МІНІСТЕРСТВО ОСВІТИ І НАУКИ УКРАЇНИ
НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ
ФАКУЛЬТЕТ АЕРОНАВІГАЦІЇ,
ЕЛЕКТРОНІКИ ТА ТЕЛЕКОМУНІКАЦІЙ
КАФЕДРА ТЕЛЕКОМУНІКАЦІЙНИХ ТА РАДІОЕЛЕКТРОННИХ СИСТЕМ

ДОПУСТИТИ ДО ЗАХИСТУ
Завідувач кафедри

_____ Одарченко Р.С.
“_____”_____2021 р.

ДИПЛОМНА РОБОТА
(ПОЯСНЮВАЛЬНА ЗАПИСКА)

ВИПУСКНИКА ОСВІТНЬОГО СТУПЕНЯ БАКАЛАВР

Тема: «Захищена система передавання персональних даних в медичній установі»

Виконавець: _____ Хоменко В. Ю.
(підпис)

Керівник: _____ Пузиренко О. Ю.
(підпис)

Нормоконтролер: _____ Бахтіяров Д. І.
(підпис)

Київ 2021

НАЦІОНАЛЬНИЙ АВІАЦІЙНИЙ УНІВЕРСИТЕТ

Факультет аеронавігації, електроніки та телекомунікацій
Кафедра телекомунікаційних та радіоелектронних систем
Спеціальність 172 «Телекомунікації та радіотехніка»
Освітньо-професійна програма «Телекомунікаційні системи та мережі»

ЗАТВЕРДЖУЮ
Завідувач кафедри

_____ Одарченко Р.С.
“_____”_____2021 р.

ЗАВДАННЯ
на виконання дипломної роботи

Хоменка Владислава Юрійовича
(прізвище, ім'я, по батькові випускника в родовому відмінку)

1. Тема дипломної роботи (проекту): «Захищена система передавання персональних даних в медичній установі»
затверджена наказом ректора від «06» квітня 2021 р. №559 / ст
2. Термін виконання роботи: з 17.05.2021 р. по 20.06.2021 р.
3. Вихідні дані до роботи: захищена система передавання персональних даних в медичній установі
4. Зміст пояснювальної записки: класифікація загроз інформаційній безпеці персональних даних; характеристика загроз безпеки персональних даних, реалізованих з використанням протоколів міжмережевої взаємодії; моделі представлення даних; засоби захисту інформації; організаційні заходи захисту інформації в медичній установі; цикл обробки персональних даних; заходи щодо захисту локально-обчислювальної мережі та баз даних медичної установи; програмні та апаратні засоби захисту ПЕОМ; базова політика безпеки
5. Перелік обов'язкового графічного (ілюстративного) матеріалу: слайди презентації в програмному пакеті Microsoft Power Point

6. Календарний план-графік

№ пор.	Завдання	Термін виконання	Відмітка про виконання
1	Розробити деталізований зміст розділів диплому	17.05.2021-20.05.2021	Виконано
2	Вступ	21.05.2021-22.05.2021	Виконано
3	Аналіз загроз інформаційної безпеки при обробці персональних даних	23.05.2021-27.05.2021	Виконано
4	Аналіз інформаційної системи персональних даних	28.05.2021-03.06.2021	Виконано
5	Розробка заходів захисту персональних даних в медичній установі	04.06.2021-09.06.2021	Виконано
6	Усунення недоліків дипломної роботи	10.06.2021-14.06.2021	Виконано

7. Дата видачі завдання: “26" квітня 2021 р.

Керівник дипломної роботи _____ Пузиренко О. Ю.
(підпис керівника) (П.І.Б.)

Завдання прийняв до виконання _____ Хоменко В. Ю.
(підпис випускника) (П.І.Б.)

РЕФЕРАТ

Дипломна робота «Захищена система передавання персональних даних в медичній установі» містить 60 сторінок, 13 рисунків, 2 таблиці, 15 використаних джерел.

КОНФІДЕНЦІЙНІСТЬ, ЦІЛІСНІСТЬ, ДОСТУПНІСТЬ, МІЖМЕРЕЖЕВИЙ ЕКРАН, СИСТЕМА ОБРОБКИ ПЕРСОНАЛЬНИХ ДАНИХ, IDS.

Об’єкт дослідження –. процес передавання персональних даних пацієнтів та співробітників медичної установи.

Предмет дослідження –. персональні дані пацієнтів та співробітників медичної установи.

Мета дипломної роботи –. розробка захищеної системи передавання персональних даних в мережі медичної установи.

Метод дослідження –. математичного та комп’ютерного моделювання, теорії інформації, моделювання засобів розмежування доступу.

ЗМІСТ

ПЕРЕЛІК СКОРОЧЕНЬ, УМОВНИХ ПОЗНАЧЕНЬ

АРМ - автоматизоване робоче місце.

АС - автоматизована система.

ІСПДн - інформаційна система персональних даних.

НСД - несанкціонований доступ.

ПАК - програмно-апаратний комплекс.

ПАТ - публічне акціонерне товариство.

ПДН - персональні дані.

ПЗ - програмне забезпечення.

СЗІ - система захисту інформації.

СЗІ від НСД - система захисту інформації від несанкціонованого доступу.

ЗМІ - засоби масової інформації.

ЗБПДн - загроза безпеку персональних даних.

ВСТУП

Актуальність теми. Комплексна комп'ютеризація всіх сфер національної економіки, починаючи з 20-го століття, продовжується. Впровадження інформаційної системи (ІР) покращує продуктивність будь-якої організації з будь-яким типом власності. Користувач цієї системи може отримати необхідні дані для задоволення своїх службових обов'язків. Однак є ще одна сторона в процесі комп'ютеризації: зловмисники також загрожують масивам даних і досягають бази даних. З доступом до різних баз даних, зловмисник може використовувати їх, щоб вкрасти гроші, іншу цінну інформацію, фізичні цінності та інші речі.

Тому в нашу "цифрову" епоху вартість захисту інформації більше і більше, ніж будь-коли. Часто зловмисники зацікавлені в інформації, що зберігається в базі даних державних структур, таких як внутрішні справи, міністерств і відомств, а також контрольовані організації, такі як установи охорони здоров'я, освіта. Все більше, на тему популярного SMS-шахрайства з'являються статті в засобах масової інформації. Але, нарешті, після досягнення бази даних деякої медичної організації, зловмисник може шантажувати пацієнта або її родичів, або він може зіпсувати репутацію конфіденційною інформацією.

Захист персональних даних є важливою темою в нашій країні, оскільки законодавча структура повільно оновлюється та не встигає за розвитком сучасних технологій. Завдяки цьому, особа, відповідальна за обробку персональних даних, не знає основних правил безпеки достовірної інформації. Тому експерти з інформаційної безпеки не тільки відповідальність за безпеку інформаційної системи, але й за організацію навчальної системи персоналу [1].

Ця робота присвячена розробці комплексної системи безпеки персональних даних у медичній організації.

Мета і завдання дослідження.

Мета дипломної роботи – розробка захищеної системи передавання персональних даних в мережі медичної установи.

Для досягнення поставленої мети вирішуються такі наукові завдання.

1. Аналіз загроз інформаційної безпеки при передаванні персональних даних.

2. Аналіз існуючої структури мережі медичної установи.

3. Аналіз апаратних, програмних та програмно-апаратних засобів захисту інформації в мережі.

4. Розробка структури захищеної мережі передавання персональних даних в медичній установі.

5. Розробка політики безпеки при обробці персональних даних в мережі медичної установи.

Об'єктом дослідження – процес передавання персональних даних пацієнтів та співробітників медичної установи.

Предметом дослідження – персональні дані пацієнтів та співробітників медичної установи.

Методи досліджень – математичного та комп'ютерного моделювання, теорії інформації, моделювання засобів розмежування доступу.

Апробація отриманих результатів. Основні положення роботи доповідалися та обговорювалися на таких конференціях:

- Науково-практична конференція «Проблеми експлуатації та захисту інформаційно-комунікаційних систем», м. Київ, 2021 р.

РОЗДІЛ 1
АНАЛІЗ ЗАГРОЗ ІНФОРМАЦІЙНОЇ БЕЗПЕКИ ПРИ ОБРОБЦІ ПЕРСОНАЛЬНИХ ДАНИХ

1.1. Класифікація загроз інформаційній безпеці персональних даних

Під загрозою інформаційної безпеки розуміється ризик порушення властивостей інформації – цілісності або конфіденційності.

Перелік небезпек, поряд з оцінкою можливості їх реалізації, працює як основа аналізу ризиків та вимог щодо потоків небезпек для автоматизованої системи. На додаток до виявлення потенційних загроз, необхідно проаналізувати небезпеку, визначену на основі їх класифікаційної основи для багатьох сигналів. Загрози, що відповідають кожному сигналу класифікації, дозволяють розширити необхідність відображати цей об'єкт [1].

Оскільки сучасні тенденції зберігаються і інформація включає велику кількість факторів, стає неможливим сформулювати роботу, щоб описати повний набір небезпек. Тому для захищеної системи, як правило, не існує переліку загроз, але визначається список класів загроз.

Існує три основних інформаційних класи загроз безпеці, що направлені безпосередньо на захищену інформацію [1]:

Порушення конфіденційності - конфіденційна інформація змінюється, але вона доступна для третьої сторони. При застосуванні цієї загрози, інформація про крадіжку є високо ймовірною, що буде розкрита зловмисником, яка може реалізувати фінансову або престижну шкоду [1].

Порушення цілісності захищеної інформації є руйнування спотворення, зміни інформації. Інформаційна цілісність може бути порушена внаслідок некомпетентно-

сті або недбалості працівника підприємства. Крім того, цілісність може бути порушена зловмисником для досягнення власних цілей. Наприклад, щоб отримати інформацію про співробітництво клієнта з організацією для заміни або заміни окремих даних [1].

Порушення доступності інформації - уповноважений користувач не може досягти захищеної інформації внаслідок таких причин: відмова обладнання, програмного забезпечення, локальної комп'ютерної мережі.

Після розгляду небезпек автоматизованої системи можна проаналізувати небезпеку інформаційної системи персональних даних [1].

Інформаційна система персональних даних - це сукупність персональних даних, що містяться в базі даних, що забезпечує їх обробку за рахунок інформаційних технологій та технічних засобів.

Інформаційна система персональних даних - це поєднання інформаційно-програмних та апаратних елементів, а також інформаційні технології, що використовуються при обробці персональних даних.

Основними елементами є ПДН:

• особисті дані, що містяться в базі даних;

• інформаційні технології, що використовуються в процесі обробки ПДН;

• Технічний інструмент (обчислювальне обладнання, інформаційні та обчислювальні комплекси та мережі);

• програмне забезпечення (операційна система, СУБД тощо);

• Пристрій інформаційної безпеки ПДН;

• Помічник технічних засобів та систем - технічні інструменти та системи які не задіяні для обробки персональних даних.

Захист особистих даних - це безліч умов та факторів, які забезпечують уникнення таких дій, що призводить до руйнування, зміни, перехоплення, копіювання, передачу персональних даних, а також іншу несанкціоновану діяльність з інформацією [2].

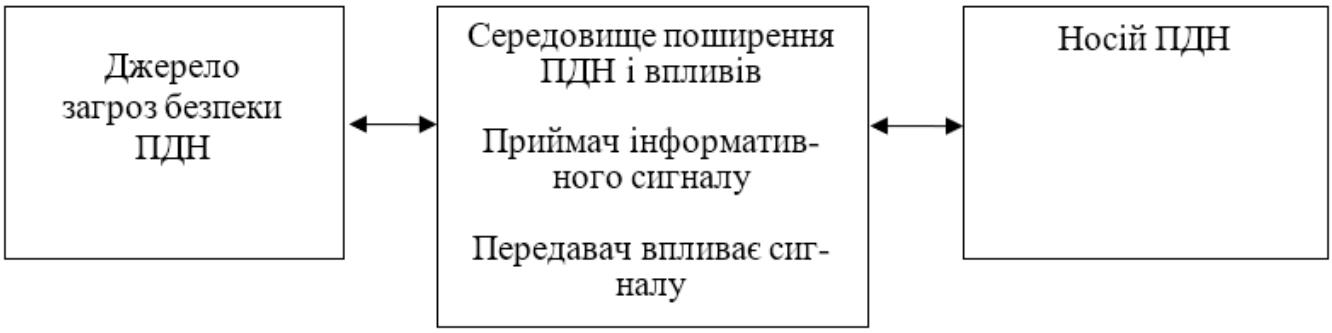

Рис. 1.1. Узагальнена схема каналу реалізації загроз безпеки персональних даних

Носій ПДН може мати інформацію, представлену в наступних типах:

- • Акустична (мовна) інформація.
- Видова (зображення / відео) інформація.
- Інформація оброблювана у ІСПДН, що представлена в таких видах як електричний, електромагнітний, оптичний сигнал.
- Розміщення інформації представленої у вигляді бітів, байтів, файлів та інших логічних структур.

1.2. Загальна характеристика загроз безпеки персональних даних, реалізованих з використанням протоколів міжмережевої взаємодії

Якщо база даних була реалізована на основі локальної або розподіленої інформаційної системи, вона може бути вразливою до загроз безпеки використання протоколу взаємозв'язку. Це може бути НСД (несанкціонований доступ), щоб зруйнувати ПДН або перехопити їх. Схема класифікації загроз, що застосовується до мережі, показана на рис. 1.1. Ця класифікація заснована на семи наступних первинних чинниках.

Основні типи атак на ІСПДН:

1. Аналіз мережевого трафіку.
2. Сканування мережі.
3. Загроза для виявлення пароля.

4. Компрометація надійного суб'єкта мережі використання його облікового запису та паролю.

5. Застосовуйте хибного маршруту в мережі.

6. Впровадження помилкового об'єкта мережі.

7. Відмова в обслуговування.

8. Запуск віддаленого додатку [2].

