умов експлуатації, і їх типи залежать від ситуацій, що вимагають екстреного доступу до інформаційних систем або програм, що містять EPHI. Процедури повинні бути заздалегідь встановлені, щоб навчати співробітників, як отримати доступ до необхідної ePHI у випадку пошкодження звичайних систем через природні або техногенні катастрофи.

Приклади запитань для організацій для розгляду:

- Кому потрібен доступ до ePHI у разі надзвичайної ситуації?
- Чи існують політики та процедури для забезпечення відповідного доступу до EPHI в надзвичайних ситуаціях?

3. Автоматичний вихід.

Як частина цієї специфікації, організація повинна впровадити електронні процедури для автоматичного виходу з системи після попередньо визначеного періоду бездіяльності. Це застосовується, коли користувачі залишають робочу станцію без нагляду. Автоматичний вихід з системи забезпечує захист від несанкціонованого доступу до ePHI на робочій станції без нагляду. Багато програм мають налаштування, які дозволяють автоматично виходити з системи після періоду бездіяльності, а інші можуть активувати заставку екрана з паролем. Це гарантує, що інформація, що була на екрані, не буде доступна для несанкціонованих користувачів.

Приклади запитань для організацій для розгляду:

- Чи мають поточні інформаційні системи можливість автоматичного виходу з системи?
- Чи активована функція автоматичного виходу з системи на всіх робочих станціях з доступом до ePHI?

4. Шифрування та дешифрування.

Ця специфікація вимагає, щоб організація впровадила механізм шифрування та дешифрування електронної захищеної інформації про стан здоров'я. Шифрування - це перетворення тексту у закодований вигляд, що забезпечує конфіденційність даних. Тільки особа з відповідним ключем або доступом може розшифрувати і прочитати дані. Існує багато методів і технологій шифрування для захисту від несанкціонованого доступу до даних. Про це, також, йдеться в минулій рекомендації.

Приклади запитань для організацій для розгляду:

- Який ePHI слід зашифрувати та розшифрувати, щоб запобігти доступу особам або програмним забезпеченням, яким не надано права доступу?
- Які механізми шифрування та дешифрування доцільно застосувати, щоб запобігти доступу до ePHI особами або програмним забезпеченням, яким не надано права доступу?

Застосування контролю доступу до медичних інформаційних систем є критичним для забезпечення безпеки та конфіденційності персональних даних. Це допомагає зменшити ризик несанкціонованого доступу, витоку даних або зловживання інформацією.

3.3 Аудит та моніторинг

Аудит та моніторинг є важливими компонентами для забезпечення безпеки та захисту персональних даних у медичних інформаційних системах. Вони дозволяють виявляти потенційні загрози, виявляти несанкціоновані дії та вживати відповідних заходів для їх усунення.

У розділі "Технічні заходи безпеки" HIPAA [11] є стандарт "Аудиторський контроль". Цей стандарт вимагає, щоб організація впровадила апаратні, програмні та процедурні механізми, які записують і перевіряють дії в інформаційних системах, що містять або використовують електронну захищену інформацію про здоров'я. Більшість інформаційних систем вже мають певний рівень контролю аудиту, який забезпечує звітність про дії в системі. Це дозволяє записувати та аналізувати активність системи, зокрема виявляти можливі порушення безпеки. Важливо враховувати, що стандарт не встановлює конкретні дані, які мають бути зібрані аудиторськими засобами, або частоту перегляду аудиторських звітів. Підприємство повинно здійснити аналіз ризиків та врахувати організаційні фактори, такі як інфраструктура та можливості безпеки, для визначення належних методів контролю аудиту для інформаційних систем, що містять або використовують ePHI.

