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

ПРОТОКОЛ ПОЛІТИКИ БЕЗПЕКИ В МЕДИЦИНІ

І. М. Шупяцький

Державна служба спеціального зв'язку та захисту інформації України

В статті проаналізовано елементи та постулати політики безпеки, як нові термінологічні засади.

Ключові слова: постулати, онтологія, політика, елементи.

ПРОТОКОЛ ПОЛИТИКИ БЕЗОПАСТНОСТИ В МЕДИЦИНЕ

И. М. Шупяцкий

Государственная служба специальной связи и защиты информации Украины

В статье проанализированы елементы и постулаты политики безопасности, как новые терминологические принципы.

Ключевые слова: постулаты, онтология, политика, элементы.

PROTOCOL OF THE SECURITY POLICY IN THE MEDICINE

I. M. Shypiatskyi

State Department of the Special Connect & Information Protection of Ukraine

The article adduces the elements and postulates of security policy, as terminilogical bases.

Key words: postulates, ontology, policy, elements.

Вступ. У спеціальній літературі з криптографії, яка на сьогодні описує і пояснює особливості захисту інформації при передачі її на відстані, йдеться про політику або гарантованість безпечної системи. Але вельми мало уваги приділяється проблемі безпечної системи щодо медичної інформації. Тобто ми можемо керувати доступом до медичної інформації так, що тільки авторизовані реципієнти або процеси, що діють від їх імені, мають право читати, писати або видаляти медичну інформацію.

Надійна система в криптографії – це система, яка використовує, насамперед, апаратні і програмні засоби для забезпечення одночасної обробки інформації різного ступеня секретності групою користувачів без порушень прав доступу. Надійність системи – це політика безпеки і гарантованості. Подібні постулати з криптографії можуть бути використані для забезпечення захисту медичної інформації при передачі її на відстань за допомогою телеметрії.

Такий криптографічний постулат, як політика безпеки – це набір законів, правил та норм, які забезпечують дисципліну обробки, захисту і поширення інформації. Політика безпеки обумовлює вибір конкретних механізмів, забезпечуючи безпеку системи, і є активним компонентом захисту інформації, включаючи в себе аналіз можливих загроз і вибір заходів протидії.

Наступний постулат – гарантованість – це рівень довіри, який може бути наданий конкретній реалізації системи. Гарантованість висвітлює ступінь коректності механізмів, що забезпечує безпеку. Гарантованість можна вважати пасивним компонентом захисту, що наглядає за механізмами забезпечення безпеки, що є необхідним при передачі даних.

Концепція надійної електронної бази інформації є центральною при оцінці ступеня гарантованості надійності системи. Механізм протоколювання є важливим засобом забезпечення безпеки. Ведення протоколів інформації повинно доповнюватись аудитом, тобто аналізом реєстрації інформації.

Політика безпеки інформаційних даних включає в себе такі елементи:

· довільне управління доступом до інформації;

· безпека повторного використання інформації;

· мітки безпеки;

· контролююче – дозвільне управління доступом до інформації.

Довільне управління доступом до інформації полягає в обмеженні доступу до об'єктів на основі обліку персональних характеристик суб'єкта або групи, в яку суб'єкт входить. Також довільне управління це – власник об'єкта за своїм рішенням може надавати, забороняти або обмежувати доступ інших суб'єктів до даного об'єкта. Стабільний стан прав доступу до інформації при довільному управлінні описаний матрицею, у рядках якої перераховані суб'єкти, а в стовпцях – об'єкти. На перетині рядків і стовпців знаходяться ідентифікатори засобів доступу до інформації, допустимі для суб'єкта по відношенню до об'єкта, наприклад читання, запис, виконання можливості передачі прав іншим суб'єктам.

Безпека повторного використання дозволяє захиститися від випадкового або цільового отримання прихованої 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 декілька сторінок документів, які залишаться в пам'яті навіть після закінчення друку. Необхідне здійснення спеціальних дій задля "анулювання" пристрою.

Контролююче – дозвільне управління доступом реалізується за допомогою міток безпеки, асоційованих із суб'єктами й об'єктами. Мітка суб'єкта характеризує його благонадійність, мітка об'єкта – ступінь закритості наявної інформації.