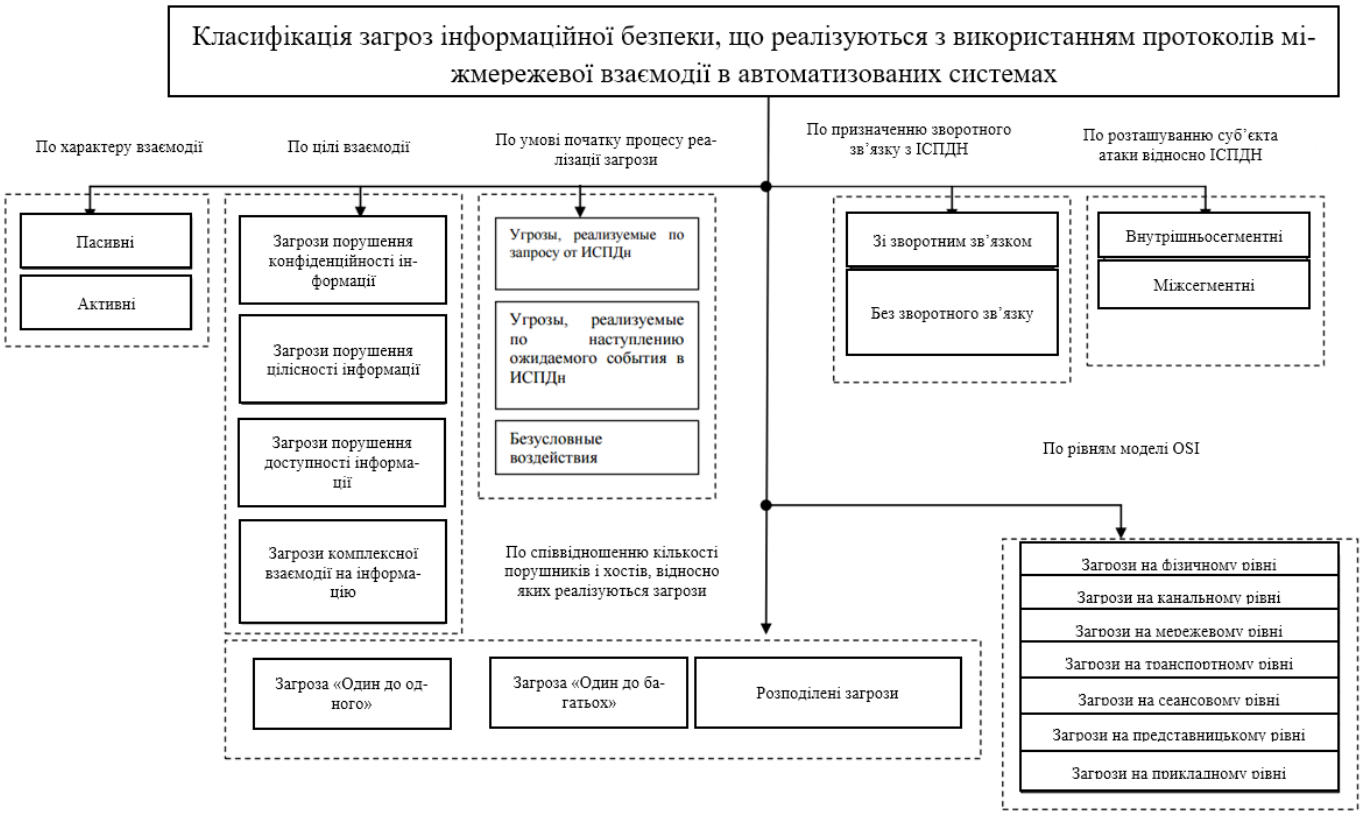

Рис. 1.2. Класифікаційна схема загроз з використанням протоколів міжмережевої взаємодії

Конкретні загрози першого підкласу базуються на активізації файлів, що поширюються у випадку НСД. Приклади таких файлів можуть служити: файли, що містять виконуваний код у вигляді макросів (Microsoft Word, Excel) та тих, що містять виконувані коди у документах HTML, інтерпретовані Java скрипти.

Послуги електронної пошти, передача файлів, мережеві файлові системи можуть бути використані для розповсюдження шкідливих файлів.

Загрози другого підкласу характеризуються втратою контролю над ПЗ, що реалізують мережеві послуги для виконання коду, що містяться в буфері, модифікації системного реєстру та перехоплення ресурсів процесору після блокування через переповнення буфера.

У загрозах третього підкласу злочину використовує здатність дистанційно керувати системою, наданою прихованими компонентами або регулярним контролем та введенням комп'ютерної мережі. В результаті їх використання можна отримати пульт дистанційного керування на вокзалі. Схематичне, основні етапи роботи цих програм є наступним: встановлення в пам'ять; Чекаючи на запит віддаленого хоста, на якому працює клієнтська програма, і вона буде готова поділитися ним; Передайте інформацію клієнту або забезпечити контроль над атакою. Потенційні результати продажу небезпек різних розділів показані в таблиці 1.1.

Таблиця 1.1

Можливі наслідки реалізації загроз різних класів

№ п/п	Тип атаки	Можливі наслідки
1	Аналіз мережевого трафіку	Дослідження характеристик мережевого трафіку, перехоплення переданих даних, в тому числі ідентифікаторів і паролів користувачів
2	Сканування мережі	Визначення протоколів, доступних портів мережевих служб, законів формування ідентифікаторів з'єднань, активних мережевих сервісів, ідентифікаторів і паролів користувачів
3	«Парольна» атака	Виконання будь-якої деструктивної дії, пов'язаної з отриманням несанкціонованого доступу
4	Підміна довіреного об'єкта мережі	Зміна траси проходження повідомлень, несанкціонованих змін маршрутно-адресних даних. Несанкціонований доступ до мережевих ресурсів, нав'язування неправдивої інформації
5	Нав'язування помилкового маршруту	Несанкціонована зміна маршрутно-адресних даних, аналіз і модифікація переданих даних, нав'язування помилкових повідомлень

Закінчення таблиці 1.1

6	Впровадження помилкового об'єкта мережі		Перехоплення і перегляд трафіку. Несанкціонований доступ до мережевих ресурсів, нав'язування неправдивої інформації
7	Відмова в обслуговуванні	Часткове вичерпання ресурсів	Зниження пропускної здатності каналів зв'язку, ефективності мережевих пристроїв. Зниження продуктивності серверних додатків.
		Повне вичерпання ресурсів	Неможливість передачі повідомлень через відсутність доступу до середовища передачі, відмова у встановленні з'єднання. Відмова в наданні сервісу.
		Порушення логічної зв'язаності між атрибутами, даними, об'єктами	Неможливість передачі повідомлень через відсутність коректних маршрутно-адресних даних. Неможливість отримання послуг через несанкціоновану модифікацію ідентифікаторів, паролів і т.п.
		Використання помилок в програмах	Порушення працездатності мережевих пристроїв.
8	Віддалений запуск додатків	Шляхом розсилки файлів, що містять деструктивний код, вірусне зараження.	Порушення конфіденційності, цілісності, доступності інформації.
		Шляхом переповнення буфера серверного додатка	
		Шляхом використання можливостей віддаленого управління системою, що надаються прихованими програмними і апаратними закладками або використовуваними штатними засобами	Приховане управління системою.

У загальному випадку існує чотири етапи в процесі реалізації ризику:

• збирання інформації;

• вторгнення (введення в експлуатаційне середовище);

• реалізація несанкціонованого доступу;

• знищення ознак несанкціонованого доступу.

На етапі збору, порушники зацікавлені в різних відомостях, у тому числі:

• топологія мережі, в якій працює система;

• тип операційної системи (ОС);

• операційні послуги з хостів [1].

У етапі вторгнення присутність конкретної уразливості розглядається в системних службах або помилках у системному адмініструванні. Успішні результати використання вразливості, як правило, отримуються за допомогою процесу привілейованого режиму виконання (доступ до привілейованого режиму процесора), який надходить у нелегальний обліковий запис користувача.

Цей етап небезпеки, як правило, є багатофункціональним. На етапах процесу впровадження небезпеки, наприклад: встановлення спілкування з хостом, де загроза є відносною; Початок шкідливої програми в інтересах розширення прав та інших.

Загроза кінцевої фази відноситься до стека TCP / IP-протоколу, оскільки вона утворюється в мережі на основі механізму вторгнення. Загрози на мережевих та транспортних рівнях поділяються на:

• загроза спрямованості на заміну надійного об'єкта;

• загроза спрямована на створення помилкового маршруту в мережі;

• небезпека з метою прийняття помилкового рішення, використовуючи недоліки алгоритмів дистанційного пошуку;

• "відмова в обслуговуванні" [2].

РОЗДІЛ 2
АНАЛІЗ ІНФОРМАЦІЙНОЇ СИСТЕМИ ПЕРСОНАЛЬНИХ ДАНИХ

2.1. Моделі представлення даних

База даних (БД) являє собою сукупність спеціальним чином організованих даних, що зберігаються в пам'яті обчислювальної системи і відображають стан об'єктів і їх взаємозв'язків в розглянутій предметній області [3].

Логічну структуру збережених в базі даних називають моделлю представлення даних. До основних моделей представлення даних (моделей даних) відносяться наступні: ієрархічна, мережева, реляційна, постреляційна, багатовимірна і об'єктно-орієнтована [3].

Система управління базами даних (СУБД) - це комплекс програмних засобів, призначений для створення, ведення та спільного використання БД багатьма користувачами. Зазвичай СУБД розрізняють по моделі даних. Так, СУБД, засновані на використанні реляційної моделі даних, називають реляційними СУБД [3].

Класифікація СУБД. У загальному випадку під СУБД можна розуміти будь-який програмний продукт, що підтримує процеси створення, ведення і використання БД. Розглянемо, які з наявних на ринку ПЗ мають відношення до БД і в якій мірі вони пов'язані з базами даних.

До СУБД відносяться такі основні види програм:

- повнофункціональні СУБД;
- сервери БД;
- клієнти БД;
- засоби розробки програм роботи з БД [3].

Повнофункціональні СУБД (ПФСУБД) являють собою традиційні СУБД, які спочатку з'явилися для великих машин, потім для міні-машин і для ПЕОМ. З числа

всіх СУБД сучасні ПФСУБД є найбільш численними і потужними за своїми можливостями. До ПФСУБД відносяться, наприклад, такі пакети, як Clarion Database Developer, DataEase, DataFlex, dBase IV, Microsoft Access, Microsoft FoxPro і Paradox R:BASE [3].

Зазвичай ПФСУБД мають розвинений інтерфейс, що дозволяє за допомогою команд меню виконувати основні дії з БД: створювати і модифікувати структури таблиць, вводити дані, формувати запити, розробляти звіти, виводити їх на друк і т.п. Для створення запитів і звітів не обов'язково програмування, а зручно користуватися мовою QBE (Query By Example - формулювання запитів за зразком). Багато ПФСУБД включають засоби програмування для професійних розробників.

Деякі системи мають в якості допоміжних і додаткові засоби проектування схем БД або Case-підсистеми. Для забезпечення доступу до інших БД або до даних SQL-серверів повнофункціональні СУБД мають факультативні модулі [3].

Сервери БД призначені для організації центрів обробки даних в мережах ЕОМ. Ця група БД в даний час менш численна, але їх кількість поступово зростає. Сервери БД реалізують функції управління базами даних, запитувані іншими (клієнтськими) програмами зазвичай за допомогою операторів SQL.

Прикладами серверів БД є наступні програми: MySQL, Oracle Database (Oracle), MS SQL Server (Microsoft), InterBase (Borland), SQLBase.

У ролі клієнтських програм для серверів БД в загальному випадку можуть використовуватися різні програми: ПФСУБД, електронні таблиці, текстові процесори, програми електронної пошти і т.д. При цьому елементи пари «клієнт - сервер» можуть належати одному або різним виробникам програмного забезпечення.

У разі, коли клієнтська і серверна частини виконані однією фірмою, природно очікувати, що розподіл функцій між ними виконано раціонально. В інших випадках зазвичай переслідується мета забезпечення доступу до даних "за всяку ціну". Прикладом такого з'єднання є випадок, коли одна з повнофункціональних СУБД грає роль сервера, а друга СУБД (іншого виробника) - роль клієнта. Так, для сервера БД SQL Server (Microsoft) в ролі клієнтських (фронтальних) програм можуть виступати багато СУБД, такі як dBASE IV, Blyth Software, Paradox, DataEase, Focus, 1-2-3, MDBS III,

Revelation та інші [3].

До засобів розробки призначених для користувача додатків відносяться системи програмування, наприклад Clipper, різноманітні бібліотеки програм для різних мов програмування, а також пакети автоматизації розробок (у тому числі систем типу клієнт-сервер). У числі найбільш поширених можна назвати наступні інструментальні системи: Delphi і C++ Builder (Embarcadero), Visual Basic (Microsoft), SILVERRUN (Computer Advisers Inc.), S-Designor (SDP і Powersoft) і ERwin (LogicWorks).

З точки зору користувача, СУБД реалізує функції зберігання, зміни (поповнення, редагування і видалення) і обробки інформації, а також розробки та отримання різних вихідних документів [3].

Реалізація функції управління даними у зовнішній пам'яті в різних системах може відрізнятися і на рівні управління ресурсами (використовуючи файлові системи ОС або безпосереднє управління пристроями ПЕОМ), і за логікою самих алгоритмів управління даними. В основному методи і алгоритми управління даними є «внутрішньою справою» СУБД і прямого відношення до користувача не мають. Якість реалізації цієї функції найбільш сильно впливає на ефективність роботи специфічних ІС, наприклад, з величезними БД, зі складними запитами, великим обсягом обробки даних.

Необхідність буферизації даних і як наслідок реалізації функції управління буферами оперативної пам'яті обумовлено тим, що обсяг оперативної пам'яті менше обсягу зовнішньої пам'яті.