Рекомендується проводити регулярний аудит системи, який включає перевірку доступу, контроль прав доступу та виявлення можливих уразливостей. Моніторинг є неперервним процесом спостереження за діяльністю користувачів, системи та мережі. Він дозволяє в реальному часі виявляти підозрілу або нестандартну активність, таку як намагання несанкціонованого доступу або невдалі спроби автентифікації. Моніторинг також включає аналіз журналів подій, що дозволяє виявити потенційні загрози або порушення безпеки.

Аудит та моніторинг є важливими елементами системи захисту персональних даних у медичних інформаційних системах, що дозволяють виявляти, усувати та запобігати потенційним загрозам безпеці. Їх впровадження допомагає забезпечити надійність, конфіденційність та цілісність медичних даних пацієнтів.

3.4 Фізична безпека

Фізична безпека є важливим аспектом захисту персональних даних у медичних інформаційних системах і передбачає заходи для забезпечення безпечного фізичного середовища, де зберігаються та обробляються ці дані.

У розділі "Фізичні гарантії" HIPAA є стандарт "Контроль доступу до об'єктів" [14]. Згідно з цим стандартом, організації повинні впровадити політику та процедури, які обмежують фізичний доступ до своїх електронних інформаційних систем і об'єктів, включаючи будівлі та їхні внутрішні та зовнішні частини. При цьому необхідно забезпечити належний авторизований доступ до цих об'єктів. Термін "об'єкт" визначається в правилах як фізичне приміщення, а також внутрішня та зовнішня частини будівлі.

Стандарт Контроль доступу до об'єктів має чотири специфікації реалізації.

1. Операції в надзвичайних ситуаціях.

Специфікація реалізації операцій на випадок надзвичайних ситуацій включає фізичні заходи безпеки, які суб'єкти встановлюють та застосовують під час активації планів на випадок надзвичайних ситуацій. Організація, яка є об'єктом цих вимог, повинна встановити процедури для доступу до об'єктів, необхідних для відновлення втрачених даних згідно з планами аварійного відновлення та роботи в аварійному режимі.

Операції на випадок надзвичайних ситуацій можуть починатися під час або після стихійного лиха чи іншої надзвичайної ситуації. Під час таких операцій важливо забезпечити фізичну безпеку та належний доступ до ePHI і одночасно відновлювати дані. Контроль доступу до об'єктів під час операцій у надзвичайних ситуаціях може варіюватися залежно від організації.

Приклади запитань для організацій для розгляду:

- Чи розроблено процедури, які дозволять отримати доступ до об’єкта під час відновлення втрачених даних у разі надзвичайної ситуації, наприклад втрата живлення?
- Чи можуть бути належним чином реалізовані процедури тими співробітниками, які відповідають за процес відновлення даних?
- Чи ідентифікують процедури персонал, якому дозволено повторно входити на об’єкт для виконання відновлення даних?
- Чи зміст цієї процедури також розглядається в плані дій організації? Якщо так, то чи варто об’єднувати вміст?

2. План безпеки об'єкта.

План безпеки об'єкта визначає запобіжні заходи для захисту об'єкта та обладнання. Організація, яка підлягає цій специфікації, повинна впроваджувати політику та процедури для обмеження фізичного доступу, втручання та крадіжки. Засоби контролю фізичного доступу повинні гарантувати лише уповноваженим особам доступ до приміщень та обладнання, що містять ePHI, та запобігати несанкціонованому доступу. План безпеки об'єкта повинен включати процедури для запобігання втручанню та крадіжці ePHI та обладнання.

Деякі загальні засоби контролю для запобігання несанкціонованому фізичному доступу, втручанню та крадіжці, які можуть бути розглянуті суб’єктами, включають:

- Замкнені двері, знаки, що попереджають про заборонені зони, камери спостереження, сигналізація
- Засоби контролю власності, такі як теги контролю власності, гравіювання на обладнанні
- Засоби контролю персоналу, такі як ідентифікаційні бейджи, бейджи відвідувачів та/або супровід для великих офісів
- Приватна охоронна служба або патруль на об'єкті

Крім того, персонал повинен знати свою роль у забезпеченні безпеки об'єкта, а підприємства повинні періодично переглядати план з урахуванням змін у середовищі та інформаційних системах.