Для інформаційної галузі краще використовувати мітки таких рівнів захисту із наступних елементів:

· абсолютно секретно;
· секретно;
· конфіденційно;
· несекретно.

Призначення категорій – опис предметної області, до якої належать дані. Механізм категорій дозволяє розділити інформацію, що вдосконалює безпеку системи. Так, суб'єкт не може отримати доступ до «чужих» категорій, навіть як що він є абсолютно благонадійним.

Постановка проблеми. Використання термінів і методологічних особливостей криптографічного порядку інформаційної безпеки має місце і як особлива методологія, що до захисту медичних даних при передачі їх на відстань за допомогою телеметрії. Гарантованість – це міра впевненості, що дозволяє реалізовувати сформульовану політику безпеки. Операційна гарантованість включає в себе аналіз:

· архітектури і цілісності системи;
· схованих каналів виходу інформації;
· методів адміністрування інформації
· технології відновлення після збоїв при передачі інформації.

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

В якості загрози можна розглядати конкретно фізичну особу або подію, які представляють небезпеку для ресурсів, що призводить до порушення їх конфіденційності, цілісності, доступності і законного використання.

Загрози можна поділити на цільові (вхід зі сторони хакера) і випадкові (адресна помилка під час пересилки при збої системи). Цільові загрози поділяють на пасивні і активні. Пасивні загрози – це несанкціоноване зчитування інформації, вони не пов'язані з тією чи іншою зміною інформації. Активні загрози – це отримання і зміна інформації. Класифікуються загрози як фундаментальні, первинні ініціюючі загрози і базові загрози. До фундаментальних загроз відносять наступні.

Витік інформації. Розкриття інформації неавторизованому користувачу або процесу.

Порушення цілісності. Компрометація домовленості (не протиріччя) даних шляхом цілеспрямованого складання, заміни і ліквідації даних.

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

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

Маскарад. Користувач інформації (або інша сутність – процес, підсистема) маскується і пробує видавати себе за іншого користувача. Ця загроза, як правило, пов'язана зі спробою внутрішнього проникнення до периметру безпеки й часто реалізується хакерами.

Обхід захисту. Використання слабких місць системи безпеки для обходу захистних механізмів з метою отримання законних прав та привілеїв щодо використання даних.

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

До загроз впровадження належать наступні:

Троянські програми. Програми, які включають прихований або явний програмний хід, при виконанні якого порушується функціонування системи безпе-

ки. Приклад троянської програми – текстовий редактор, який окрім простих функцій редагування виконує приховане копіювання відредагованої документації до файлу хакера.

Приховані. Деякі додаткові можливості таємно вбудовані в систему або її компоненти, порушуючи функціонування системи безпеки при введені специфічної інформації або інших даних.

Наприклад, підсистема login може нехтувати запит і перевірку пароля при введенні безпосереднього імені користувача.

Розглядаючи фундаментальні загрози, необхідно враховувати також загрози базові. Наприклад, витік телемедичної інформації пов'язаний із такими базовими загрозами, як:

· підслуховування;
· аналіз трафіку;
· персональна необережність;
· «копання у смітті».

Взвємоз'язок може бути досить складним (рис. 1). Так, маскарад є загрозою, що ініціює фундаментальні загрози, в тому числі й витік інформації. Однак маскарад сам по собі також може залежати від витоку інформації. Наприклад, розкриття пароля може ініціювати загрозу маскараду.

Аналіз більше трьох тисяч комп'ютерних злочинів показав, що найчастіше виникають наступні загрози:

· порушення прав;

