УДК: 61:651.928:681.3:003.26:681.31:007

Комплексна система захисту інформації медичної – надійний алгоритм надання якісної медичної допомоги в закладах охорони здоров'я

Шупяцький І.М.

Резюме. *Проаналізовано елементи комплексної системи захисту політики безпеки в телемедицині, запропоновані нові термінологічні положення.*

Ключові слова: *система, захист, телемедицина, криптотелемедицина, політика, елементи.*

Актуальність проблеми. У спеціальній літературі, яка сьогодні описує й пояснює особливості захисту інформації при її передачі на відстані, йдеться про комплексну систему захисту інформації (КСЗІ), яка описує такі елементи, як політика або гарантованість безпечної системи. [1]

Пропонуємо розглянути КСЗІ, як безпечну систему щодо захисту медичної інформації. Доступність, цілісність, конфіденційність – основа системи комплексу. Тобто можна керувати доступом до медичної інформації таким чином, що тільки авторизовані реципієнти або процеси, що діють від їх імені, мають право читати, писати або видаляти інформацію. Надійна система – це система, яка використовує насамперед апаратні та програмні засоби для забезпечення одночасної обробки медичної інформації різного ступеня секретності групою користувачів без порушень прав доступу. Надійність системи – це політика безпеки і гарантованості.

Політика безпеки являє комплекс законів, правил і норм, які забезпе-чують дисципліну обробки, захисту й розповсюдження медичної інформації. Політика безпеки обумовлює вибір конкретних механізмів, забезпечуючи безпеку системи, і є активним компонентом захисту медичної інформації, включаючи аналіз можливих загроз і вибір заходів протидії.

Гарантованість – це рівень довіри, який може бути наданий конкретній реалізації системи. Гарантованість висвітлює ступінь коректності механізмів, що забезпечують безпеку. Гарантованість можна вважати пасивним компонентом захисту, яка наглядає за механізмами забезпечення безпеки, що є необхідним при передачі медичних даних. [2,3,4]

Концепція надійної електронної бази медичної інформації є центральною при оцінюванні ступеня гарантованості надійності системи. Механізм протоколювання є важливим засобом забезпечення безпеки. Ведення протоколів медичної інформації повинно доповнюватись аудитом, тобто аналізом реєстрації медичної інформації. [5,7,8]

Політика безпеки медичних даних включає такі елементи:

довільне управління доступом до медичної інформації;

безпека повторного використання медичної інформації;

мітки (маркери) безпеки;

контрольно-дозвільне управління доступом до медичної інформації.

Довільне управління доступом до медичної інформації полягає в обмеженні доступу до об'єктів на основі обліку персональних характеристик суб'єкта або групи, до якої входить суб'єкт. Також довільне управління – це коли власник об'єкта за власним рішенням може надавати, забороняти, або обмежувати доступ інших суб'єктів до даного об'єкта. Стабільний стан прав доступу до медичної інформації при довільному управлінні описується матрицею, в рядках якої перераховані суб'єкти, а у стовпчиках – об'єкти. На перетині рядків і стовпчиків знаходяться ідентифікатори засобів доступу до медичної інформації, що допускаються

суб'єктом відносно об'єкта, наприклад, читання, запис, виконання, можливості передачі прав іншим суб'єктам. [9]

Безпека повторного використання дозволяє захиститися від випадкового або цільового отримання прихованої медичної інформації. Безпека повторного використання повинна гарантуватися для областей оперативної пам'яті (буфери з образами екрану, паролями, ключами), а також різноманітних носіїв інформації. Сучасні периферійні технічні засоби ускладнюють забезпечення безпеки повторного використання. Наприклад, апарат МРТ-принтер може буферизувати кілька сторінок документів, які залишаться в пам'яті навіть після закінчення друку. Необхідно здійснення спеціальних дій, задля «анулювання» пристрою.

Контрольно-дозвільне управління доступом реалізується з допомогою міток безпеки, асоційованих із суб'єктами та об'єктами. Мітка суб'єкта характеризує його благонадійність, мітка об'єкта – ступінь закритості наявної телемедичної інформації.

Для телемедичної галузі краще використовувати мітки таких рівнів захисту із наведених елементів:

абсолютно секретно;

секретно;

конфіденційно;

несекретно.

Призначення категорій – опис предметної області, до якої належать дані, включно дані по телемедицині. Механізм категорій дозволяє розділити інформацію, в тому числі й телемедичну, що вдосконалює безпеку системи. Так, суб'єкт не може отримати доступ до «чужих» категорій, навіть якщо він є абсолютно благонадійним.

Постановка проблеми. Гарантованість – це міра впевненості в тому, що вибраний набір засобів телемедицини, а, точніше, криптотелемедицини дозволяє реалізовувати сформульовану політику безпеки. Операційна гарантованість включає в себе аналіз:

архітектури і цілісності системи;

прихованих каналів виходу телемедичної інформації;

методів адміністрування телемедичної інформації;

технології відновлення після збоїв при передачі медичної інформації.

Архітектура системи повинна розроблятися з урахуванням сформульованих заходів безпеки або допускати принципову можливість їх добудови.

