Медичні аспекти створення медичного електронного паспорту. Звіт про науково-дослідну роботу «Медичний електронний паспорт громадянина України» (перше повідомлення)

ARTICLE · JANUARY 2010

6 AUTHORS, INCLUDING:

Ozar Mintser
Shupyk National Medical Academy Of Post…
765 PUBLICATIONS **13** CITATIONS

УДК 61:001.8-054.5 (477)
№ держреєстрації: 0108и001039

ЗВІТ ПРО НАУКОВО-ДОСЛІДНУ РОБОТУ «МЕДИЧНИЙ ЕЛЕКТРОННИЙ ПАСПОРТ ГРОМАДЯНИНА УКРАЇНИ»

Основні автори роботи: О. П. Мінцер (*науковий керівник),* В. В. Петров, А. А. Крючин, Л. Ю. Бабінцева (*відповідальний виконавець),* І. В. Горбов, М. С. Денисюк

Національна медична академія післядипломної освіти імені П. Л. Шупика МОЗ України

REPORT ON SCIENTIFICAL AND RESEARCH WORK "MEDICAL ELECTRONIC PASSPORT OF CITIZEN OF UKRAINE"

Basic authors of the work: O. P. Mintser, (*Scientific supervisor),* V. V. Petrov, A. A. Kriuchyn, L. Yu. Babintseva (*Responsible performer),* I. V. Horbov, M. S. Denysiuk

National Medical Academy of Post-Graduate Education by P.L. Shupyk of the Ministry of Public Health of Ukraine

Звіт про науково-дослідну роботу (НДР) включає: 404 е., 77 рис., 23 табл., 137 літературних джерел, 10 додатків.

Мета науково-дослідної роботи - створення механізмів інформаційного відображення здоров'я людини протягом її життя, забезпечення моніторингу рівня здоров'я населення, наступності та спадкоємності медичних дій, надання інформаційної підтримки лікарям у прийнятті рішень, підвищення якості медичної допомоги в Україні.

Ключові слова: медичний електронний паспорт, бази даних, портативні носії інформації, цифровий запис інформації, якість медичної допомоги, інформаційно - телекомунікаційна система, комплексна система захисту інформації, оцінка здоров'я населення, мікроконтролер, медико-технічні вимоги.

Друге повідомлення

ФОРМУВАННЯ МЕДИЧНОЇ АВТОМАТИЗОВАНОЇ ІНФОРМАЦІЙНОЇ СИСТЕМИ ДЛЯ ВПРОВАДЖЕННЯ МЕП ГРОМАДЯНИНА УКРАЇНИ: РОЗРОБЛЕННЯ СКЛАДНИХ СИСТЕМ

Співавтори даного розділу НДР: В. В. Чернов, І. Л. Владимировський, В. М. Голота, П. С. Родський, С. Я. Фейло

Ключові слова: медична автоматизована інформаційна система, криптографія, акредитований центр сертифікації ключів, електронний цифровий підпис, інфраструктура відкритих ключів.

ФОРМИРОВАНИЕ МЕДИЦИНСКОЙ АВТОМАТИЗИРОВАННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ ДЛЯ ВНЕДРЕНИЯ МЕДИЦИНСКОГО ЭЛЕКТРОННОГО ПАСПОРТА ГРАЖДАНИНА УКРАИНЫ: РАЗРАБОТКА СЛОЖНЫХ СИСТЕМ

Соавторы данной главы НИР: В. В. Чернов, И. Л. Владимировский, В. М. Голота, П. С. Родский, С. Я. Фейло

Ключевые слова: медицинская автоматизированная информационная система, криптография, аккредитованный центр сертификации ключей, электронная цифровая подпись, инфраструктура открытых ключей.

FORMATION OF THE MEDICAL AUTOMATED INFORMATION SYSTEM FOR INTRODUCTION OF THE MEDICAL ELECTRONIC PASSPORT OF THE CITIZEN OF UKRAINE: DEVELOPMENT OF DIFFICULT SYSTEMS

Coauthors of this chapter of SRW: V. V. Chernov, I. L. Vladymyrovskyi, V. M. Holota, P. S. Rodskyi, S. Ya. Feylo

Key words: medical automated information system, cryptography, accredited center of certification of the keys, electronic digital signature, public key infrastructure.