Приклади запитань для організацій для розгляду:

- Чи розроблено та впроваджено політику та процедури для захисту об’єкта та відповідного обладнання від несанкціонованого фізичного доступу, втручання та крадіжки?
- Чи визначають політика та процедури засоби контролю для запобігання несанкціонованому фізичному доступу, втручанню та крадіжці, як-от ті, що перераховані в загальних засобах керування для розгляду куль вище?

3. Контроль доступу та процедури перевірки.

Стандарт Контроль доступу до об'єктів вимагає впровадження процедур контролю доступу осіб до об'єктів на основі їх ролі або функції. Ці процедури повинні бути узгоджені з планом безпеки об'єкта і дозволяти регулювати доступ осіб до інформації відповідно до їх ролі або функції в організації. Засоби контролю можуть різнитися в залежності від розміру та характеристик організації, наприклад, вимагати підтвердження особи за допомогою посвідчення з фотографією перед наданням доступу до закладу. Практики контролю можуть варіюватися від великих організацій, де це необхідно для кожного відвідувача, до невеликих кабінетів, де перевірка особи може не знадобитися в разі вже відомих осіб.

Приклади запитань для організацій для розгляду:

- Чи розроблено та впроваджено процедури для контролю та підтвердження доступу особи до об’єктів відповідно до її ролі чи функції, включаючи контроль відвідувачів і контроль доступу до програмного забезпечення для тестування та перегляду?
- Чи визначають процедури методи контролю та підтвердження доступу працівника до об’єктів, наприклад, використання охоронців, ідентифікаційних бейджів або пристроїв для входу, таких як ключ-картки?
- Чи процедури також визначають засоби контролю відвідувачів, такі як вимога до них входити в обліковий запис, носити бейджи відвідувача та супроводжуватися уповноваженою особою?

- Чи визначають процедури осіб, посади або посадові функції, які мають право доступу до програмного забезпечення з метою тестування та перегляду з метою зменшення помилок?
- Чи регулярно переглядає керівництво списки осіб, які мають фізичний доступ до чутливих об’єктів?

4. Записи технічного обслуговування.

Організації повинні запровадити політику та процедури для документування ремонту та модифікації фізичних компонентів об'єкта, пов'язаних із безпекою, як обладнання, стіни, двері та замки. У невеликому офісі документація може бути ведена у простому журналі, де фіксуються дата, причина ремонту чи модифікації, а також інформація про те, хто санкціонував ці дії. У великій організації можуть застосовуватись більш детальні процедури та зберігання такої документації у базі даних.

В деяких організаціях найпоширенішими змінами фізичної безпеки можуть бути заміна ключів на дверних замках або зміна кодів на дверях після звільнення працівників. Деякі заклади використовують дверні замки, що працюють зчитувачами карток або бейджів. З метою відповідності даній специфікації також може бути потрібна документація щодо ремонту, додавання або видалення таких пристроїв.

Приклади запитань для організацій для розгляду:

- Чи розроблені та впроваджені політики та процедури, які визначають, як документувати ремонти та модифікації фізичних компонентів об’єкта, пов’язані з безпекою?
- Чи визначають політики та процедури всі компоненти фізичної безпеки, які потребують документації?
- Чи визначають політики та процедури особливі обставини, коли потрібен ремонт або модифікація компонентів фізичної безпеки, наприклад, коли певні співробітники (наприклад, адміністратори додатків), які мають доступ до великої кількості ePHI, перестають його мати?

Також, варто сказати про те, що контроль доступу включає встановлення системи ідентифікації та автентифікації, таких як магнітні картки, біометричні

пристрої або кодові замки, для обмеження фізичного доступу до приміщень з медичними інформаційними системами. Це дозволяє забезпечити, що лише уповноважені працівники мають доступ до цієї інформації.

