УДК 681.3

ЗАХИСТ КОНФІДЕНЦІЙНОЇ ІНФОРМАЦІЇ В СИСТЕМАХ ТЕЛЕМЕДИЦИНИ

Микола Грайворонський
Фізико-технічний інститут Національного технічного університету України "КПІ"

Анотація: **В контексті захисту оброблюваної інформації розглядаються системи телемедицини (надання послуг у галузі охорони здоров'я через телекомунікації). Обґрунтовується необхідність впровадження засобів захисту, досліджуються ймовірні загрози, пропонуються адекватні методи захисту. Особлива увага приділяється технології VPN для захисту інформації, що передається у глобальній мережі.**
Summary: **Telemedicine systems (providing health care services via telecommunication) are considered from the standpoint of information security. The necessity of additional measures of information protection is grounded, possible threats are studied, adequate methods of protection are proposed. Special attention is payed to VPN technology.**
Ключові слова: **Телемедицина, захист інформації, конфіденційність, загрози, VPN.**

I Вступ

Згідно з визначенням, телемедициною називають надання послуг у ґалузі охорони здоров'я через телекомунікації. Здебільшого надаються інтерактивні консультативні та діагностичні послуги. Типовими сервісами, задіяними в телемедицині, є електронна пошта, обмін файлами визначених форматів, доступ до інформаційних ресурсів (файлів, баз даних, Web-сторінок) через глобальну мережу, а також телеконференції.

Як приклад можна розглянути такі типові сценарії застосування телемедицини.

1 Пацієнт направляється лікарем (терапевтом) на консультацію до спеціаліста. Інформація про пацієнта зберігається лікарем у файлі, доступ до якого через мережу має спеціаліст. Висновки і рекомендації спеціаліста надсилаються через мережу терапевту. Коли терапевт або спеціаліст виписують пацієнту рецепт, останній одночасно надходить через мережу фармацевту.

2 Фармацевт отримує через мережу рецепти від різних лікарів. Він має повну інформацію про ліки, що прописані кожному пацієнту, і може перевірити їх на сумісність і відсутність побічних явищ. У складних ситуаціях він може звертатись до централізованої бази данних щодо застосування комбінацій різних ліків.

3 У разі необхідності (важкий або нетиповий випадок, віддаленість від медичного центру) надається телеконсультація спеціаліста. Найчастіше телеконсультації проводяться між лікарями, рідше – між пацієнтом і лікарем. Необхідною складовою телеконсультації є можливість обміну повідомленнями (запитання – відповіді) і файлами різних форматів (наприклад, результати аналізів або рентгенівські знімки). Така консультація може здійснюватись із застосуванням відеоконференції в реальному часі. Хоча одночасне застосування трансляції звуку, відеозображення і пересилання файлів є найефектнішою демонстрацією можливостей сучасних інформаційних технологій, насправді асинхронні комунікації (обмін файлами і електроною поштою) є найбільш ефективними і економічно виправданими.

В усіх розглянутих нами випадках має місце передача через мережу інформації, яка носить конфіденційний характер, оскільки містить персональні дані певної особи (пацієнта), а в деяких випадках має для останнього життєво важливе значення. Таким чином очевидно, що будь-яке використання телемедицини повинно відбуватись із застосуванням достатніх заходів із захисту інформації.

На жаль, у сучасних реалізацій систем телемедицини, як і багатьох інших інформаційно-телекомунікаційних систем, спостерігаються суттєві вади захищеності оброблюваної інформації. Причини цього полягають, зокрема, у тому, що послуги захисту інформації розглядаються окремо від телекомунікаційних послуг. Як правило, фахівці з інтеграції інформаційно-телекомунікаційних систем, розробники програмного забезпечення і апаратних засобів і навіть адміністратори систем розглядають послуги безпеки як вторинні, додаткові і навіть як перешкоду нормальному функціонуванню системи. З іншого боку, фахівці із захисту інформації мають тенденцію ставити завищені вимоги до обладнання, програмного забезпечення, організаційних заходів, реалізації системи в цілому, що є наслідком досвіду у забезпеченні захисту державної таємниці, але не є адекватними вимогами до комерційних систем, в яких обробляється інформація, що не є власністю держави.