Буфери являють собою області оперативної пам'яті, призначені для прискорення обміну між зовнішньою і оперативною пам'яттю. У буферах тимчасово зберігаються фрагменти БД, дані з яких передбачається використовувати при зверненні до СУБД або планується записати в базу після обробки.

Механізм транзакцій використовується в СУБД для підтримки цілісності даних в базі. Транзакцією називається деяка неподільна послідовність операцій над даними БД, яка відстежується СУБД від початку і до завершення. Якщо з яких-небудь причин (збої і відмови обладнання, помилки в програмному забезпеченні (ПЗ), включаючи

додаток) транзакція залишається не завершеною, то вона скасовується [3].

Збережені в базі дані мають певну логічну структуру-іншими словами, описуються деякою моделлю представлення даних (моделлю даних), підтримуваної СУБД. До числа класичних відносяться наступні моделі даних:

- ієрархічна;
- мережна;
- реляційна.

Крім того, в останні роки з'явилися, і стали більш активно впроваджуватися на практиці наступні моделі даних:

- постреляційна;
- багатовимірна;
- об'єктно-орієнтована.

Розробляються також всілякі системи, засновані на інших моделях даних, що розширюють відомі моделі. У їх числі можна назвати об'єктно-реляційні, дедуктивно-об'єктно-орієнтовані, семантичні, концептуальні та орієнтовані моделі. Деякі з цих моделей служать для інтеграції баз даних, баз знань і мов програмування.

У деяких СУБД підтримуються одночасно кілька моделей даних.

2.2. База персональних даних

Розглянувши різні моделі подання даних, перейдемо до детального опису БД ПДн. У медичній організації можна виділити два основних підрозділи, що обробляють інформацію, в яку включені ПДн:

Лікувальна (складається зі збору, обробки, зберігання, уточнення, модифікації, знищення персональних даних пацієнтів);

Бухгалтерія та кадри (обробка персональних даних співробітників і контрагентів).

Інші джерела, що містять переважно знеособлення ПДн і ПД для необмеженого кола осіб (поштові клієнти, інтернет сайти та інше ПЗ).

Кожен з підрозділів формує свою БД, що відповідає його специфіці діяльності. Залежно від вимог нормативних і керівних документів, а також внутрішніх наказів і розпоряджень, база може варіюватися. Найчастіше, головну роль у створенні БД надає ПЗ, наявне в наявності, наприклад, СУБД MS Access, що поставляється в комплекті MS Office, дозволяє в короткі терміни створити БД. Розглянемо приклади БД кожного з вищевказаних підрозділів.

Бази даних лікувального підрозділу медичного закладу створюються безпосередньо для:

- підвищення продуктивності праці медпрацівників;
- формування та складання звітності для Міністерства охорони здоров'я України;
- ведення статистики захворюваності (у тому числі на COVID-19) та якості надання медичних послуг установи.

У медичному закладі БД зберігатися на паперових носіях (база карт пацієнтів) і на серверах БД (в ролі сервера може виступити будь-яка ПЕОМ, як окремо стоїть, в разі локальної БД, так і включена в мережу, в разі використанні клієнт-серверної технології).

Розглянемо БД паперових носіїв на прикладі карти пацієнта. Вона включає:

- прізвище;
- ім'я;
- по батькові;
- номер картки;
- дата народження (число, місяць, рік);
- домашня адреса;
- номер телефону;
- місце роботи;
- відомості про здоров'я (включає в себе різноманітну інформації про діагноз, характер лікування, процедури, направлення на госпіталізацію та інші відомості, що відносяться до поняття «історія хвороби») [3].

Організація карт може відрізнятися в різних установах, і для прискорення пошуку використовувати індексацію за номером карти, або за прізвищем. Також можливі вкладені види індексацій, наприклад, по захворюванню і номеру карти, або за місцем проживання і прізвища.

БД, що зберігаються в ЕОМ, можуть досить різноманітні, оскільки потрібно найбільш детально висвітлити різні аспекти діяльності підприємства. Істотною відмінністю від паперового аналога є швидкість доступу і обсяг відомостей одержуваним при автоматизованій обробці БД. Тому для захисту інформації в БД, а також зменшення займаного місця на диску, використовують:

Сегментація. Фізична або логічна сегментація БД в ІСПДН за класами оброблюваної інформації, виділення сегментів мережі, в яких відбувається автоматизована обробка персональних даних.

Знеособлювання. Введення в процес обробки персональних даних процедури знеособлення істотно спростить завдання щодо захисту персональних даних. Знеособлення можна провести шляхом нормалізації баз даних, або кодуванням, або шифруванням (рис. 2.1) [3].

ID	Прізвище	Ім'я	По батькові	Дата народження	Стать
1	Іванов	Іван	Іванович	04.05.2015	м

ID	Прізвище	Ім'я	По батькові	Дата народження	Стать
1	Внвіао	Аівн	Іванович	04.05.2015	м

Рис. 2.1. Знеособлення таблиці шляхом шифрування.

Поділ ПДн на частини. У цьому випадку можливе зменшення кількості суб'єктів ПДн, які обробляються в системі. Це може бути досягнуто, наприклад, за рахунок використання таблиць перехресних посилань в базах даних.

Абстрагування ПДн. Найчастіше на деяких ділянках обробки або сегментах мережі персональні дані можна зробити менш точними, наприклад, шляхом групування загальних характеристик [3].

ID	Прізвище	Ім'я	По батькові	Дата народження	Стать
1	Іванов	Іван	Іванович	04.05.2015	м
2	Петров	Іван	Іванович	25.05.2012	м

ID	Прізвище	Ім'я	По батькові	Вік	Стать
1	Іванов	Іван	Іванович	менше 18	м
2	Петров	Іван	Іванович	менше 18	м

Рис. 2.2. Абстрагування ПДн

Бази даних лікарні створюються і використовуються декількома типами програм: Office Access 2019, або Microsoft Office Access 2010 (дані зберігаються у форматі *.mdbx, рідше *.accdb); Office Excel 2019, або Microsoft Office Excel 2010 (дані зберігаються у форматі *.xlsx).

Переваги даних СУБД:

- швидкість розробки;
- сумісність з більшістю ПЕОМ під управлінням ОС Windows.

Недоліки:

- відсутність захисту, або низький захист даних;
- проблеми з багатокористувацьким доступом (для xlsx, DBF більше 3, для mdbx більше 7 користувачів);
- низька швидкість роботи з великим об'ємом даних;
- циркуляція великого обсягу даних в мережі при багатокористувацькому доступі.

Розглянемо приклад, БД, створену в MS Access, з 12 полями і 10000 записами, що займає дискового простору близько 111 МБ. Дана БД зберігатися на сервері і 3 Користувача починають працювати з нею одночасно. При кожному виконаному процесі, користувачеві направляється копія БД зі змінами інших користувачів. У підсумку виходить циркуляція в мережі трафіку на 333 МБ і, якщо обладнання не справляється, виникає «відмова в обслуговуванні» санкціонованих користувачів. Ілюстрація наведена на рис. 2.3.

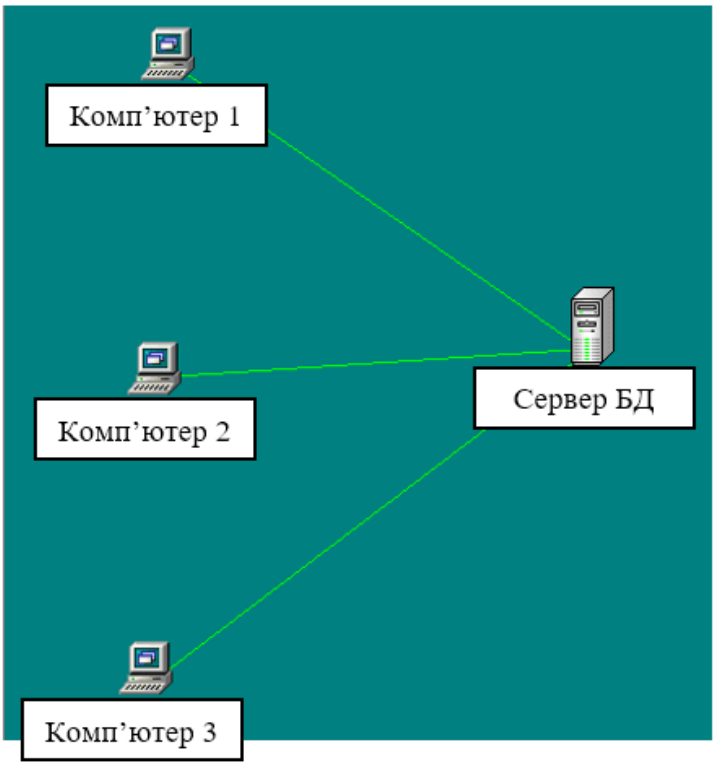

Рис. 2.3. Проблеми доступу до БД за допомогою MS Access, BDE

Розглянувши БД лікувального підрозділу медичної установи, потім перейдемо до бухгалтерії та кадрів. ПДн в даному підрозділі можна розділити на два типи: ПДн співробітників і контрагентів, які взаємодіють з підприємством за договорами. Основними відомостями про працівників підприємства, що підлягають захисту є:

- прізвище, ім'я, по батькові;
- місце, рік і дата народження;
- адреса за пропискою;
- паспортні дані (Серія, номер паспорта, ким і коли виданий);
- інформація про освіту (найменування освітнього закладу, відомості про документи, що підтверджують освіту: найменування, номер, дата видачі, спеціальність);
- інформація про трудову діяльність до прийому на роботу;
- інформація про трудовий стаж (місце роботи, посада, період роботи, причини звільнення);
- адреса проживання (реальна);

- телефонний номер (домашній, робочий, мобільний);
- сімейний стан і склад сім'ї (чоловік / дружина, діти);
- інформація про знання іноземних мов;
- форма допуску;
- оклад;
- дані про трудовий договір (№ трудового договору, дата його укладення, дата початку і дата закінчення договору, вид роботи, термін дії договору, наявність випробувального терміну, режим праці, тривалість основної відпустки, тривалість додаткової відпустки, тривалість додаткової відпустки за ненормований робочий день, обов'язки працівника, додаткові соціальні пільги і гарантії, № і число зміни до трудового договору, характер роботи, форма оплати, категорія персоналу, умови праці, тривалість робочого тижня, система оплати);
- відомості про військовий облік (категорія запасу, військове звання, категорія придатності до військової служби, інформація про зняття з військового обліку);
- ІПН;
- дані про атестацію працівників;
- дані про підвищення кваліфікації;
- дані про нагороди, медалі, заохочення, почесні звання;
- інформація про прийняття на роботу, переміщення за посадою, звільнення;
- інформація про відпустки;
- інформація про відрядження;
- інформація про хвороби;

Відомості про контрагентів включають:

- прізвище, ім'я, по батькові;
- місце, рік і дата народження;
- юридична та фактична адреса;

- паспортні дані (серія, номер паспорта, ким і коли виданий), або реєстраційний номер підприємства, код за класифікатором та ін.;
- ІПН;
- номер рахунку в банку;
- телефон контактної особи.

Зазвичай дані поля зберігаються в одному місці і змінити формат БД неможливо, або важко, оскільки наявне ПЗ, не дозволяє цього зробити, або більше не підтримується автором (багато установ працюю на програмах більше 10-річної давності, а оновлення більше не виходять). Наприклад, популярна бухгалтерська програма» 1С Підприємство " зберігає всі відомості в одному файлі (починаючи з версії 8.0).

2.3. Структура і загрози мережі медичної установи

Медичні установи, в залежності від їх розміру, включають:

- лабораторія;
- поліклініка;
- управління;
- косметологічні відділення;
- лікарня.

Локальна мережа конкретного медичного закладу являє собою односекційну мережу з топологією "зірка", в якій використовується технологія Fast Ethernet, показана на рис.2.4.

Немає контролера домену і, отже, немає дискримінації прав доступу до АРМ користувачів, а сервер також використовується в якості інтернет-шлюзу і сховища файлів.

Для зв'язку з організаціями високого рівня (Міністерство охорони здоров’я України) використовується надійний кур'єр зі знімним носієм. Цей метод перенесення неефективний з кількох причин:

- низька швидкість передачі даних;

- висока ймовірність крадіжки, втрати або зміни Даних під час доставки; необхідність відвернути співробітника від його основних обов'язків.