Використання систем відеоспостереження допомагає відстежувати дії персоналу та виявляти потенційні загрози безпеці. Вони забезпечують запис та збереження відеофайлів, які можуть бути використані для розслідування подій та виявлення несанкціонованих дій.

Додаткові заходи фізичної безпеки можуть включати використання фізичних бар'єрів, які обмежують фізичний доступ до серверів або зберігання медичних даних в безпечних приміщеннях з контрольованими умовами, такими як захищені приміщення з електронним контролем температури і вологості.

Забезпечення фізичної безпеки має на меті запобігти фізичному доступу до медичних інформаційних систем, що може призвести до незаконного використання або втрати персональних даних. Ці заходи варто впроваджувати разом з іншими технічними та організаційними заходами захисту даних для максимальної ефективності та комплексного підходу до безпеки медичних інформаційних систем.

3.5 Освіта та навчання персоналу

Освіта та навчання персоналу є ключовими елементами в забезпеченні безпеки персональних даних у медичних інформаційних системах. Враховуючи постійний розвиток технологій та збільшення кількості кіберзагроз, актуальність організації навчань та підвищення обізнаності персоналу в цій сфері стає все важливішою.

GDPR згадує навчання співробітників лише один раз як завдання для спеціаліста із захисту даних (DPO). Одним із їхніх головних завдань є підвищення обізнаності та навчання персоналу, який бере участь у процесах обробки. Однак це не означає, що лише компанії, які зобов’язані призначати DPO, повинні навчати своїх працівників щодо захисту даних і вимог GDPR. Всі підприємства повинні навчати свій персонал. Можна подумати, що навчання працівників не є обов’язковою умовою, але це помилка. Простіше кажучи, технічні заходи можуть не працювати, якщо ваші

співробітники не знають, як ними користуватися. Тому навчання ваших співробітників захисту персональних даних має важливе значення.

В свою чергу, вимоги HIPAA до навчання найкраще можна описати як «гнучкі», оскільки вони мають враховувати багато різних типів організацій та ділових партнерів. Навчання є обов'язковим, оскільки воно є адміністративною вимогою Правила конфіденційності [15] та адміністративного захисту Правила безпеки [13]. Однак стандарти, пов'язані з навчанням, допускають багато прогалин у знаннях HIPAA, що може призвести до порушень HIPAA, яких можна уникнути.

Персонал, який має доступ до медичних інформаційних систем, повинен бути ознайомлений з основними принципами захисту персональних даних, нормативно-правовими актами, політиками та процедурами, що стосуються безпеки і конфіденційності даних. Це включає усвідомлення загроз, методів автентифікації та авторизації, процедур реагування на інциденти безпеки та відповідальності щодо збереження та захисту інформації.

Організація регулярних навчань та тренінгів з питань кібербезпеки, конфіденційності та захисту персональних даних допомагає персоналу оновлювати свої знання та навички, а також виявляти нові загрози та ризики. Це може включати проведення лекцій, вебінарів, семінарів, практичних занять або використання онлайн-навчання.

Крім навчання персоналу, важливо створити свідому культуру безпеки даних у всій медичній організації. Це може включати оформлення політик та процедур безпеки, підкреслення важливості дотримання правил та забезпечення постійного моніторингу та оцінки безпекових заходів.

Освіта та навчання персоналу щодо захисту персональних даних у медичних інформаційних системах сприяє забезпеченню свідомого та відповідального підходу до безпеки даних. Це дозволяє знизити ризики порушення конфіденційності, збереження та неправомірного використання персональних даних пацієнтів, сприяє покращенню загальної культури безпеки в організації та забезпечує високий рівень захисту даних у медичних інформаційних системах.

3.6 Резервне копіювання та відновлення даних

Резервне копіювання та відновлення даних є важливими елементами стратегії захисту персональних даних у медичних інформаційних системах. Враховуючи ризики втрати даних через технічні несправності, збої у системі, зломи або природні катастрофи, резервне копіювання дозволяє забезпечити збереження та доступність важливої інформації.