Таким чином, необхідний системний підхід до проектування систем телемедицини. Останні мають забезпечувати комплекс послуг, невід'ємною частиною якого є послуги безпеки, що гарантують достатній захист оброблюваної інформації відповідно до вимог власника інформації. В цій роботі розглядаються і

обґрунтовуються типові загрози і вимоги до захищеності інформації в системах телемедицини, а також пропонуються рішення, здатні задовольнити зазначені вимоги.

II Аналіз задач захисту інформації в телемедицині
Типова архітектура системи телемедицини

Як було зазначено вище, призначення будь-якої системи телемедицини – організація взаємодії віддалених користувачів, що здебільшого передбачає використання глобальних мереж. Система телемедицини може включати досить розвинену центральну підсистему – локальну мережу лікувального закладу або дослідного інституту, яка крім робочих станцій включає сервери і сховища даних. Але головною ознакою такої системи є наявність віддалених підключень через глобальну мережу. Такі підключення можуть бути симетричними (взаємодія двох підсистем одного масштабу), або асиметричними. В останньому випадку віддалений доступ можуть отримувати або підсистеми, які умовно можна назвати регіональними (в англомовній літературі їм відповідає термін ROBO – Regional office/Branch office), які мають масштаб суттєво менший, ніж центральна підсистема, або зовсім маленькі локальні мережі й навіть окремі користувачі (яким в англомовній літературі відповідає термін SOHO – Small office/Home office).

Симетричні системи можуть використовувати мережі Frame Relay, ISDN або ATM, але з міркувань економічної ефективності найчастіше використовується Internet, який характеризується відносно низькою якістю послуг і їх найнижчою вартістю. Асиметричні системи практично завжди використовують Internet, особливо у випадку підсистем класу SOHO. На рис. 1 наведена можлива архітектура асиметричної системи телемедицини, яка включає як регіональні підсистеми, так і окремих користувачів – так званих телеробітників, якими можуть бути окремі медичні пункти, аптеки, лікарі, що використовують мобільний доступ до Internet.

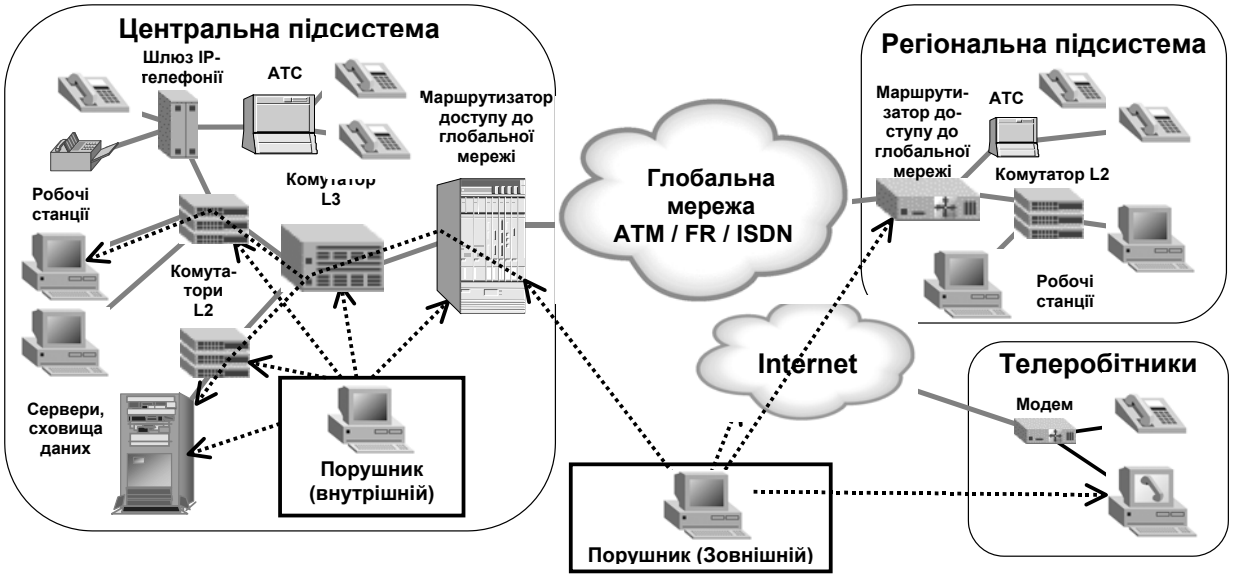

Рисунок 1 – Приклад архітектури системи телемедицини з демонстрацією вузлів, найбільш вразливих до дій порушників

Побудова моделі загроз і оцінка ризиків

Джерелом загроз безпеці інформації у телемедицині можуть бути зміни зовнішнього середовища (стихійні лиха і аварії: землетрус, повінь, пожежа або інші випадкові події), збої та відмови обладнання, наслідки помилок під час проектування і розробки системи, а також дії персоналу і зовнішніх порушників.