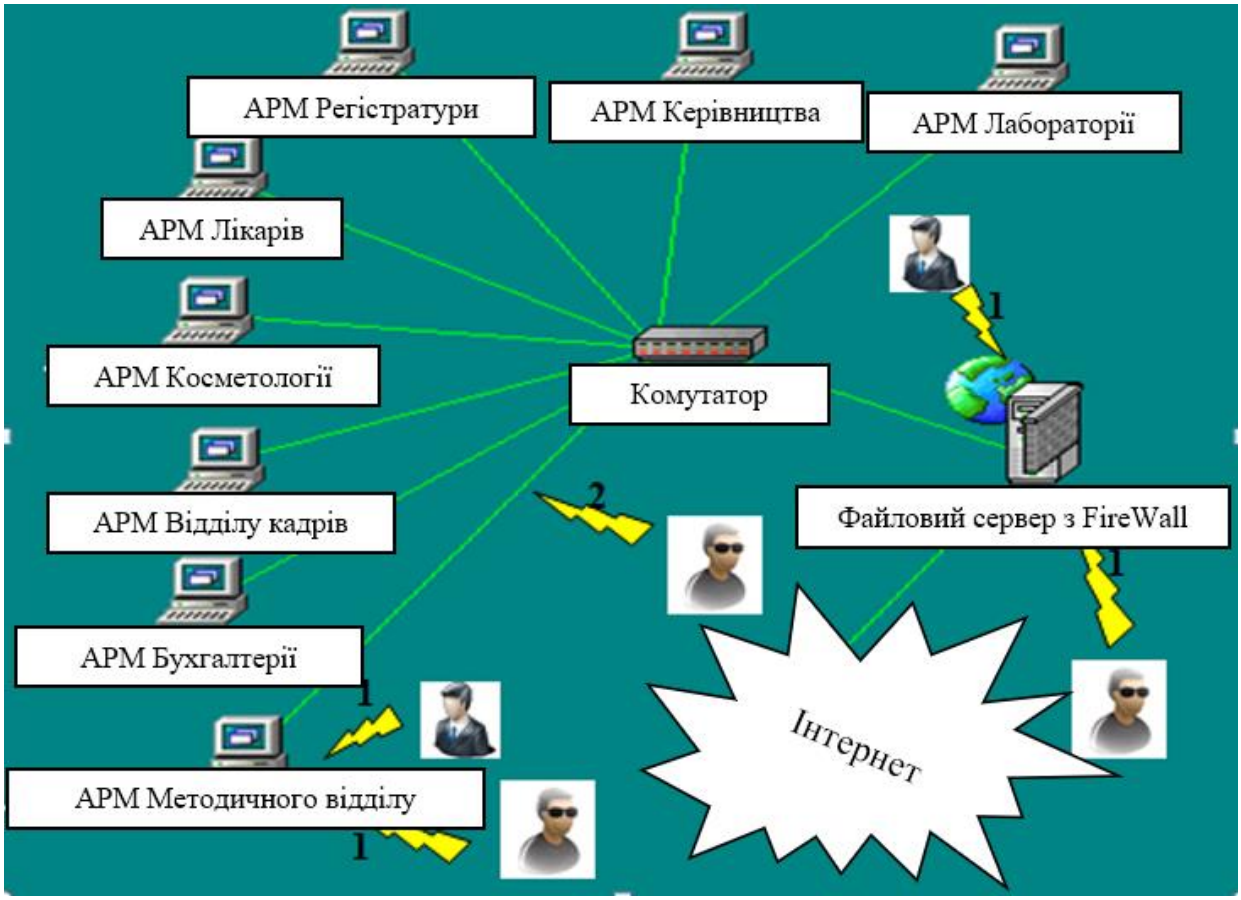

Рис. 2.4. Мережа медичної установи (1 - загрози несанкціонованого доступу до інформації, 2 - загрози витоку конфіденційної інформації)

У цьому медичному закладі використовуються виключно несертифіковані засоби захисту:

- Avira безкоштовний антивірус;
- вбудований ITU в Windows 10 Server.

Перераховані засоби безпеки забезпечують незначний захист від вузького спектру загроз (просте шкідливе ПЗ, захист від НСД зовнішніх непідготовлених зловмисників).

На основі структури локальної мережі ми можемо визначити основні загрози:

- загроза витоку інформації по технічних каналах;

- загрози НСД для ПДН автоматично обробляються на робочому місці.

До небезпек витоку інформації по технічних каналах відносяться:

- загроза витоку акустичної (мовної) інформації;
- загроза витоку інформації про види;
- загроза витоку інформації по каналу ПЕМВН [4].

Виникнення загроз витоку акустичної (мовної) інформації, що безпосередньо міститься в усному мовленні користувача ІСПДН, можливо при наявності функцій голосового введення ПД в ІСПДН або відтворення ПД акустичними засобами ІСПДН.

Реалізація загрози витоку конкретної інформації можлива шляхом перегляду інформації з використанням оптичних (оптико-електронних) екранів відображення та інших засобів відображення комп'ютерної техніки, інформаційно-обчислювальних комплексів, технічних засобів обробки графічної, відео-і буквено-цифрової інформації, що входять до складу ІСПДН [4].

Загроза витоку інформації по каналу ПЕМВН можлива через наявність електромагнітного випромінювання, в першу чергу моніторів і блоків комп'ютерної системи. Основною небезпекою є ризик витоку через наявність електромагнітного випромінювання монітора [4].

Загрози НСД для AWP пов'язані з діями порушників, що мають доступ до ІСПДН, в тому числі користувачів ІСПДН, які застосовують загрози безпосередньо до ІСПДН. Крім того, апаратні закладки та носії шкідливих програм можуть бути джерелами загроз інформації в автоматизованих системах управління. Загрози НСД в ІСПДН пов'язані з діями порушників, що мають доступ до ІСПДН, в тому числі користувачів ІСПДН, що реалізують загрози безпосередньо в ІСПДН, а також порушників, які не мають доступу до ІСПДН, що реалізують загрози із зовнішніх мереж зв'язку загального користування і (або) міжнародних мереж обміну інформацією [4, 6].

До небезпек НСД в ІСПДН, пов'язаних з діями порушників, відносяться:

- модифікація базової системи введення-виведення (BIOS), перехоплення управління завантаженням з метою перехоплення паролів або ідентифікаторів, що застосовуються під час завантаження операційної системи;

- загрози, що реалізуються після завантаження операційної системи і спрямовані на здійснення несанкціонованого доступу з використанням стандартних дій (знищення, копіювання).
- форматування носія даних і т. д. з використанням операційних систем або будь-яких прикладних програм (наприклад, системи управління базами даних), з використанням програм, створених спеціально для роботи НСД (програми для перегляду і зміни реєстру, пошуку текстів в текстових файлах і ін.);
- загрози впровадження шкідливих програм.

Загрози для зовнішніх мереж включають в себе:

- із загрозою "аналізу мережевого трафіку" і перехоплення переданої з нього інформації;
- зовнішня мережа "аналіз мережевого трафіку" загрожує перехопленням інформації, переданої і отриманої із зовнішніх мереж;
- сканування загроз, спрямованих на виявлення типу операційної системи AWP, відкритих портів і служб, відкритих з'єднань і т. д.;
- загрози виявлення паролів;
- загрози отримання НСД шляхом підміни довіреного об'єкта;
- загрози відмови в обслуговуванні»;
- загрози для віддаленого запуску додатків;
- загрози впровадження шкідливих програм в мережу.

Ризик зараження комп'ютера виникає через поширення шкідливих програм:

- знімний носій;
- заражені веб-сторінки;
- вкладення електронної пошти;
- дірки в мережевій безпеці;
- заражені файли і документи [4, 6-8].

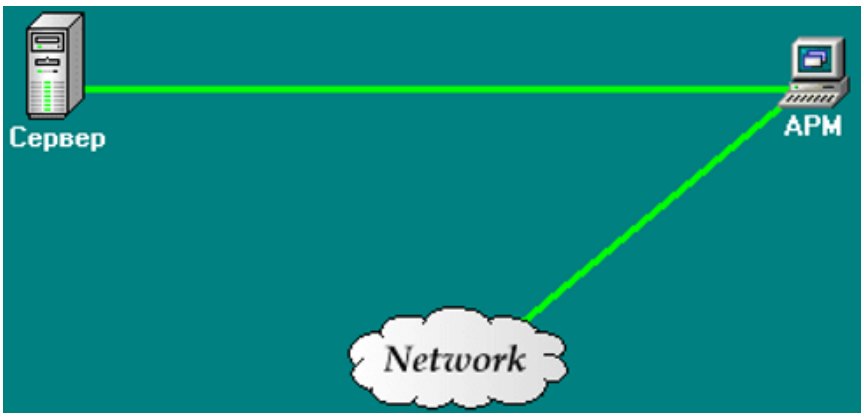

Рис. 2.5. Канали поширення шкідливого програмного забезпечення

Причини відсутності небезпеки НСД для ПД виникають:

- диференціація прав доступу;
- захист передачі даних по каналах зв'язку;
- ідентифікація та аутентифікація об'єктів ПДН;
- витоку по технічних каналах.

Загрози відмови в обслуговуванні викликані:

- помилки програмного забезпечення;
- не відповідає потужності ПК для завдань, покладених на нього (рис. 2.5);
- повінь (flood) [7].

Небезпека перехоплення даних і підміни виникає з наступних причин:

- уразливості в стеку протоколів TCP / IP;
- відсутність шифрування каналів передачі інформації;
- компрометація криптографічних ключів.

Причини виникнення небезпеки крадіжки знімних носіїв:

- відсутність безпечних місць зберігання даних;
- відсутність спеціалізованих засобів обробки даних;
- загрози видалення інформації виникають через особливості процесів, що відбуваються в лініях зв'язку [7].

2.4. Засоби захисту інформації

Засоби захисту інформації - це сукупність інженерно-технічних, електричних, електронних, оптичних та інших пристроїв і технічних систем, а також інших фірмових елементів, використовуваних для вирішення різних завдань захисту інформації, в тому числі запобігання витоків і забезпечення збереження інформації, що захищається [8].

В цілому засоби забезпечення інформаційної безпеки з точки зору запобігання навмисних дій в залежності від способу реалізації можна розділити на групи:

Апаратне забезпечення - це окремий тип пристрою (механічне, електричне, електронне і т.д.), апаратне забезпечення якого вирішує проблему інформаційної безпеки. Вони блокують доступ до інформації, в тому числі маскують її. Апаратне забезпечення включає в себе: генератор шуму, фільтр перенапруги, скануюче радіо і багато інших пристроїв, які "блокують" можливі канали витоку інформації або дозволяють їх виявляти. Переваги технічних засобів пов'язані з їх надійністю, незалежністю від суб'єктивних факторів і високою стійкістю до модифікації. Слабкість-відсутність гнучкості, відносно великий обсяг і вага, висока вартість [8].

До основних апаратних засобів забезпечення інформаційної безпеки відносяться:

- інструменти для введення, що ідентифікує користувача інформації (магнітні та пластикові карти, відбитки пальців і т.д.);
- інструменти для шифрування інформації (наприклад, akpsh «Континент»);
- інструменти для запобігання несанкціонованій активації робочих станцій і серверів (електронні замки і блокатори);
- інструменти для знищення інформації в засобах масової інформації;
- пристрої сигналізації про спроби несанкціонованих дій користувачів комп'ютерних систем і т.д. [10].

Програмні засоби включають програми для ідентифікації користувачів, контролю доступу, шифрування інформації, видалення залишкової (робочої) інформації, такої як тимчасові файли, тестового контролю системи безпеки і т.д. Перевагами програмних засобів є універсальність, гнучкість, надійність, простота установки, можливість модифікації і розробки. Недоліки - обмежена функціональність мережі, використання частини ресурсів файлових серверів і робочих станцій, висока чутливість до випадкових або навмисних змін, можлива залежність від типу комп'ютерів (їх апаратного забезпечення) [5].

Програмні засоби включають в себе:

- засоби інформаційної безпеки, вбудовані в ОС (механізми ідентифікації та аутентифікації, контроль доступу, аудит і т.д.);
- антивірус (antivirus) - програма для виявлення комп'ютерних вірусів і лікування заражених файлів, а також для запобігання зараження файлів або операційної системи шкідливим кодом (найбільш відомими антивірусними програмами є ESET NOD 32, Антивірус Касперського, Dr.Web, PANDA Antivirus Avira Antivirus);
- криптографічні методи захисту інформації - це методи шифрування, кодування або іншого перетворення інформації, в результаті яких її зміст стає недоступним без пред'явлення ключа криптограми і зворотного перетворення. Криптографічний метод захисту на сьогоднішній день є найбільш надійним методом захисту, оскільки сама інформація захищена, не має доступу до неї (наприклад, зашифрований файл не може бути прочитаний, навіть якщо носій вкрадений). Криптографічні програми діляться на вбудовані в операційну систему (cryptographic service provider (CSP) - постачальник криптографічних послуг) і виконуються як окремі додатки. Найбільш поширеними є Microsoft Cryptographic Provider, CryptoPro CSP, VIPNET CSP, Shipka CSP [5].

Брандмауер (FireWall) – це пристрій контролю доступу до мережі, призначений для блокування всього трафіку, за винятком дозволених даних. Існує два основних типи брандмауерів: брандмауери на рівні додатків і брандмауери з фільтрацією пакетів. Вони засновані на різних принципах роботи, але при правильному налаштуванні

обидва типи пристроїв забезпечують правильне виконання функцій безпеки, включаючи блокування забороненого трафіку [9]. Приклад розташування брандмауера (ITU) показаний на рис. 2.6.

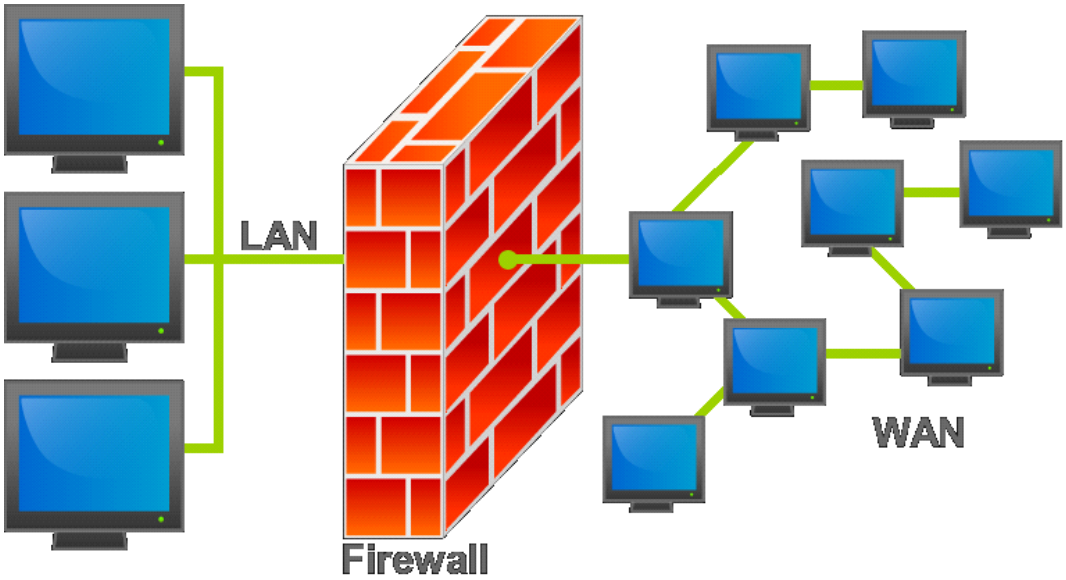

Рис. 2.6. Місце FireWall в мережі

Proxy-сервер (від англійського proxy – «делегувати, авторизувати») - це служба в комп'ютерних мережах, яка дозволяє клієнтам робити непрямі запити до інших мережевих служб. Спочатку клієнт підключається до проксі-сервера і запитує деякий ресурс (наприклад, електронну пошту), розташований на іншому сервері. Потім проксі-сервер або підключається до зазначеного сервера і отримує від нього ресурс, або повертає ресурс зі свого кешу (в тих випадках, коли проксі має свій власний кеш). У деяких випадках запит клієнта або відповідь сервера може бути змінений проксі-сервером для певних цілей. Крім того, проксі-сервери дозволяють захистити клієнтські комп'ютери від певних мережевих атак і допомагають підтримувати анонімність клієнтів. Найбільш поширеними є 3Proxy, Kerio Control, Squid і UserGate [9]. Приклад проксі-сервера показаний на рис. 2.7.