Згідно з [14], якщо специфікація реалізації є підходящою організації, то організація повинна створити відновлену точну копію ePHI, якщо це необхідно, перед переміщенням обладнання.

Організація може використовувати різні підходи для виконання цієї специфікації. Наприклад, вона може вирішити створити резервну копію жорсткого диска перед переміщенням обладнання, щоб запобігти втраті ePHI, якщо наявний план резервного копіювання даних не передбачає таку можливість. Іншим варіантом може бути введення обмежень щодо того, де користувачі комп'ютерів можуть зберігати свої файли, наприклад, вимагати зберігати всю інформацію в мережі, щоб уникнути необхідності резервного копіювання жорсткого диска перед переміщенням. Вибір конкретного підходу залежить від середовища та потреб організації, на яку поширюється дія.

Підхід до резервного копіювання та відновлення даних повинен бути систематичним і цілеспрямованим. Рекомендується регулярно робити повні та інкрементальні резервні копії даних медичної інформаційної системи. Повні копії дозволяють відновити систему до повного стану, в той час як інкрементальні копії фіксують лише зміни, що сталися з моменту останньої повної копії. Це забезпечує ефективність процесу відновлення та зменшує обсяг збереженої інформації.

Крім резервного копіювання, важливо також перевіряти і тестувати процедури відновлення даних. Це дозволяє переконатися, що у разі втрати даних можна успішно відновити їх до робочого стану. Такі тестування можуть бути проведені у контрольованому середовищі, де перевіряються резервні копії та процедури відновлення.

Додатковою рекомендацією є збереження резервних копій даних у безпечних зонах або в оффлайн-сховищах, що захищені від несанкціонованого доступу. Це забезпечує фізичну безпеку даних і запобігає їх втраті чи пошкодженню.

Загальна мета резервного копіювання та відновлення даних полягає в тому, щоб забезпечити надійність та доступність персональних даних пацієнтів у випадку непередбачуваних подій або випадків втрати даних. Регулярне резервне копіювання та відновлення даних виступає як важлива складова стратегії захисту персональних даних у медичних інформаційних системах, що сприяє забезпеченню конфіденційності, цілісності та доступності даних.

3.7 Фізична та програмна охорона мережі

Забезпечення безпеки мережі персоналу є одним із ключових аспектів захисту персональних даних у медичних інформаційних системах. Використання відповідних фізичних та програмних заходів може допомогти уникнути несанкціонованого доступу до даних і запобігти потенційним загрозам безпеки.

Згідно з HIPAA, останнім стандартом, перерахованим у розділі «Технічні заходи безпеки» [11], є «Безпека передачі». Цей стандарт вимагає від організації:

«Запровадити технічні заходи безпеки для захисту від несанкціонованого доступу до електронної захищеної інформації про здоров'я, яка передається через мережу електронного зв'язку».

Щоб визначити технічні заходи безпеки, які необхідно застосувати для відповідності цьому стандарту, охоплені організації повинні переглянути поточні методи, що використовуються для передачі ePHI. Наприклад, чи передається ePHI через електронну пошту, через Інтернет або через певну форму приватної мережі або мережі point-to-point? Після перегляду методів передачі суб'єкт, що покривається, повинен визначити доступні та відповідні засоби захисту ePHI під час передачі, вибрати відповідні рішення та задокументувати свої рішення. Правило безпеки дозволяє надсилати ePHI через електронну відкриту мережу, якщо вона належним чином захищена.

Фізична охорона мережі персоналу передбачає застосування фізичних заходів для обмеження доступу до інфраструктури мережі. Це може включати контроль доступу до приміщень, встановлення систем відеоспостереження та використання системи ідентифікації та автентифікації для обмеження доступу до серверів і мережевого обладнання. Такі заходи допомагають убезпечити мережеву інфраструктуру від фізичного вторгнення та несанкціонованого доступу.