В якості загрози можна розглянути конкретну фізичну особу або подію, які являють небезпеку для ресурсів, що призводить до порушення їх конфіденційності, цілісності, доступності та законного використання.

Загрози можна поділити на цільові (вхід зі сторони хакера) і випадкові (адресна помилка під час пересилки при збої системи).

Цільові загрози поділяються на пасивні й активні. Пасивні загрози – це несанкціоноване зчитування медичної інформації, не пов'язане зі зміною медичної інформації. Активні загрози – це отримання і зміна (заміна) медичної інформації. Загрози ще класифікуються як фундаментальні, первинні, ініціюючі і базові загрози.

До фундаментальних загроз відносять такі:

1. Витік інформації. Розкриття телемедичної інформації неавторизованому користувачу або процесу.

2. Порушення цілісності. Компрометація домовленості (непротиріччя) даних шляхом цілеспрямованого складання, заміни і ліквідації даних.

3. Відмова в послузі. Безпосереднє блокування легального доступу до медичної інформації або інших телемедичних ресурсів (наприклад, з допомогою перевантаження потоком запитів).

4. Незаконне використання. Використання телемедичних ресурсів незаконним засобом. Використання телемедичних ресурсів неавторизованим об'єктом або суб'єктом. Наприклад, використання віддаленого комп'ютера з метою «зламу» інших комп'ютерів мережі.

5. Маскарад. Користувач телемедичної інформації (або процес, підсистема) маскується і пробує видавати себе за іншого користувача. Така загроза, як правило, пов'язана зі спробою внутрішнього проникнення до периметру безпеки і досить часто реалізується хакерами.

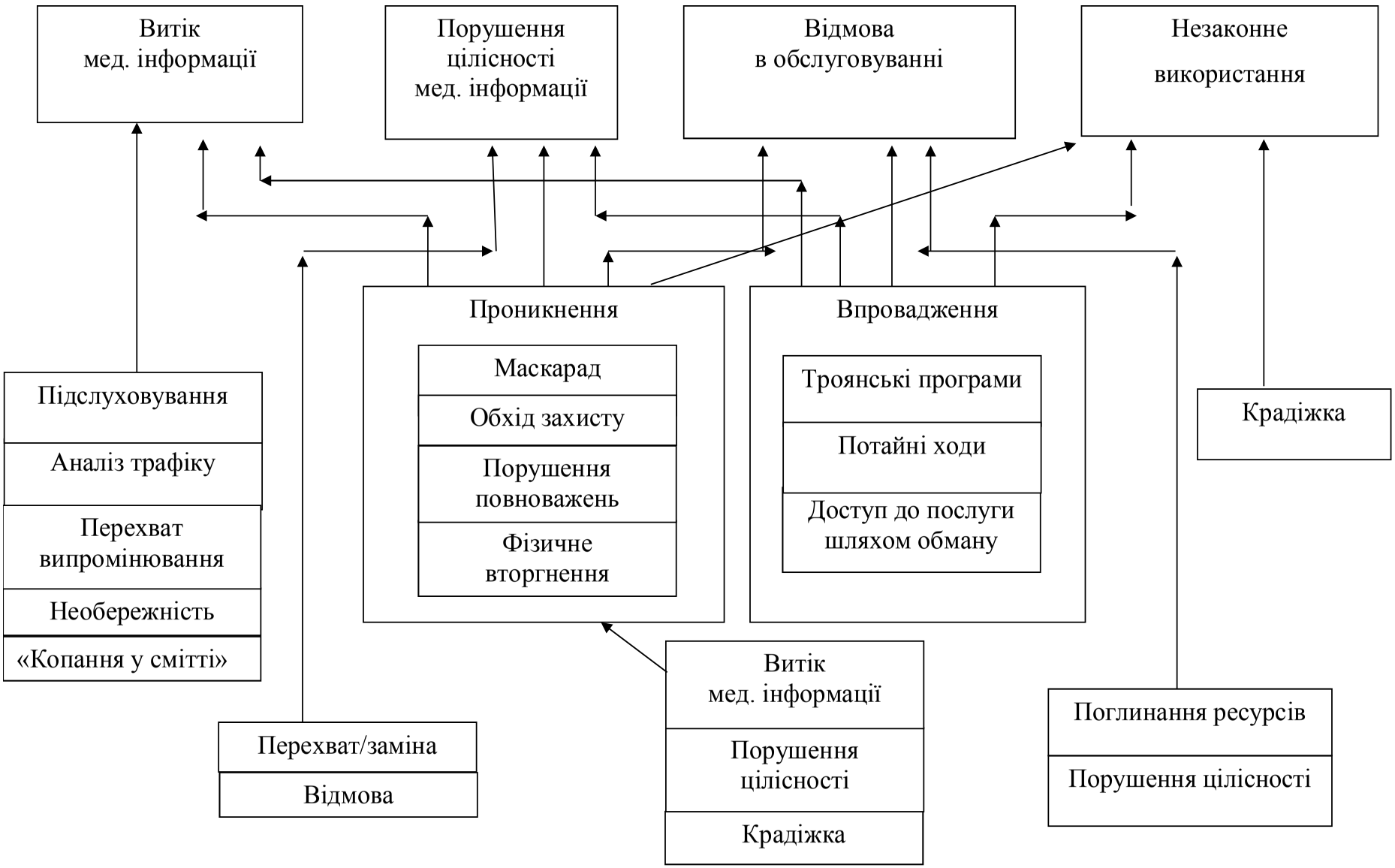

Рис. 1. Взаємозв’язок різноманітних видів загроз

6. Обхід захисту. Використання слабких місць системи для обходу захисних механізмів з метою отримання законних прав і привілеїв щодо використання телемедичних даних.