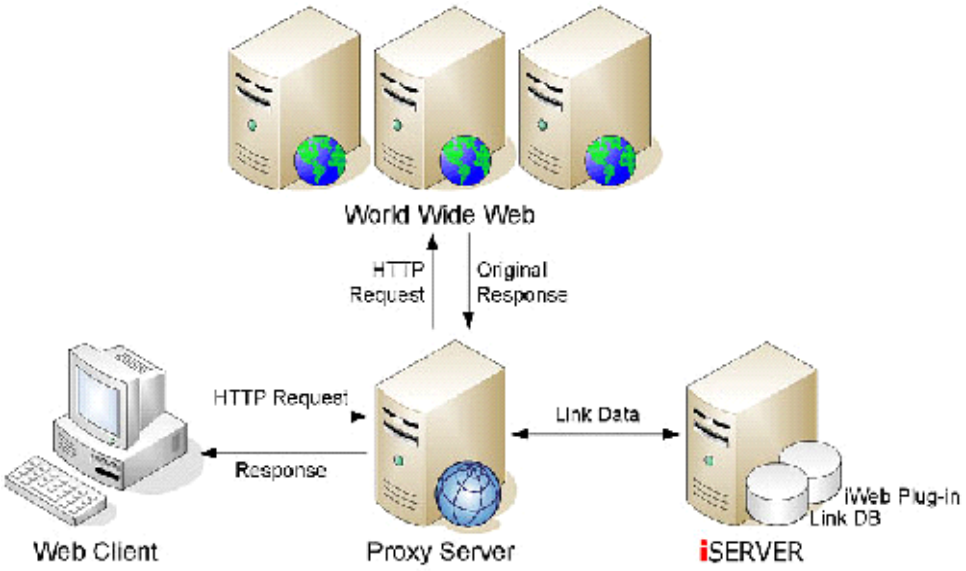

Рис. 2.7. Приклад використання Proxy-сервера

VPN називається інтеграцією локальних мереж і персональних комп'ютерів через відкрите зовнішнє середовище для передачі інформації в єдину віртуальну корпоративну мережу, що забезпечує безпеку циркулюючих даних (рис. 2.8) [9].

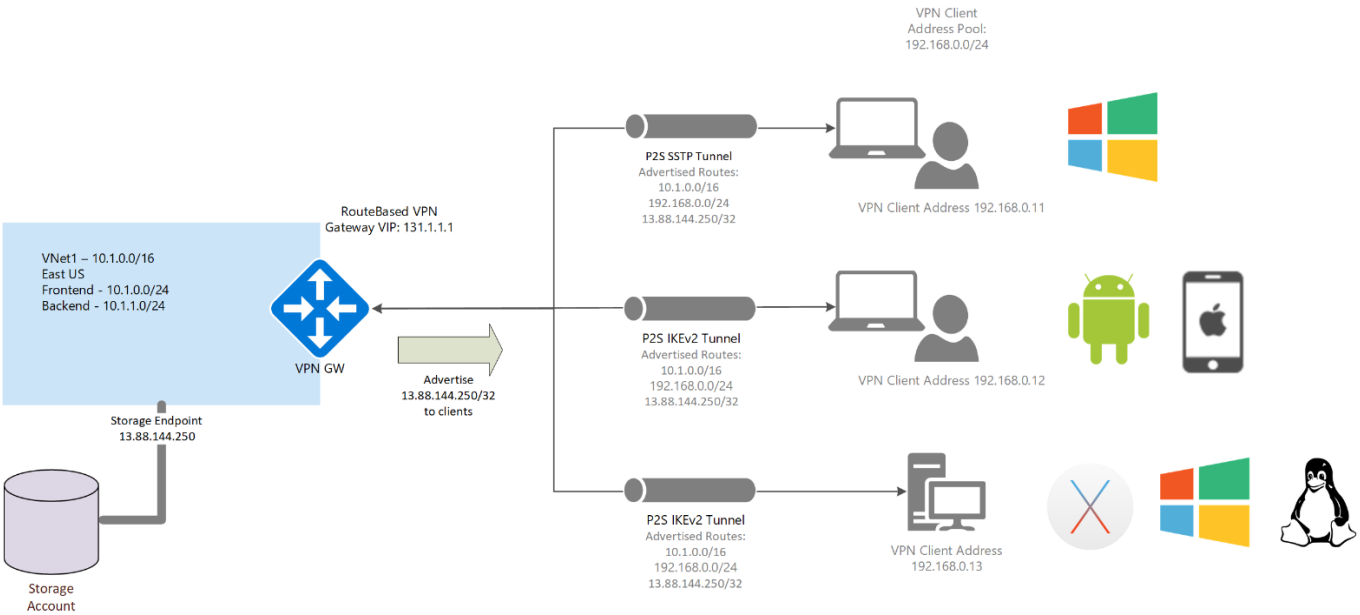

Рис. 2.8. Конфігурація користувальницької VPN

Найбільш поширеними програмами для створення VPN є: OpenVPN, CISCO WORK VPN, VIPNET, CUSTOM CSP VPN, StoneGate SSL VPN.

Система виявлення вторгнень (IDS) - це програмний засіб, призначений в першу чергу для виявлення фактів несанкціонованого використання комп'ютерної системи або мережі або несанкціонованого управління ними через Інтернет [9]. Класифікація ідентифікаторів може бути:

- метод реакції;
- виявлення атаки;
- метод збору інформації про атаку.

Відповідно до методу відповіді розрізняють пасивні і активні ідентифікатори. Пасивні ідентифікатори просто записують факт атаки, записують дані в файл журналу і видають попередження. Активні ідентифікатори намагаються протистояти атаці, наприклад, переналаштовуючи або створюючи списки доступу до маршрутизатора.

Відповідно до методу виявлення атаки системи IDS зазвичай діляться на дві категорії:

- виявлення аномальної поведінки (на основі аномалій);
- виявлення зловживань (виявлення зловживань або на основі підпису).

Класифікація за способом збору інформації про атаку:

- виявлення атак на мережевому рівні (на основі мережі);
- на основі хоста;
- виявлення атак на основі додатків.

Програмно-апаратні засоби реалізують ті ж функції, що і апаратні та програмні засоби окремо, і мають проміжні властивості [11].

Ці пристрої зазвичай складаються з декількох частин:

- апаратний ключ, що забезпечує ідентифікацію та аутентифікацію користувача (наприклад, ibaton, etokan, rutokan);
- читач;
- PCIe-карти для інтеграції механізмів безпеки в ПК.

Найбільш відомими засобами є: НЕТТО ПАК "Соболь", КриптоЗамок, МДЗ-Ешелон.

2.5. Організаційні заходи захисту інформації в медичній установі

Неможливо досягти високого рівня безпеки без вжиття відповідних організаційних заходів. З одного боку, ці заходи повинні бути спрямовані на забезпечення правильного функціонування механізмів безпеки і здійснюватися адміністратором системної безпеки. З іншого боку, керівництво організації, що експлуатує засоби автоматизації, має регламентувати правила автоматизованої обробки інформації, в тому числі правила її безпеки, а також встановити міру відповідальності за порушення цих правил.

Для безпосередньої організації (створення) та ефективного функціонування системи інформаційної безпеки в АС може бути створена спеціальна штатна служба безпеки (служба комп'ютерної безпеки) (а для великого обсягу інформації, що захищається вона повинна бути) [11, 14-15].

Служба комп'ютерної безпеки - це штатний або нестандартний підрозділ, створений для організації кваліфікованого розвитку системи інформаційної безпеки та забезпечення її функціонування.

Основними функціями сервісу є наступні:

- формування вимог до системи безпеки в процесі створення АС;
- участь у проектуванні системи безпеки, її випробуваннях та введенні в експлуатацію;
- планування, організація та забезпечення функціонування системи інформаційної безпеки при експлуатації автоматизованої системи управління;
- розподіл необхідних відомостей про безпеку між користувачами;
- моніторинг функціонування системи безпеки та її елементів;
- організація перевірок надійності систем безпеки;
- навчання користувачів і персоналу автоматизованих систем управління правилам безпечної обробки інформації;
- контроль за дотриманням користувачами і персоналом автоматизованих систем управління встановлених правил поводження з захищеною інформацією в

процесі її автоматизованої обробки;

- вжиття заходів у разі спроб НРД отримати доступ до інформації та порушення правил функціонування системи безпеки.

Організаційно-правовий статус Служби безпеки (СБ) визначається наступним чином:

- кількість співробітників СБ повинна бути достатньою для виконання всіх перерахованих вище дій;
- СБ повинна звітувати перед особою, яка несе особисту відповідальність за дотримання правил поводження із захищеною інформацією в даній установі;
- співробітники СБ не повинні мати інших обов'язків, пов'язаних з операцією обробки ПДН;
- співробітники СБ повинні мати право доступу в усі приміщення, де встановлено обладнання СБ, і мати право припинити автоматичну обробку інформації, якщо існує безпосередня загроза інформації, що захищається;
- керівнику СБ має бути надано право заборонити включення нових елементів АС в число існуючих, якщо вони не відповідають вимогам інформаційної безпеки;
- СБ повинна бути забезпечена всіма умовами, необхідними для виконання її функцій [12].

Всі ці функції не під силу одній людині, особливо якщо організація досить велика. Крім того, в службу комп'ютерної безпеки можуть входити співробітники з різними функціональними обов'язками. Як правило, існує чотири групи співробітників (в порядку зростання ієрархії).

Член команди безпеки. В його обов'язки входить забезпечення належного контролю за безпекою наборів даних і програм, надання допомоги користувачам і організація загальної підтримки для управління безпекою та управлінських груп в їх зоні відповідальності. У разі децентралізованого управління кожна підсистема АС має своїх власних співробітників групи безпеки.

Адміністратор системної безпеки. У його обов'язки входить щомісячна публікація інновацій в області безпеки, нових стандартів, а також безперервна робота і моніторинг планів відновлення (при необхідності) і зберігання резервних копій.

Адміністратор захисту даних. У його обов'язки входить впровадження і заміна засобів захисту даних, Моніторинг стану безпеки наборів даних, посилення безпеки, якщо це необхідно, і координація з іншими адміністраторами.

Керівник групи обробки інформації та управління безпекою. В його обов'язки входить розробка і підтримка ефективних заходів безпеки при обробці інформації для забезпечення безпеки даних, обладнання та програмного забезпечення; моніторинг здійснення планування відновлення і загального Управління адміністративними групами в підсистемах АС (з децентралізованим управлінням).

Існують різні варіанти докладного штатного розкладу для такої групи, яке включає перелік функціональних обов'язків, розподіл необхідних знань і навичок, а також час і зусилля. При організації безпеки існування такої групи і докладні обов'язки її співробітників абсолютно необхідні [14].

Для організації та забезпечення ефективного функціонування інтегрованої системи комп'ютерної безпеки необхідно розробити наступні групи організаційно-розпорядчих документів:

- документи, що визначають порядок і правила забезпечення безпеки інформації при її обробці в АС (план захисту інформації в АС, план забезпечення безперервної роботи і відновлення інформації);
- документи, що визначають відповідальність організацій (суб'єктів), що взаємодіють при обміні електронними документами (угода про організацію обміну електронними документами).

План інформаційної безпеки в АС повинен містити наступну інформацію:

- опис захищеної системи (основні характеристики об'єкту, що охороняється): призначення, перелік завдань, що вирішуються АС, конфігурація, характеристики і розміщення категорій технічних засобів і програмного забезпечення, перелік інформації (пакетів, файлів, наборів і баз даних, в яких вони містяться), що підлягає захисту в АС, і вимоги до забезпечення доступності, конфіденційності, цілісності цих категорій інформації, список користувачів і їх право на використання системних ресурсів і т. д.; Мета захисту систем і методів забезпечення безпеки АС і переданої інформації;
- перелік важливих загроз безпеці АС, захист від яких необхідний і найбільш ймовірні способи нанесення збитку;
- основні вимоги до організації процесу функціонування автоматизованих систем управління та заходи щодо забезпечення безпеки оброблюваної інформації ;
- вимоги до визначення зон відповідальності встановлюються в системі Умов використання та технічних засобів захисту від НРД;
- основні правила, що регулюють діяльність персоналу з питань забезпечення безпеки АС (спеціальні обов'язки співробітників АС).
- план забезпечення безперервної роботи і відновлення інформації повинен відображати наступні питання системи.

Угода про порядок організації обміну електронними документами повинна включати документи, що відображають наступні питання:

- розмежування відповідальності суб'єктів, які беруть участь в обміні електронними документами;
- визначення порядку підготовки, обробки, передачі, отримання, перевірки справжності та цілісності електронних документів;
- визначення процесу генерації, аутентифікації і поширення важливої інформації (ключів, паролів і т.д.);
- визначення порядку вирішення спорів у разі виникнення конфліктів.