Програмна охорона мережі персоналу охоплює використання різноманітних програмних засобів та заходів для забезпечення безпеки даних. Це включає встановлення і налаштування мережевих брандмауерів, систем виявлення і запобігання вторгнень (IDS/IPS), антивірусного програмного забезпечення та інших захисних програм. Крім того, важливо встановити політики доступу та правильно налаштувати права доступу до різних рівнів системи, щоб забезпечити конфіденційність та цілісність даних.

Комбінація фізичної та програмної охорони мережі персоналу створює надійну систему захисту персональних даних у медичних інформаційних системах. Ці заходи допомагають забезпечити конфіденційність, цілісність та доступність даних, а також запобігти несанкціонованому доступу та атакам на мережу. Організації повинні ретельно планувати та реалізовувати ці заходи, враховуючи специфічні потреби та вимоги щодо захисту персональних даних у медичному середовищі.

Висновок до третього розділу

У цьому розділі кваліфікаційної роботи були розглянуті різноманітні засоби та заходи захисту персональних даних у медичних інформаційних системах. Виявлено, що захист персональних даних є надзвичайно важливим аспектом в медичній сфері, оскільки такі дані містять конфіденційну інформацію про пацієнтів.

У розділі були розглянуті технічні засоби захисту даних, такі як шифрування, бекапи, багатофакторна автентифікація та контроль доступу. Зазначено, що використання шифрування є ефективним методом для захисту даних від

несанкціонованого доступу, а бекапи дозволяють забезпечити резервне копіювання даних та відновлення інформації в разі втрати або пошкодження.

Також були розглянуті організаційні заходи, включаючи розробку політик безпеки, проведення навчання та свідомості персоналу щодо захисту даних, контроль доступу до приміщень та інших фізичних об'єктів. Підкреслено, що належна організаційна культура безпеки та свідоме дотримання правил і процедур є важливими чинниками у забезпеченні безпеки персональних даних.

Висновок з цього розділу полягає в тому, що захист персональних даних у медичних інформаційних системах є складним завданням, яке вимагає комплексного підходу. Використання технічних та організаційних засобів захисту, разом з дотриманням міжнародних стандартів та законодавчих вимог, дозволить забезпечити високий рівень безпеки та конфіденційності персональних даних у медичному секторі. Рекомендується медичним організаціям і компаніям, що працюють з медичними даними, ретельно впроваджувати ці засоби та заходи захисту, забезпечуючи захист інформації та довіру пацієнтів.

ВИСНОВКИ

Метою цієї кваліфікаційної роботи було розробити рекомендації щодо захисту персональних даних у медичних інформаційних системах з використанням міжнародних стандартів задля підвищення безпеки та правомірності використання персональних даних в медичному секторі інформаційних систем.

У сучасному цифровому світі, де обмін медичною інформацією стає все більшим, захист персональних даних має вирішальне значення для забезпечення конфіденційності, цілісності та доступності цих даних. Медична інформаційна система, що містить персональні дані, повинна бути добре захищеною від несанкціонованого доступу та потенційних загроз безпеці. Також, вона повинна відповідати вимогам законодавства та міжнародних стандартів з охорони персональних даних, зокрема HIPAA і GDPR.

В рамках роботи було проведено аналіз проблем та загроз безпеці персональних даних у медичному секторі інформаційних систем. Було виявлено такі проблеми, як можливість несанкціонованого доступу до медичних даних, втрата конфіденційності через недостатній рівень захисту, а також ризик порушення правил обробки персональних даних.

