УДК:004.056.5:512.624.95:[002-027.552:616-052]

І.М. Шупяцький

ЗАХИСТ ПЕРСОНІФІКОВАНОЇ МЕДИЧНОЇ ІНФОРМАЦІЇ В НОВИХ УМОВАХ СТВОРЕННЯ ТА ВЗАЄМОДІЇ ДЕРЖАВНИХ РЕЄСТРІВ

Державна служба спеціального зв'язку та захисту інформації України, м. Київ

Ключові слова: *криптографія, медицина, персоніфікована інформація, захист.*

I.M. Shupyatskii

Protection of personalized medical information in conditions of new environment creation and interaction of state registers

Key words: *cryptography, medicine, personalized information, protection.*

У спеціалізованій літературі з криптографії, що на сьогодні описує і пояснює особливості захисту інформації при передачі її на відстані, йдеться про політику або гарантованість безпечної системи. Проте, дуже мало уваги приділяється проблемі безпеки системи медичної інформації.

МЕТА РОБОТИ

Проаналізувати постулати політики безпеки з точки зору захисту персональної медичної інформації в нових умовах створення та взаємодії державних реєстрів.

Використання термінів і методологічних особливостей криптографічного порядку інформаційної безпеки застосовується як особлива методологія до захисту медичних даних при їх передаванні на відстань за допомогою телеметрії. Поняття «гарантованість» як міри впевненості дозволяє реалізовувати сформульовану політику безпеки. Операційна гарантованість включає аналіз:

- архітектури та цілісності системи;
- схованих каналів виходу інформації;
- методів адміністрування інформації;
- технології відновлення після збоїв при передаванні інформації.

Концепція надійної електронної бази інформації є центральною при оцінюванні ступеня гарантованості надійності системи.

Політика безпеки інформаційних даних включає такі елементи:

- довільне управління доступом до інформації;
- безпеку повторного використання інформації;
- мітки безпеки;
- контролююче і дозвільне управління доступом до інформації.

Для інформаційної галузі краще використовувати мітки таких рівнів захисту з наступних елементів: абсолютно секретно; секретно; конфіденційно; несекретно.

Архітектуру системи необхідно розробляти з урахуванням сформульованих заходів безпеки або допускати принципову можливість їх добудови.

У якості загрози слід розглядати конкретну фізичну особу або подію, що становить небезпеку для ресурсів, що призводячи до порушення їх конфіденційності, цілісності, доступності та законного використання.

До загроз впровадження належать зокрема троянські програми. Програми, що включають прихований або явний програмний хід, при виконанні якого порушується функціонування системи безпеки. Приклад троянської програми – текстовий редактор, що крім простих функцій редагування виконує приховане копіювання відредагованої документації до файлу хакера.

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

ВИСНОВКИ

Онтологічна аналітика методології криптографічного захисту інформації унеможливлює використання останньої для хакерського або іншого несанкціонованого використання. Методологія, постулати, терміни криптографічного захисту інформації можуть бути використані як основа для захисту телемедичної інформації. Особливостями впровадження є існуючий механізм взаємодії в інформаційному просторі різних за обсягом і схожих за проблематикою спеціальних тем і завдань.