2.6. Цикл обробки персональних даних

Обробка персональних даних вимагає створення спеціального режиму, в якому чітко визначені технологія їх обробки, порядок і умови існування ПДН на кожному етапі їх життєвого циклу. Вона включає в себе розробку і впровадження процедур їх збору, прийому, обліку, реєстрації, зберігання, використання, знищення і т.д. велике значення має термін придатності ПДС, а також наявність системи моніторингу обробки ПДС на всіх етапах їх життєвого циклу.

Час обробки також визначається на підставі інших нормативних правових актів. Таким чином, вимоги трудового, цивільного, пенсійного законодавства та галузевих нормативних актів встановлюють певні терміни обробки персональних даних.

Концепція життєвого циклу (LC), яка є однією з основних концепцій методології проектування САПР та багатьох інших ІС, лежить в основі її створення та використання (ІСПДН є її приватною частиною). В даний час існує кілька поширених методів розробки ІС. Головне в них-єдина дисципліна роботи на всіх етапах життєвого циклу системи, облік важливих завдань і моніторинг їх вирішення, використання передових інструментів підтримки процесів аналізу, проектування і впровадження ІС.

В цілому термін "життєвий цикл системи" відноситься до певного розвитку, періоду часу і набору функцій, які змінюють стан системи від появи концепції і початку її розвитку до кінця експлуатації. Вона зазвичай ділиться на окремі етапи-аналіз вимог, проектування, впровадження (створення), верифікація та експлуатація. Етапи розвитку системи можуть повторюватися у зв'язку з поступовим уточненням вимог до системи та/або необхідністю її адаптації до змін, що відбуваються в предметній області системи.

Концепція системи LC дозволяє визначити поняття життєвого циклу ІС (LC is) - моделі створення і використання (розвитку) ІС, що відображає різні її стану, починаючи з моменту виникнення необхідності в даному наборі інструментів для створення та обміну інформацією і закінчуючи моментом її повного виведення з використання Користувачем.

ЛК - це сукупність періодів часу і завдань, від моменту виникнення і обґрунтування необхідності будівництва до моменту недоцільності його подальшої експлуатації, тобто це сукупність взаємопов'язаних процесів створення і поступової зміни стану ІС, що змінюють стан системи, від формування вихідних вимог [11].

Що стосується ПД, то життєвий цикл ІС має етапи від їх виникнення до повного знищення.

Приклад. Пацієнт, який потребує медичної допомоги, приходить до медичного закладу. У реєстрі його просять вказати номер карти або повне ім'я. Повідомивши ідентифікаційну інформацію, співробітники реєстратури шукають в базі даних картку цього пацієнта. Якщо карта не відкрита, вона запускається, потім візит реєструється і відправляється до лікаря пацієнта. Якщо карта вже відкрита, пацієнт направляється до лікаря відразу після реєстрації візиту. У лікаря пацієнт знову проходить стадії 1,2 і 4. Повторний візит-етап 3, він передається пацієнтами в разі зміни їх персональних даних, наприклад, прізвища або політики. Потім ПД обробляється методичним відділом, де збирається статистика по захворюваності і якості медичної допомоги. Знищення ПД відбувається тільки після досягнення мети їх обробки.

Якщо замість поліклініки ви розглянете інше відділення, то зміняться тільки назви місць і посад осіб, відповідальних за обробку ПДН, наприклад, начальник відділу кадрів і діловодства або бухгалтерія і бухгалтер.

Таким чином, в цьому розділі розглядаються основні компоненти для створення захищеної мережі обробки ПДН. Детально розглянуто організацію зберігання ПД у базі даних, класифікацію програмного та апаратного забезпечення, основні засоби захисту локальної мережі, наведено організаційні заходи безпеки.

…

РОЗДІЛ 3
РОЗРОБКА ЗАХОДІВ ЗАХИСТУ ПЕРСОНАЛЬНИХ ДАНИХ В МЕДИЧНІЙ УСТАНОВІ

3.1. Заходи щодо захисту локально-обчислювальної мережі та баз даних медичної установи

Щоб захистити локальну мережу, необхідно розділити її на 4 секції:

- загальна медицина (зберігає лише загальну інформацію про повне ім'я, дату народження, поле, домашню адресу, номер карти, серію та номер паспорту пацієнта);
- спеціальна медицина (зберігає інформацію про стан здоров'я, лабораторні аналізи та інші відомості про пацієнта, що відносяться до певної категорії);
- бухгалтерський облік і управління персоналом (зберігає інформацію про співробітників медичного закладу);
- загальні відомості (всі інші відомості про абонентів мережі).

Після зміни організації мережі зміниться і організація бази даних, що складається з декількох розподілених частин.

На файловому сервері (SRV2), крім його основного призначення (для зберігання різних призначених для користувача файлів), буде створена база даних, що складається з таблиць, які не мають зв'язку один з одним і зберігають довідкову інформацію. Ці дані буде поміщено в базу даних:

- довідник прізвищ, імен, по батькові;
- довідник суб'єктів, населених пунктів, адміністративно-територіальних одиниць суб'єктів, доріг;
- довідники діагностики відповідно до Міжнародної класифікації хвороб (МКБ);
- довідник страхових компаній (містить назву страхової компанії і серію

полісів, які її видають).

Таким чином, ця база даних містить тільки репліковану інформацію (між таблицями немає зв'язків).

Сервер, на якому зберігається Загальна медична інформація (SRV4), буде містити наступні дані:

- номер картки;
- дата народження;
- стать;
- індекс прізвища, імені, по батькові, місця проживання;
- індекс ланцюжка політик, номер політики;
- місце роботи;
- телефон;
- інша інформація, необхідна для медичної діяльності, але не пов'язана з ПДН.

Всі індекси беруться з каталогів SRV2, що в кінцевому підсумку призводить до зменшення обсягу ПД, не ставлячи під загрозу роботу установи. Зв'язок між таблицями встановлюється на основі "ПД + номер карти", де ПД - пункти 2-8 перераховані вище.

Сервер, на якому зберігається спеціальна медична інформація (SRV5), матиме наступні дані:

- номер картки;
- індекс діагностики МКБ;
- інформація про стан здоров'я (історія хвороби);

інша інформація, необхідна для медичної діяльності, пов'язаної з особливою категорією ПДН.

Спроектована захищена мережа лікарні показана на рис .3.1.

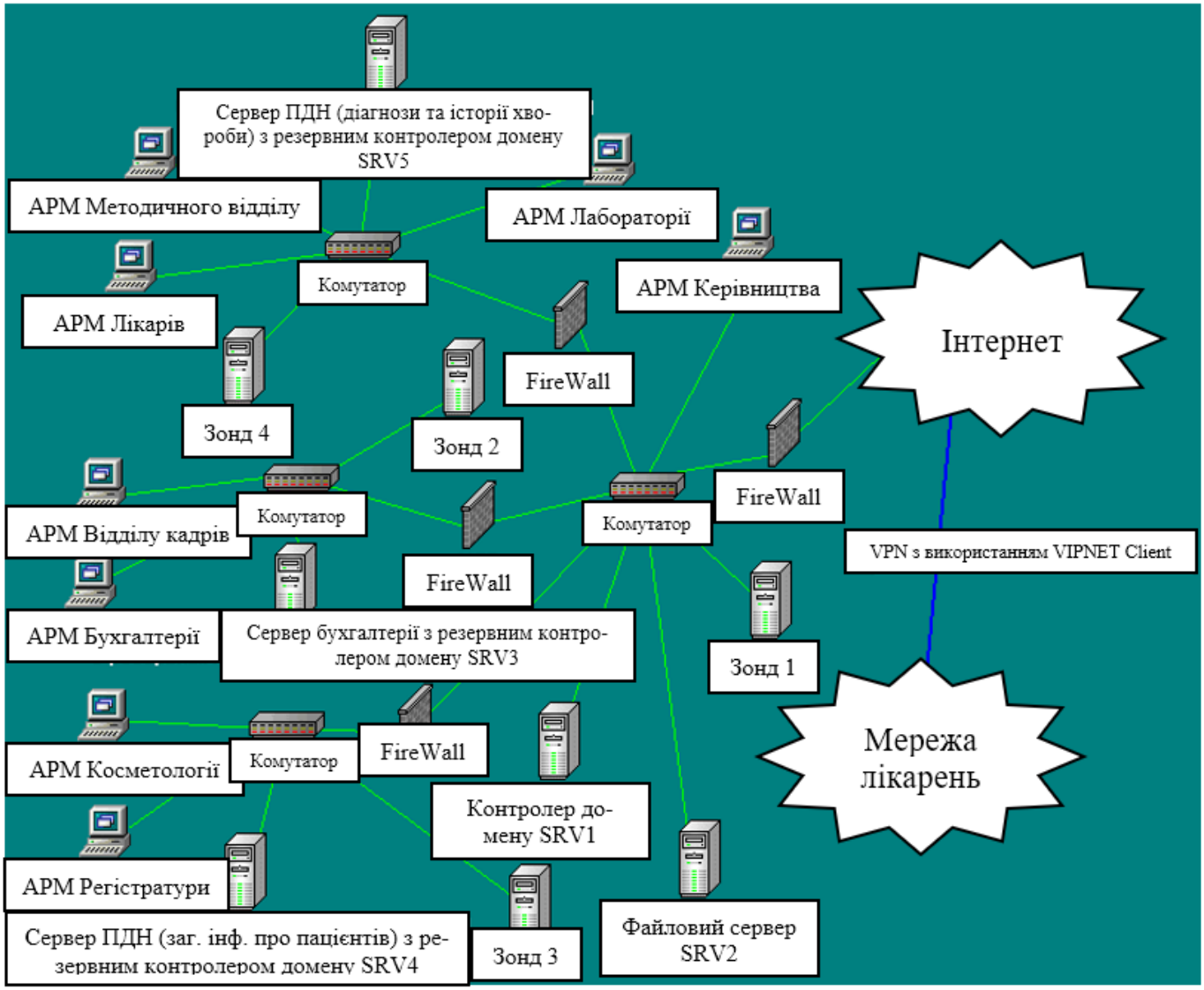

Рис. 3.1. Захищена мережа медичної установи (лікарні)

Всі індекси також беруться з каталогів SRV2. Зв'язок між таблицями встановлюється на основі "ПД + номер карти", де ПД - пункти 2-4 перераховані вище.

Бази даних бухгалтерії та відділу кадрів включають в себе весь набір інформації про співробітників, так як використовується програмне забезпечення з певною внутрішньою структурою, наприклад, «ME.Doc».

Окремо були розділені бази даних на SRV2, SRV4 і SRV5, що в кінцевому підсумку призведе до скорочення класу ІСПДН.

Спроектована мережа складається з безлічі пристроїв, які виконують різні функції для забезпечення здоров'я і безпеки мережі.

Сервери SRV2, SRV4 і SRV5 управляються операційною системою Debian

GNU/Linux 10.0. Ця операційна система заснована на ядрі Linux, є стабільною і гнучкою операційною системою, підтримує велику кількість архітектур і ліцензована під ліцензією General Public License (GPL).

MySQL 8.0 використовується в якості СУБД. MySQL має багато переваг, у тому числі:

Висока продуктивність. MySQL, безсумнівно, дуже швидкий. З результатами порівняльних експлуатаційних випробувань, проведених виробником, можна ознайомитися на сторінці http://www.mysql.com/why-mysql/benchmarks /. Багато з цих тестів бенчмаркінгу показують, що MySQL на порядок швидше, ніж конкуруючі продукти.

Низька вартість. Пакет MySQL доступний безкоштовно за ліцензією на програмне забезпечення з відкритим кодом або, якщо це необхідно для програми, Комерційна ліцензія може бути придбана за невелику суму.

Простота у використанні. Більшість сучасних баз даних використовують SQL. Установка MySQL настільки проста, що дозволяє встановити і запустити сервер за 10 хвилин.

Портативність. MySQL може використовуватися в багатьох різних системах Unix, а також в середовищах Microsoft Windows 10.

Підтримка SSL. SSL-це криптографічний протокол, який забезпечує безпечне з'єднання між клієнтом і сервером. Протокол забезпечує конфіденційність обміну даними між клієнтом і сервером з використанням TCP / IP, а для шифрування використовується асиметричний алгоритм з відкритим ключем. Шифрування з відкритим ключем використовує два ключі, і будь-який з них може бути використаний для шифрування повідомлення. Таким чином, якщо для шифрування використовується один ключ, то, відповідно, для розшифровки слід використовувати інший ключ. У такій ситуації ви можете отримувати захищені повідомлення, публікуючи відкритий ключ і зберігаючи секретний ключ в секреті.

Протокол SSL складається з двох підпротоколів: протоколу запису SSL і протоколу рукостискання. Протокол запису SSL визначає формат, який використовується для передачі даних. Протокол SSL включає в себе рукостискання з використанням протоколу запису SSL для обміну серією повідомлень між сервером і клієнтом

під час встановлення першого з'єднання. SSL вимагає, щоб сервер мав сертифікат SSL [13]. Надає канал, який має 3 основні властивості:

Посвідчення. Сервер завжди автентифікується, тоді як клієнт автентифікується на основі алгоритмів.

Чесність. Повідомлення включає в себе перевірку цілісності .

Конфіденційність каналу. Шифрування використовується після встановлення з'єднання і використовується для всіх наступних повідомлень. Підтримує 3 типи аутентифікації:

- аутентифікація обох сторін (клієнт-сервер),
- аутентифікація сервера з невідомими клієнтами
- повна анонімність.