На основі аналізу були розроблені рекомендації щодо застосування міжнародних стандартів в області захисту персональних даних у медичних інформаційних системах. Зокрема, використання стандартів HIPAA і GDPR може допомогти підвищити рівень безпеки та правомірності обробки персональних даних. Рекомендації включають впровадження технічних та організаційних заходів, таких як шифрування даних, контроль доступу, проведення регулярних аудитів безпеки, навчання персоналу та усвідомлення їхньої ролі у забезпеченні безпеки даних.

У цій кваліфікаційній роботі було продемонстровано, що захист персональних даних у медичних інформаційних системах є складним завданням, що вимагає комплексного підходу та використання міжнародних стандартів. Реалізація рекомендацій, розроблених у цій роботі, сприятиме підвищенню безпеки та правомірності використання персональних даних в медичному секторі інформаційних систем.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

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

2. Конституція України. [Електронний ресурс] Режим доступу до ресурсу: https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text

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

4. Захищені та здорові: як регламентується захист персональних даних пацієнтів в Україні. [Електронний ресурс] Режим доступу до ресурсу: https://yur-gazeta.com/dumka-eksperta/zahishcheni-ta-zdorovi-yak-reglamentuetsya-zahist-personalnih-danih-pacientiv-v-ukrayini.html

5. Що таке відповідність HIPAA? [Електронний ресурс] Режим доступу до ресурсу: https://www.websiterating.com/uk/cloud-storage/glossary/what-is-hipaa-compliance/

6. GDPR або General Data Protection Regulation. Тренди 2022. [Електронний ресурс] Режим доступу до ресурсу: https://legalitgroup.com/gdpr-novi-eu-tendentsii/

7. Захист персональних даних за правилами GDPR. [Електронний ресурс] Режим доступу до ресурсу: https://ecpl.com.ua/news/zakhyst-personal-nykh-danykh-za-pravylamy-gdpr/

8. Чи потрібно українським компаніям дотримуватись регламенту ЄС із GDPR. [Електронний ресурс] Режим доступу до ресурсу: https://www.uhy-prostor.com/blog/zagalnij-reglament-shhodo-zahistu-danih/

9. HIPAA: як захищають медичні дані пацієнтів в США? [Електронний ресурс] Режим доступу до ресурсу: https://everlegal.ua/hipaa-yak-zakhyschayut-medychni-dani-patsientiv-v-ssha

10. HIPAA Encryption Requirements. [Електронний ресурс] Режим доступу до ресурсу: https://www.hipaajournal.com/hipaa-encryption-requirements/

11. Code of Federal Regulations. 45 CFR §164.312 Technical safeguards. [Електронний ресурс] Режим доступу до ресурсу: https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-C/section-164.312

12. Code of Federal Regulations. 45 CFR §164.304 Definitions. [Електронний ресурс] Режим доступу до ресурсу: https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-C/section-164.304

13. Code of Federal Regulations. 45 CFR § 164.308 Administrative safeguards. [Електронний ресурс] Режим доступу до ресурсу: https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-C/section-164.308

14. Code of Federal Regulations. 45 CFR § 164.310 Physical safeguards. [Електронний ресурс] Режим доступу до ресурсу: https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-C/section-164.310

15. Code of Federal Regulations. 45 CFR §164.530 Administrative requirements. [Електронний ресурс] Режим доступу до ресурсу: https://www.ecfr.gov/current/title-45/subtitle-A/subchapter-C/part-164/subpart-E/section-164.530

ДОДАТОК А
СПИСОК ОПУБЛІКОВАНИХ ПРАЦЬ

Тези наукових доповідей:

1. С. Даков, Л. Дакова, А. Торчило, А.Голубнича. Рекомендації з оцінки відповідності вимогам надавачів хмарних послуг. V Міжнародна науково-практична конференція, Проблеми кібербезпеки інформаційно-телекомунікаційних систем (PCSITS). – Київ, 2022. – с. 108
2. Dakov S., Holubnycha A. Results of the Study of the State of Information Security in the Medical Information System. IX International conference, Information Technology and Implementation (IT&Is-2022). – Kyiv, 2022. – p. 33