Метою реалізації загроз може бути порушення конфіденційності, цілісності та доступність інформації.

Конфіденційність зберігається тоді, коли ознайомитись з інформацією можуть лише авторизовані особи. Значення цієї властивості інформації для застосувань телемедицини є очевидним і базується на тому факті, що медична інформація є приватною. Розголошення такої інформації є порушенням її конфіденційності (приватності). Загроза розголошення інформації є вкрай актуальною для розподілених інформаційних систем, до яких належать і системи телемедицини. Найтиповішими шляхами реалізації цієї

загрози в розподілених системах є прослуховування каналів зв'язку ("sniffing") і підміна авторизованого об'єкта. Також порушники можуть атакувати кінцеві вузли системи – файлові сервери, сервери баз даних, а також робочі станції користувачів.

Цілісність зберігається тоді, коли лише авторизовані особи можуть будь-яким чином модифікувати інформацію. Ймовірними загрозами цілісності є часткова або повна втрата даних, а також цілеспрямована фальсифікація. Перша загроза є значно ймовірнішою і типовою для будь-яких інформаційних систем, вона може реалізовуватись як внаслідок відмов і збоїв обладнання, так і внаслідок необережних чи з умисних дій користувачів, в тому числі через дію комп'ютерних вірусів та іншого шкідливого програмного забезпечення. Друга загроза в системах телемедицини не настільки ймовірна, але вона може мати дуже значні наслідки (наприклад, можлива фальсифікація відомостей про стан здоров'я особи, підміна рецептури або дозування ліків).

Доступність означає, що будь-який авторизований об'єкт може отримати інформацію протягом визначеного (малого) інтервалу часу. Типова загроза доступності – це так звана відмова в обслуговуванні (denial of service, DoS), дуже поширена проблема в розподілених інформаційних системах. Загроза може реалізовуватись через DoS-атаки, спрямовані як на кінцеві вузли у телекомунікаційній системі, так і на проміжні вузли (маршрутизатори). Також порушення доступності інформації може відбуватись внаслідок відмов і збоїв обладнання, що особливо актуально для систем віддаленого доступу, а також через пошкодження каналів зв'язку. Для систем телемедицини такі загрози слід вважати більш актуальними, ніж для більшості інших інформаційно-телекомунікаційних систем, що використовують технології віддаленого доступу, оскільки застосування телемедицини найчастіше потрібно у віддалених регіонах з недостатньо розвинутою телекомунікаційною інфраструктурою, а також у зонах стихійного лиха чи регіональних конфліктів.

Таким чином, можна виділити такі головні ризики в системі телемедицини:

- реалізація випадкових загроз (цілісність, доступність), пов'язаних із збоями і відмовами обладнання, пошкодженням каналів зв'язку, некомпетентними діями користувачів;
- умисне порушення цілісності або доступності інформації внаслідок дій зловмисників (терористи, вандали);
- порушення конфіденційності інформації на кінцевих вузлах;
- порушення конфіденційності та цілісності інформації під час передачі її мережею.

Розраховуючи прийнятні затрати на впровадження і підтримання заходів захисту з міркувань економічної ефективності, слід враховувати, що для сторонніх осіб цінність інформації, що може оброблятись у системі телемедицини, суттєво залежить від соціального статусу пацієнта. Наприклад, відомості про політичного діяча чи популярного артиста можуть бути об'єктом продажу, тому активність і задіяні ресурси порушників щодо здобуття таких відомостей можуть бути дуже високими.

III Методи захисту інформації в телемедицині

Виходячи з визначених ризиків, розглянемо можливі рішення щодо надання послуг захисту інформації в системі телемедицини.

Захист від реалізації випадкових загроз

Оскільки ця проблема є типовою для всіх інформаційно-телекомунікаційних систем, слід застосовувати стандартні технічні рішення з захисту інформації. Основними методами захисту є застосування надлишковості ресурсів і даних як в системах зберігання даних, так і в системах телекомунікації, резервне копіювання, антивірусний захист. Захисту від некомпетентних дій користувачів під час розробки системи слід приділити особливу увагу, оскільки система телемедицини орієнтована на її застосування людьми, які не є фахівцями у використанні комп'ютерів. Проектні рішення повинні враховувати простоту і однозначність інтерфейсу користувача, автоматичність і прозорість всіх операцій, спрямованих на захист інформації, таких як резервне копіювання або виявлення і видалення комп'ютерних вірусів і іншого шкідливого програмного забезпечення.