Всякий раз, коли сервер автентифікується, канал захищений від спроби перехоплення даних між веб-сервером і браузером, але повністю анонімний сеанс, природно, вразливий для такої атаки. Анонімний сервер не може автентифікувати клієнта. Якщо сервер сертифікований, його повідомлення про сертифікацію повинно містити правильний ланцюжок сертифікації для прийнятного центру сертифікації. Простіше кажучи, сертифікований клієнт повинен надати серверу дійсний сертифікат. Кожна сторона несе відповідальність за перевірку того, що термін дії сертифіката іншої сторони ще не закінчився або не відкликаний. Основна мета процесу обміну ключами-створити секрет клієнта (pre_master_secret), який відомий тільки клієнту і серверу. Секрет (pre_master_secret) використовується для створення загального секрету (master_secret). Загальний секрет необхідний для створення повідомлення для перевірки сертифіката, ключа шифрування, секрету Mac (коду аутентифікації повідомлення) і "готового" повідомлення. Відправивши правильне "готове" повідомлення, сторони доведуть, що вони знають правильний секрет (pre_master_secret) [20].

Найбільш популярним рішенням для захисту трафіку від перехоплення є шифрування з'єднання за допомогою SSL. Крос-платформний продукт OpenSSL інтегрується в багато важливих програм, такі як СУБД MySQL, веб-сервер Apache. Для за-

безпечення сумісності (за замовчуванням OpenSSL реалізує тільки зарубіжні алгоритми шифрування Des/3DES, RC4, Blowfish, idea, AES, MD5, SHA/SHA-1, RSA, DSA та інші) та можна включити підтримку вітчизняних стандартів шифрування. У OpenSSL використання вітчизняних алгоритмів не вимагає модифікації бібліотек OpenSSL. Дистрибутив OpenSSL включає в себе приклад реалізації модулів підтримки вітчизняних алгоритмів (engine/ccgost catalog), розроблених фахівцями компанії cryptocom [13].

Для централізованої аутентифікації користувачів в мережі створюється домен з використанням Samba і Openaldap, відкритої реалізації протоколу LDAP. Samba - це програма, яка дозволяє отримувати доступ до мережевих дисків в різних операційних системах з використанням протоколу SMB/CIFS. Це клієнтська і серверна частини. Це безкоштовне програмне забезпечення, випущене під ліцензією GPL. Починаючи з третьої версії, Samba пропонує служби файлів і друку для різних клієнтів Microsoft Windows і може інтегруватися з операційною системою Windows Server або в якості основного контролера домену, або в якості резервного контролера домену, або в якості члена домену. Він також може бути частиною домену Active Directory. LDAP - це мережевий протокол клієнт-сервер для доступу до служби каталогів. Спочатку він використовувався як доповнення до X500, але також може використовуватися автономно і з іншими типами служб каталогів.

В якості брандмауера обраний брандмауер VIPNET OFFICE (представлений версіями Windows і Linux). Це сертифікований брандмауер (клас 3) з фільтрацією пакетів. У брандмауерах з фільтрацією пакетів політика доставки трафіку з однієї мережі в іншу визначається набором правил. Якщо правило явно не дозволяє певний трафік, відповідні пакети будуть відхилені або визнані недійсними брандмауером. Основними функціями є регулювання доступу користувачів до різних мережевих ресурсів, контроль IP-трафіку, що проходить через кожен мережевий інтерфейс сервера.

Основне завдання брандмауера VIPNET OFFICE - перехоплювати і фільтрувати (пропускати або блокувати) будь-які IP-пакети, що проходять через кожен інтерфейс (мережевий адаптер) сервера. Налаштування брандмауера VIPNET OFFICE Linux включає в себе вибір стандартного правила фільтрації (званого режимом безпеки) для

кожного адаптера і зміна його за допомогою додаткових фільтрів для певних протоколів, адрес і портів. Крім того, брандмауер VPNET OFFICE підтримує перетворення мережевих адрес (NAT).

Для зберігання персональних даних співробітників використовуються сервери під управлінням Windows 10 Server, сертифіковані з термінальним доступом. У ньому встановлена ME.doc. Для захисту термінальних сеансів канал шифрується за допомогою SSL.

Для виявлення мережевих атак рекомендується розгорнути систему виявлення вторгнень (NID). Вони діють на мережевому рівні відповідно до моделі OSI і відстежують встановлені з'єднання, аналізують структуру і зміст мережевих пакетів. Система NIDS аналізує весь трафік як на окремому комп'ютері, так і на виділеному сервері (шлюзі, маршрутизаторі).

Honeypot Manager використовується в якості системи виявлення вторгнень. Менеджер Honeypot моделює систему зберігання даних (СУБД Oracle або файловий сервер) за допомогою спеціальних пасток (датчиків), відстежує активність на ній і інформує про факти доступу до цих даних (рис. 3.2).

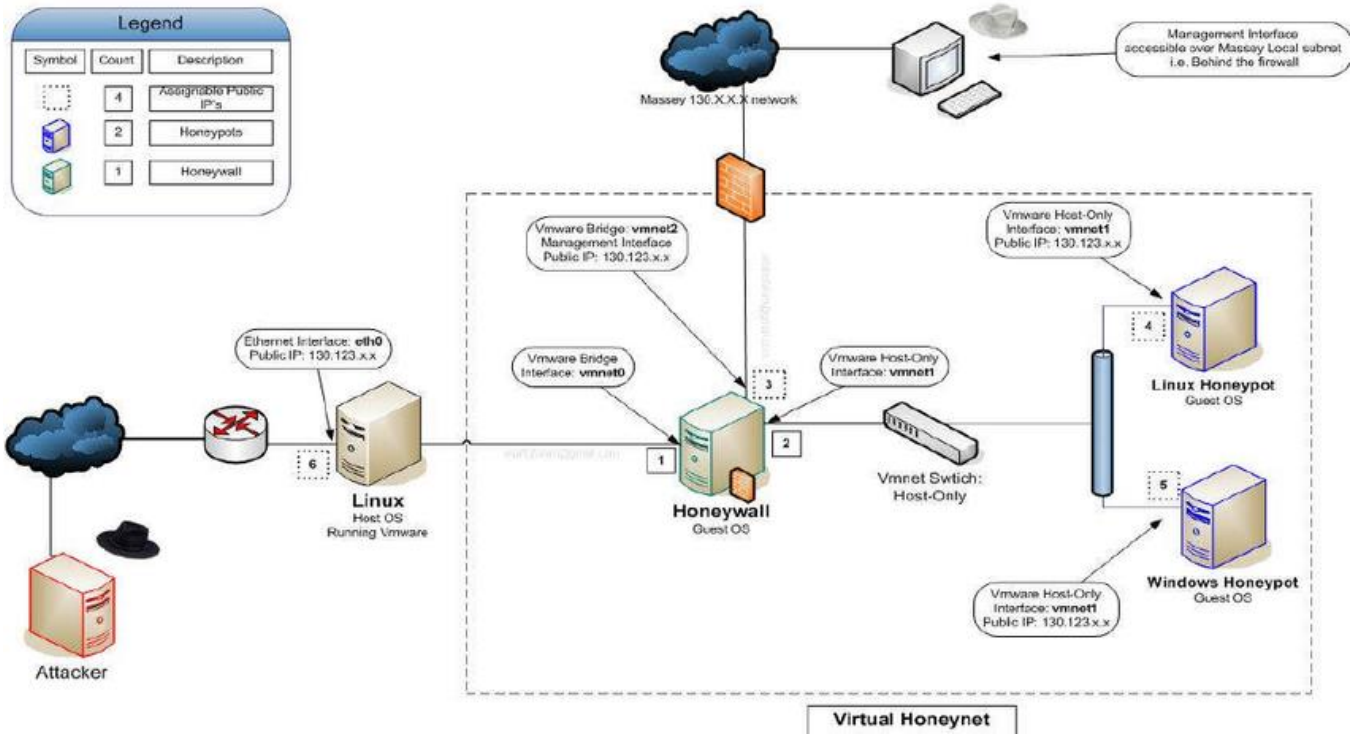

Рис. 3.2. Принцип роботи IDS Honeypot Manager

Адміністратор безпеки намагається отримати доступ до інформації про систему і в даний час може спробувати, а також визначити, чи співробітник переплутав ім'я реального сервера і випадково потрапив в пастку або навмисно діяв, і насправді в мережі є зловмисники, які намагаються знайти сервери або служби, які працюють з цінними даними для медичної установи.

Основними функціями продукту є:

- моделювання реальних систем зберігання даних;
- виявлення та реєстрація фактів НСД для даних, модельованих системою;
- інформування зацікавлених осіб про спроби НСД отримати доступ до цих даних;
- можливість відновлення системи, зміненої порушником, в початковий стан;
- підготовка звітів про роботу системи за певний час;
- централізоване управління декількома пастками (датчиками);
- авторизація та контроль доступу для управління системою;
- механізм моніторингу здоров'я (Діагностика);
- гнучка настройка правил для реагування на спроби НСД;
- створення імітаційних даних, які виглядають як реальні дані;
- періодично змінюються IP-адреси пасток (датчиків) [12].

Для підвищення надійності безпеки необхідно контролювати всю мережеву архітектуру, розміщуючи зонди (комп'ютери з NID) в кожному сегменті мережі. Ці комп'ютери не обов'язково повинні бути серверами, системи NID можуть бути встановлені на звичайних робочих станціях.

Зонд 1 розташований в максимально можливій небезпечній зоні мережі. Тут аналізується весь вхідний і вихідний трафік, і існує висока ймовірність великої кількості помилкових спрацьовувань. При підвищеному навантаженні на мережу можливо, що NID не зможе обробити весь потік трафіку і методи аналізу будуть огрублені, наприклад, за рахунок зменшення кількості сигнатур.

Зонд аналізує трафік локальної мережі 2,3,4, яка теоретично є найбезпечнішою

зоною. Кількість помилкових спрацьовувань в цій області має бути найменшою, і тому більше уваги слід приділяти повідомленням із запитами [12].

3.2. Програмні та апаратні засоби захисту ПЕОМ

Для обміну інформацією з організаціями високого рівня клієнти VIPNET будуть використовуватися для доступу до захищених мереж медичних установ. Клієнт VPNET - це програмний пакет для сімейства ОС Windows, який виконує функції VPN - клієнта, персонального екрану, клієнта захищеної поштової системи і постачальника криптографії для додатків, що використовують функцію підпису і шифрування на робочому місці користувача або на сервері.

Клієнт складається з набору взаємопов'язаних програмних модулів: [монітор] - з низькорівневим драйвером шифрування і фільтрації трафіку, він відповідає за реалізацію функцій:

Персональний брандмауер-надійно захищає робочі станції / сервери від можливих мережевих атак як з глобальних (інтернет), так і з локальних мереж. У той же час:

Захищений і відкритий трафік фільтрується по "білому " і" чорному " списками різних параметрів (IP-адреси, порти, протоколи);

Реалізований режим "стелс"(режим ініціативного підключення), який дозволяє зробити комп'ютери від відкритої мережі невидимими;

Забезпечує виявлення і блокування певних мережевих атак (елементів IDS).

Шифратор IP-трафіку-Забезпечує безпеку (конфіденційність, достовірність і цілісність) будь-якого типу трафіку (трафіку додатків, систем управління і служб ОС), переданого між будь-якими об'єктами мережі, будь то робочі станції, файлові сервери, сервери додатків.

Висока продуктивність драйвера шифрування, що підтримує сучасні багатоядерні процесори, дозволяє захистити трафік голосових і відеосервісів в мережах TCP / IP в режимі реального часу і забезпечити одночасну роботу декількох користувацьких сеансів.

Підтримує прозору роботу через статичні і динамічні пристрої маршрутизації

Nat / Pat з будь-якими методами мережевого підключення.

Чат-клієнт - дозволяє використовувати організацію чат-конференцій між службами вбудованої служби безпечного обміну повідомленнями і об'єктами захищеної мережі VPNET, на якій встановлений клієнт VPNET або координатор VPNET (Windows).

Клієнт служби обміну файлами-дозволяє обмінюватися будь-якими файлами між об'єктами захищеної мережі VPNET без установки додаткового програмного забезпечення (наприклад, FTP-сервер / клієнт) або використання функції ОС для обміну файлами в мережі.

Обмін файлами здійснюється через захищену транспортну мережу VPNET з гарантованим поширенням і "завантаженням" файлів в разі збою з'єднання. [Моніторинг додатків] - програма, що дозволяє відстежувати мережеву активність додатків і компонентів операційної системи.

При цьому можна створити "чорний" і "білий" список додатків, яким заборонена або дозволена робота в мережі, а також встановити зворотний зв'язок про мережеву активність невідомих додатків.

У більшості випадків це дозволяє запобігти несанкціонованій мережевій активності шкідливих програм, таких як троянські коні. [Business mail] - програма, що виконує функції поштового клієнта захищеної поштової служби, що працює в захищеній мережі VPNET.

Будь-який відправник кореспонденції може бути однозначно ідентифікований. Тому даний сервіс VPNET є ідеальним рішенням для внутрішньокорпоративного обміну документами та листами. MFTP - це програма, яка виконує функції обміну службовою інформацією між вузлами захищеної мережі (ключі шифрування, з'єднання вузлів, оновлення програмного забезпечення) і конвертами з діловою Поштою і конвертами обміну файлами.

Клієнт VPNET CSP має вбудований криптопровайдер, який реалізує стандартний інтерфейс Microsoft Cryptoapi 2.0 для розробників прикладних систем на базі Windows.