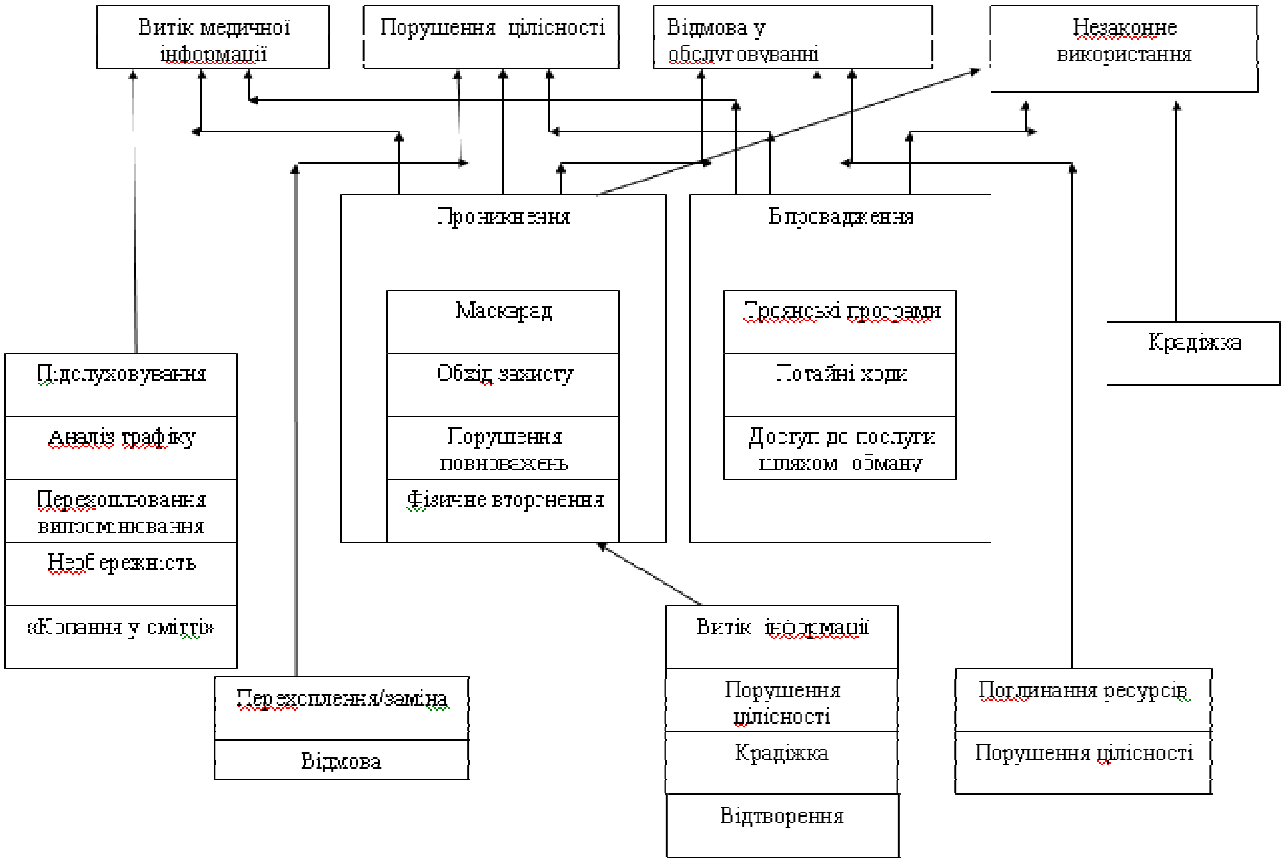

Рис. 1. Взаємозв'язок різноманітних видів загроз.

· маскарад;
· обхід захисту;
· троянські програми або таємні 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 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.

Література.

1. Иванов М. А. Криптографические методы защиты информации в компьютерных системах и сетях / М. А. Иванов. – М. : КУДИЦ-ОБРАЗ, 2001. – 368 с.
2. Кон П. Универсальная алгебра / П. Кон. - М. : Мир. – 1968. – 351 с.
3. Коробейников А. Г. Математические основы криптографии : учебное пособие / А. Г. Коробейников. – СПб. : СПб ГИТМО (ТУ), 2002. – 41 с.
4. Левин М. Криптография. Руководство пользователя / М. Левин. - 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, том III, часть I / В. И. Смирнов. – М. : Наука, Главная редакция физико-математической литературы, 1974. – 324 с.
7. Чмора А. Л. Современная прикладная криптография. 2-е изд. / А. Л. Чмора. – М. : Гелиос, АРВ, 2002. – 256 с.
8. 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., Тахере Г.] // Медична інформатика та інженерія. – 2011. – № 2. – С. 12–23.