Захист від умисного порушення цілісності або доступності інформації

Частково ця проблема вирішується тими ж засобами, що й захист від реалізації випадкових загроз. Так, резервне копіювання дозволить швидко відновити інформацію в разі її умисного знищення, антивірусний захист ускладнить впровадження віруса або "троянського коня".

Ефективним захистом від дій зловмисників через мережу є використання приватної телекомунікаційної мережі. Але цей метод занадто дорогий, і тому на практиці застосовується рідко, для систем телемедицини його слід вважати практично неприйнятним.

Для запобігання типовим атакам з глобальної мережі ефективним захистом є мережеві екрани (брандмауери). Для центральної та регіональних підсистем необхідно застосовувати міжмережеві екрани,

причому, виходячи зі специфіки системи телемедицини, є сенс впроваджувати брандмауери прикладного рівня. На робочих станціях користувачів, що користуються послугами віддаленого доступу, мають бути встановлені персональні брандмауери. Застосування систем виявлення атак у системах телемедицини є достатньо ефективним в тому випадку, коли ці системи здатні здійснювати автоматичне реагування на виявлену атаку (наприклад, знищення будь-яких пакетів, що надходять від порушника, шляхом додавання динамічних правил на брандмауері).

Для запобігання діям внутрішніх порушників (тобто таких, які є користувачами системи і здатні здійснювати доступ з локальної мережі) необхідно впроваджувати не тільки стандартні засоби захисту, але й ефективні організаційно-адміністративні заходи. Слід зазначити, що абсолютно необхідним є застосування надійної схеми автентифікації користувачів, щоби запобігти можливості будь-яких дій порушників від імені легального користувача. Особливо це стосується комп'ютерів телеробітників, потенційно найменш захищених елементів системи телемедицини.

Виходячи із специфіки користувачів систем телемедицини, слід забезпечувати максимальну прозорість функціонування системи автентифікації, тому парольний захист слід вважати найменш прийнятним, оскільки можна прогнозувати намагання користувачів або взагалі відмовитись від використання паролів, або застосовувати найпростіші і ненадійні паролі, або зберігати записані паролі у легкодоступному місці. Значно ефективнішим буде використання носимих атрибутів (смарт-карт) або автентифікаці за біометричними ознаками.

Захист від порушення конфіденційності інформації на кінцевих вузлах

Засоби захисту від дій зовнішніх порушників в цілому аналогічні засобам захисту від умисного порушення цілісності або доступності інформації. Ефективність захисту від дій внутрішніх порушників залежить від повноважень останніх, а також від ефективності організаційно-адміністративних заходів. У багатьох випадках у системі телемедицини прийнятним є забезпечення неможливості копіювання інформації (в тому числі легальним користувачем) на зовнішні носії, але це практично неможливо забезпечити для телеробітників. Таким чином, головним методом стає підтримання ефективних заходів по роботі з персоналом і недопущення сторонніх осіб до роботи із системою. Фактично, рішення щодо захисту конфіденційності інформації в системі телемедицини повинні прийматись ще на попередній стадії розробки проекту такої системи, під час визначення функцій системи і послуг, що вона надає. Саме з міркувань захисту конфіденційності інформації не слід занадто поширювати перелік послуг, що надає така система.

Захист від порушення конфіденційності та цілісності інформації під час передачі її мережею

Для захисту інформації в розподілених системах можуть застосовуватись такі методи, як зашифровування даних, автентифікація об'єктів мережевої взаємодії, керування маршрутом, використання електронного підпису тощо. З наведених вище міркувань створення приватної мережі передачі даних тут не розглядається. В публічних мережах, зокрема, в Internet, може застосовуватись технологія, яка включає комбінацію наведених вище методів, що отримала назву "віртуальна приватна (захищена) мережа" (VPN).

Типовий набір обладнання для організації VPN включає маршрутизатори доступу до глобальної мережі, брандмауери, а також специфічні пристрої, що реалізують криптографічний протокол, з використанням якого утворюються приватні віртуальні тунелі у публічній мережі (рис. 2).