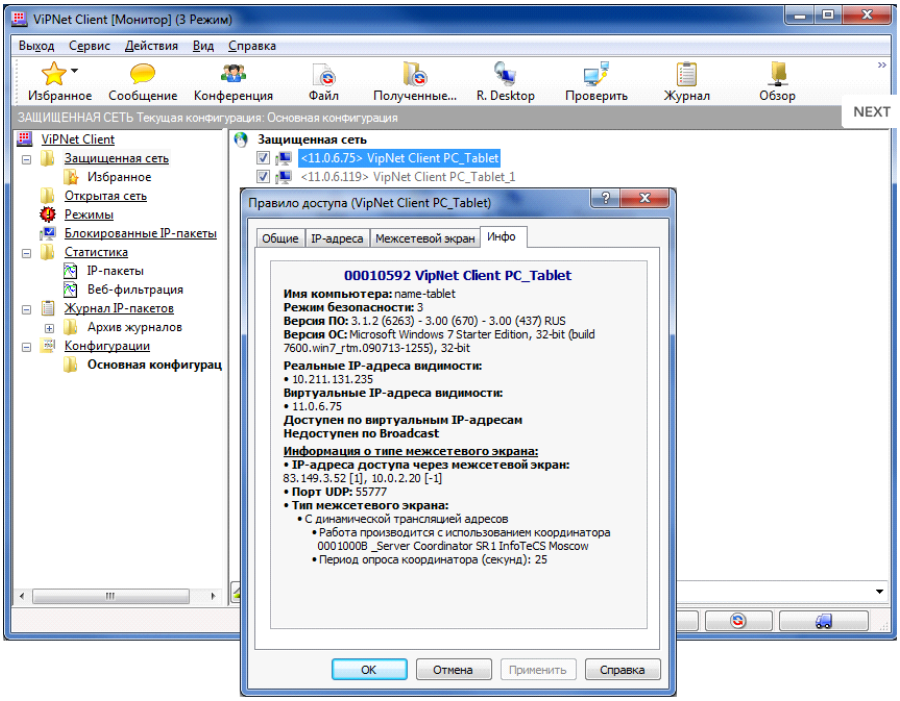

Рис. 3.3. Головне вікно VIPNET Client (приклад)

Антивірусне програмне забезпечення повинно використовуватися для захисту клієнтських комп'ютерів від вірусних атак. Вибір антивіруса був зроблений на користь ESET Internet Security 14, який, крім високої ефективності, володіє крос-платформною функціональністю і може використовуватися на комп'ютерах під управлінням як Windows, так і Linux. ESET має сертифікат Internet Security 14 і підходить для забезпечення безпеки ІСПДН.

Для контролю доступу до важливих ресурсів планується використовувати програмно-апаратну систему інформаційної безпеки "МДЗ-Ешелон".

Модуль довіреного завантаження MDZ-Echelon - це свого роду програмний інструмент для захисту від несанкціонованого доступу, який забезпечує контроль цілісності, ідентифікацію та аутентифікацію перед передачею управління операційній системі.

На відміну від звичайних апаратних і програмних модулів надійного завантаження, "MDZ-Ешелон" не схильний до атак на модифікацію BIOS.

Технічна характеристика:

Підтримка апаратних платформ сімейства Intel x64-86 з PnP BIOS "Phoenix-

Award" і " AMI " з встановленими жорсткими дисками PATA, SATA і/або SCSI і стандартами CD-ROM PATA, SATA та ін.;

Підтримка будь-якої ОС, встановленої на окремому розділі жорсткого диска: Windows, QNX, Linux, Wince з завантажувальним сектором, FreeBSD і т. д.;

Займаний обсяг жорсткого диска: близько 24 МБ;

Необхідний обсяг в мікросхемі Flash BIOS становить близько 6 КБ;

Первісна авторизація користувача перед завантаженням ОС;

Якщо авторизація пройшла успішно, вона контролює цілісність середовища, обчислюючи контрольні суми елементів файлової системи, пов'язаних з користувачем, а потім порівнюючи їх з посилальними значеннями.;

Підтримка BIOS з Rewards-Phoenix 4.5, 6.0 і amibios 7.0, 8.0 core;

Підтримка віртуальних машин VMware, Bochs, VirtualPC.

Обґрунтованість вибору цього засобу захисту наведена в таблиці 3.1.

Таблиця 3.1

Порівняння апаратних і програмних засобів забезпечення безпеки

Назва	«МДЗ-Ешелон»	АПМДЗ «КРІПТОН-ЗАМОК»	ПАК «Соболь»
Підтримувані ОС	дозволяє завантажувати будь-яку ОС, встановлену на окремий розділ жорсткого диска, включаючи МСВС і Windows (QNX, Linux, WinCE с boot-сектором, FreeBSD)	Windows 95/98/NT 4.0/2000/XP/10	Windows починаючи з 2000; FreeBSD версії 5.3, 6.2, 6.3 або 7.2; Trustverse Linux XP Desktop 2008 Secure Edition; МСВС 3.0
Підтримка файлових систем	NTFS, exFAT, FAT 32, FAT 16, UFS, EXT3, EXT2	FAT12, FAT16, FAT32 і NTFS	NTFS, FAT 32, FAT 16, UFS, EXT3, EXT2

3.3 Базова політика безпеки

На основі характеристик мережевих пристроїв, програмного та апаратного забезпечення, функцій безпеки і теоретичних даних створюється загальна політика безпеки для мережевих адміністраторів і користувачів.

Елементи управління політикою безпеки:

- порядок доступу до конфіденційної інформації (персональних даних);
- робота з криптографічними системами;
- фізична безпека (доступ в приміщення);
- диференціація прав доступу;
- робота в Інтернеті;
- дублювання, надмірність і роздільне зберігання конфіденційної інформації [15].

Процес доступу до конфіденційної інформації.

- Для забезпечення безпеки інформації в медичному закладі встановлюється наступний порядок допуску до роботи з конфіденційними джерелами:
- Рішення про доступ працівника до певного розділу конфіденційної інформації приймається керівництвом медичного закладу.
- Відповідальні особи з числа штатних програмістів забезпечують захист від читання, видалення, копіювання особистих файлів і програм особами, яким це не дозволено.
- Доступ в комп'ютерну мережу медичного закладу здійснюється тільки з персональним паролем. Користувач повинен зберігати свій пароль в секреті. Забороняється розкривати свої паролі іншим особам, а також використовувати чужі паролі. Ім'я користувача та пароль для входу в базу даних з ПДН повинні відрізнятися від імені користувача та пароля для загальної комп'ютерної мережі медичного закладу.
- Категорично забороняється робити несанкціоновані копії носіїв інформації.

Робота з криптографічними системами.

- До роботи з криптографічними системами допускаються тільки співробітники банку, які мають відповідний дозвіл керівництва медичної установи.
- Цифрові підписи і секретні ключі шифрування повинні зберігатися в сейфах під відповідальністю уповноважених осіб. Доступ сторонніх осіб до носіїв секретних ключів і шифрування повинен бути виключений.

Заборонено:

- Відображення секретних ключів і шифрування на дисплеї комп'ютера або принтері.
- Встановлення секретних ключів і носіїв шифрування на дисковод комп'ютера в непередбачуваних режимах роботи.
- Записувати зовнішню інформацію на носій секретного ключа і шифрування.

Якщо секретні ключі, шифрування та інша електронна інформація скомпрометовані, відповідальні особи вживають заходів для запобігання будь-яких операцій з використанням цих ключів та іншої інформації; вживаються заходи для зміни ключа і шифрування, пароля. За фактом угоди проводиться службове розслідування, результати якого відображаються в акті і доводяться до відома керівництва медичного закладу.

Фізичний захист.

Інформаційна безпека (всі сервери баз даних, телефонна станція, головний маршрутизатор, брандмауер) з точки зору важливих об'єктів розташовані в різних приміщеннях, доступ до яких надається тільки тим співробітникам, у яких керівництво медичного закладу дозволило мати відповідний дозвіл.

Вхід в приміщення здійснюється через металеві двері, обладнані замками (не менше двох).

Приміщення обладнане системою примусової вентиляції та пожежної сигналізації. Вхід в приміщення контролюється системою відеоспостереження з доступом до моніторів безпеки.

Дискети з ключами, паролі та інша конфіденційна інформація зберігаються в сейфах.

Доступ в приміщення сторонніх осіб заборонений. Технічний персонал займається прибиранням приміщень, ремонтом обладнання, обслуговуванням кондиціонерів і т.д. приміщення може перебувати тільки в присутності співробітників, які мають право перебувати в приміщенні у зв'язку з виконанням своїх службових обов'язків.

Доступ до приміщення в нерегулярний час або у вихідні та святкові дні здійснюється з письмового дозволу головного лікаря медичного закладу або його заступників.

Розмежування прав доступу до програмного забезпечення та систем зберігання даних.

Для входу в комп'ютерну мережу медичного закладу співробітник повинен ввести ім'я та пароль. Вільний від пароля (гостьовий) доступ до будь-якої інформації не допускається.

Для захисту конфіденційної інформації підрозділи охорони здоров'я, які мають доступ і працюють з різною інформацією (з точки зору її конфіденційності та смислової спрямованості), відрізняються організаційно і технічно. Це завдання вирішується за допомогою мережевої операційної системи, де для забезпечення безпеки даних обмежений доступ до окремих каталогів і прав користувачів. Права розподіляються відповідно до виробничої вимоги, яка визначається керівником відділу.

Параметри входу в мережу, ім'я та пароль, не розкриваються Користувачем. Друковані копії зберігаються в недоступному для сторонніх місці. Якщо пароль скомпрометований, користувач повинен негайно зв'язатися з програмістом з проханням про заміну.

Робота в Інтернеті.

До роботи з ресурсами Інтернету та електронної пошти допускаються співробітники, які отримали відповідний дозвіл від керівництва медичного закладу (досить усної форми).

При роботі з Інтернетом співробітникам забороняється:

- завантаження та встановлення програмного забезпечення на комп'ютер;

- відвідувати ресурси, які не мають прямого відношення до роботи і службових обов'язків;
- підписка на розсилку невиробничої інформації;
- повідомлення адреси електронної пошти для невиробничих цілей;
- використання різних інтернет-месенджерів;
- використання Інтернету для отримання матеріальної вигоди або в невиробничих цілях, включаючи торгівлю через Інтернет;
- дублювання, надмірність і роздільне зберігання конфіденційної інформації.

Щоб захистити конфіденційну інформацію від навмисного або ненавмисного знищення, фальсифікації або розголошення, обов'язково:

- Щоденне обов'язкове резервне копіювання всієї інформації конфіденційного характеру.
- Дублювання інформації з використанням різних фізичних і апаратних носіїв.

Відповідальність за зберігання і зберігання інформації в електронному вигляді повинна бути покладена на штатних програмістів.

Таким чином, в даному розділі були розглянуті заходи щодо створення захищеної локальної мережі медичного закладу, а також запропоновані програмні та апаратні засоби забезпечення безпеки. Також була запропонована Базова політика безпеки для захисту від доступу НСД до критичних ресурсів.

ВИСНОВКИ

Під час написання дипломної роботи були розглянуті основні нормативні документи, які контролюють правові відносини у сфері захисту персональних даних, надання інформації про потенційні загрози для захисту інформаційної системи окремих персональних даних. При розгляді загроз, особливу увагу було приділено класифікації порушення безпеки, оскільки вони відіграють важливу роль для організації захисту інформаційної системи.

Особлива увага приділяється основним компонентам для створення захищеної інформаційної системи. Організація зберігання персональних даних у базі даних, класифікація програмного та апаратного забезпечення. Загальний обіг персональних даних у інформаційній системі отримав особливу увагу, яка відображається у вигляді структури локально-обчислювальної мережі медичного закладу.

Заходи щодо створення захищеної локальної мережі медичного інституту, згідно з якою інформація, пов'язана з персональними даними користувачів і клієнтів передається по захищених каналах, що забезпечується програмним та апаратним забезпеченням. Було також запропоновано основну політику безпеки в медичній установі щодо захисту від несанкціонованого доступу до важливих ресурсів.

СПИСОК ВИКОРИСТАНИХ ДЖЕРЕЛ

1. Методические рекомендации для организации защиты информации при обработке персональных данных в учреждениях здравоохранения, социальной сферы, труда и занятости. М., 2019.
2. В.Ф. Шаньгин - Информационная безопасность компьютерных систем и сетей, М., ИД «ФОРУМ» - ИНФРА-М, 2018 г.
3. Хомоненко А.Д., Цыганков В.М., Мальцев М.Г. Базы данных; Учебник для высших учебных заведений / Под ред. проф. А.Д. Хомоненко. - 4-е изд., доп. и перераб. - СПб.: КОРОНА принт, 2014. - 736 с. ISBN 5-7931-0284-1.
4. Ржавский К.В. Информационная безопасность: практическая защита информационных технологий и телекоммуникационных систем: Учебное пособие. Волгоград: Изд-во ВолГУ, 2012. - 122с. - (Серия «Информационная безопасность»). ISBN 5-85534-640-4.
5. Гагарина Л.Г., Кокорева Е.В., Виснадул Б.Д. Технология разработки программного обеспечения. - М.: ИД «ФОРУМ»; ИНФРА-М, 2008. - ISBN 978-5-8199-0342-1.
6. Щербаков А.Ю. Современная компьютерная безопасность. Теоретические основы. Практические аспекты. - М.: Книжный мир, 2019. - 352 с. - ISBN 978-5-8041-0378-2.
7. Ярочкин В.И. Информационная безопасность: Учебник для студентов вузов. - М.: Академический Проект; Гаудеамус, 2-е изд.- 2014. - 544 с. ISBN 5-8291-0408-3.
8. Скляров Д.В. Искусство защиты и взлома информации. - СПб.: БХВ-Петербург, 2014. - 288 с: ил. ISBN 5-94157-331-6.
9. Э. Мэйволд - Безопасность сетей [Электронный ресурс] - Режим доступа: http://www.intuit.ru/department/security/netsec/11/1.html
10. Информационный бюллетень Jet Info №5 (192)/2019.
11. Братищенко В.В. Проектирование информационных систем. - Иркутск:

Изд-во БГУЭП, 2014. - 84 с.

12. Обнаружение сетевых атак [Электронный ресурс] - Режим доступа: http://www.osp.ru/pcworld/2013/06/165957/

13. Введение в SSL [Электронный ресурс] - Режим доступа: https://developer.mozilla.org/en/Introduction_to_SSL

14. Защита информации в Интернет [Электронный ресурс] - Режим доступа: http://www.cryptocom.ru/articles/internet_sec.html

15. Хорев А.А. Способы и средства зашиты информации. - М, 2010. - 316 с.