7. Порушення можливостей. Використання телемедичних ресурсів не за призначенням. Ця загроза пов'язана з діями внутрішнього порушника.

До загроз впровадження відносяться такі:

1. Троянські програми. Програми, що включають прихований або явний програмний хід, при виконанні якого порушується функціонування системи безпеки. Приклад троянської програми – текстовий редактор, який, крім простих функцій редагування, виконує приховане копіювання відредагованої медичної документації до файлу хакера.

2. Приховані ходи. Деякі додаткові можливості тайно впроваджені в систему або її компоненти, порушуючи функціонування систем безпеки при введенні специфічної медичної інформації або інших даних. Наприклад, підсистема login може нехтувати запит і перевірку пароля при введенні безпосереднього імені користувача.

Розглядаючи *фундаментальні загрози*, необхідно враховувати також *базові загрози*. Наприклад, витік телемедичної інформації пов'язаний з такими базовими загрозами, як: підслуховування; аналіз трафіку; персональна необережність; «копання у смітті».

Взаємоз'вязок може бути досить складним. Так, маскарад є загрозою, що ініціює фундаментальні загрози, в тому числі й витік інформації. Однак маскарад сам по собі може залежати і від витоку інформації. Наприклад, розкриття пароля може ініціювати загрозу маскараду.

Аналіз більш ніж трьох тисяч комп'ютерних злочинів показав, що частіше за все виникають такі загрози: порушення прав; маскарад; обхід захисту; троянські програми або потайні ходи; «копання у смітті».

Відомо, що в мережевому вірусі Internet Worn була реалізована комбінація обходу захисту і маскараду. Для обходу захисту розробники вірусу користувались слабкими місцями в системі безпеки ОС Berkley UNUX, а маскарад був реалізований шляхом відгадування паролів з допомогою спеціальної процедури.

Висновки

КСЗІ в медицині – це доступність, цілісність, конфіденційність, яка впливає на якість і своєчасність надання медичної допомоги в закладах охорони здоров'я.

Телемедицина – технічний розділ медичної науки і практики, пов'язаний з передачею медичної зорової інформації (рухливих і нерухливих зображень) на відстань радіоелектронними засобами.

Криптотелемедицина – технічний розділ криптографії медичної науки і практики, пов'язаний з передачею захищеної медичної зорової інформації (рухливих і не рухливих зображень) на відстань радіоелектронними засобами.

Список використаних джерел

1. Иванов М.А. Криптографические методы защиты информации в компью-терных системах и сетях / Иванов М.А. – М.: КУДИЦ-ОБРАЗ, 2001. – 368 с.

2. Кон П. Универсальная алгебра / Кон П. – М.: Мир, 1968. – 351 с.

3. Коробейников А.Г. Математические основы криптографии : учеб. Пособие / Коробейников А.Г. – СПб.: СПб ГИТМО (ТУ), 2002. – 41 с.

4. Левин М. Криптография. Руководство пользователя / Левин М. – М.: Познавательная книга плюс, 2001. – 320 с.

5. Молдовян А.А. Криптография / Молдовян А.А., Молдовян Н.А., Советов Б.Я. – СПб.: Лань, 2001. – 224 с.

6. Смирнов В.И. Курс высшей математики / Смирнов В.И. – Т. III. – Ч. 1. – М.: Наука, 1974. – 324 с.

8. Чмора А.Л. Современная прикладная криптография / Чмора А.Л. – 2-е изд. – М.: Гелиос, АРВ, 2002. – 256 с.

9. Мінцер О.П. Інструменти підтримки процесів аналітичної діяльності експерта при тематичному дослідженні інформаційних ресурсів та джерел / [Мінцер О.П., Палагін О.В., Величко В.Ю, Стрижак О.Є. та ін.] // Медична інформатика та інженерія. – 2011. – № 2. – С. 12–23.

Комплексная система защиты информации медицинской – надёжный алгоритм оказания качественной медицинской помощи в учереждениях здравоохранения

Шупяцкий И.М.

Резюме. *В статье проанализированы элементы комплексной системы защиты политики безопасности в телемедицине, предложены новые терминологические принципы.*

Ключевые слова: *система, защита, телемедицина, криптотелемедицина, политика, элементы.*

The full system of the protect medical information – the main algorithm for high quality medical service in the states of medicine

Shypuatskiy I.

Summary. *It was discussed the elements of the full system politics protect for tele-medcine, used new words of the starts.*

Keywords: *system protection, telemedicine, kriptotele-medicine, politics, elements.*