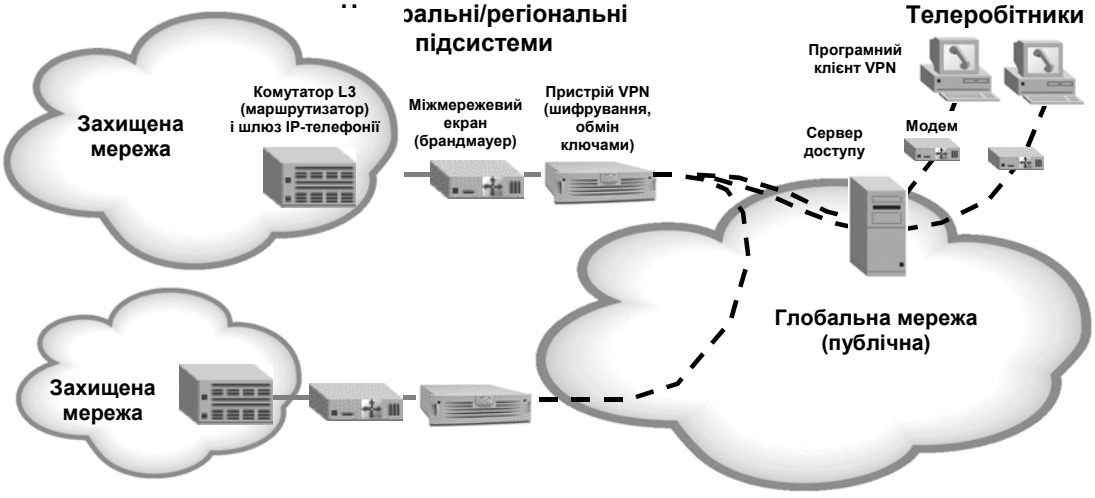

Рисунок 2 – Реалізація VPN в системі телемедицини з організацією віддаленого доступу

Провідні виробники мережевого обладнання пропонують так звані рішення “все в одному”, коли в одному пристрої реалізуються всі зазначені вище функції. Як приклад можна навести лінійку Contivity компанії Nortel Networks, до складу якої входять пристрої, що розрізняються продуктивністю, кількістю одночасно підтримуваних з’єднань (віртуальних тунелів), наявністю і кількістю слотів для модулів розширення, в тому числі для апаратних модулів шифрування, кількістю і номенклатурою портів локальних і територіальних мереж. Таким чином, існують пристрої, оптимальні для будь-якого масштабу центральної і регіональних підсистем системи телемедицини. Для телеробітників призначений програмний клієнт, який функціонує під керуванням операційних систем Windows, і забезпечує захищений зв’язок з пристроєм Contivity.

Для систем телемедицини, призначених для надання консультативних послуг, засобів VPN може бути достатньо. Але якщо система передбачає передачу в електронному вигляді документів на кшталт результатів аналізів, рецептів, медичних висновків, тощо, необхідною складовою має бути система накладання і перевірки електронного підпису, що діє прозоро для користувачів.

IV Висновки

При проектуванні системи телемедицини мають враховуватись вимоги з захисту оброблюваної інформації, яка має бути віднесена до категорії конфіденційної.

Основні загрози, яким повинні протидіяти засоби захисту в системі телемедицини, – це порушення цілісності та доступності інформації або пошкодження системи внаслідок збоїв і відмов обладнання, пошкодження каналів зв’язку, некомпетентних дій користувачів, умисне порушення конфіденційності, цілісності або доступності інформації внаслідок дій зловмисників та порушення конфіденційності та цілісності інформації під час передачі її мережею.

Рекомендованими засобами захисту для систем телемедицини є пристрої організації VPN, міжмережеві екрани (брандмауери), пристрої виявлення атак, здатні автоматично реагувати на атаки шляхом керування брандмауерами, маршрутизаторами і комутаторами, системи автентифікації з використанням носимих атрибутів (наприклад, смарт-карт) та/або біометричних характеристик, засоби антивірусного захисту, а також стандартні засоби захисту інформаційних систем від збоїв і відмов. Для телеробітників частина зазначених засобів (брандмауери, засоби виявлення атак, клієнти VPN) реалізуються у вигляді програмних рішень, але вкрай важливою є надійна система автентифікації користувача.

Особливістю вимог систем телемедицини до реалізації засобів захисту слід визнати необхідність прозорої дії всіх або більшості засобів, простоту застосування і, з іншого боку, неможливість їх обходу як порушниками, так і легальними користувачами.