Вступ. Сьогодні ніхто не заперечуватиме, що інформаційні технології є необхідною основою нашого майбутнього. Існуюча система медичного обліку все більше не відповідає сучасним вимогам інформаційних систем (ІС). Основні проблеми можна виразити в термінології систем інформаційної безпеки:

1) конфіденційність - медичні дані не захищені від несанкціонованого читання не уповноваженими особами;

2) цілісність - записи в паперовій медичній карті можуть бути змінені або підроблені;

3) доступність - практика показує, що картки пацієнтів часто втрачаються, до того ж вони доступні тільки в одному екземплярі;

4) спостережливість - не існує ніякого контролю за заповненням і читанням записів з медичної картки пацієнта.

Серед основних принципів створення та побудови системи «Персональний електронний медичний паспорт громадянина України» (ПЕМП) виділимо такі:

- інформаційна система ПЕМП створюється з метою зберігання та використання медичної інформації про пацієнтів, причому інформація може бути різних форматів;
- ПЕМП повинна забезпечувати конфіденційність, цілісність, доступність і спостережливість інформації, що зберігається;
- інформаційна система ПЕМП охоплюватиме все населення країни.

Іншими словами, ПЕМП повинна одержувати та зберігати абсолютно повну інформацію про стан здоров'я будь-якого громадянина України, об'єктивну діагностичну інформацію, що може містити в собі не тільки тексти, але й зображення, автоматичне виділення об'єктів, визначення якісних та кількісних характеристик з подальшою їх ідентифікацією і класифікацією за допомогою систем розпізнавання образів.

Багато сучасних медичних приладів формують результат безпосередньо в електронному вигляді. Для захисту даних від підробки лікарю необхідно використовувати особистий електронний цифровий підпис (ЕЦП), особисту електронну печатку лікаря з можливістю встановлення позначки часу під наданим діагнозом. Для захисту даних від випадкової втрати в результаті аварії устаткування або навмисного злому бази даних (БД) такі інформаційні системи повинні розміщуватися на добре захищених серверах, що мають засоби резервного копіювання даних і журналювання стану.

Сьогодні також активно проводиться робота зі створення єдиних міжнародних стандартів в області зберігання, обміну й оперативного доступу до медичних даних. Вже прийнято стандарт ISO 13606-1:2008 Health informatics. Electronic health record communication. Part 1: Reference model - Еталонна модель передачі електронних медичних документів (записів). Обговорюються ще чотири частини цього стандарту: ISO/DIS 13606-2 Archetype interchange specification, ISO/DIS 13606-3 Reference archetypes and term lists, ISO/NP TS 13606-4 Title missing, ISO/CD 13606-5 Interface specification. Проводиться активна робота зі стандартизації персональних машинних носіїв медичних даних (на смарт-картах тощо). Базові вимоги, що забезпечують інформаційну сумісність таких пристроїв, висловлені в міжнародному стандарті ISO 21549:2004 Health informatics. Patient healthcard data. Part 1 : General structure, Part 2: Common objects, Part 3: Limited clinical data, Part 4: Extended clinical data, FDIS Part 5: Identification data, FDIS Part 6: Administrative data, ISO 21549-7:2007 Medication data.

Отже, медична автоматизована інформаційна система повинна забезпечити обмін конфіденційною інформацією з використанням сучасних засобів телекомунікації й електронного цифрового підпису.

1. Огляд існуючих загроз безпеки розкриття особистої інформації.

Просочування конфіденційної інформації через знімні носії - одна з найактуальніших загроз ІТ-безпеки. Самою небезпечною загрозою ІТ-безпеки сьогодні є витік корпоративних даних. Про це однозначно свідчить дослідження компанії InfoWatch. Наприкінці 2007 року було опитано понад 300 великих підприємств та організацій. Саме крадіжка конфіден-

ційної інформації хвилює вітчизняні підприємства якнайбільше. На користь такої точки зору висловилися 64 % респондентів, тоді як на шкідливі коди і атаки хакерів вказали лише 49 % і 48 % відповідно (рис. 1).

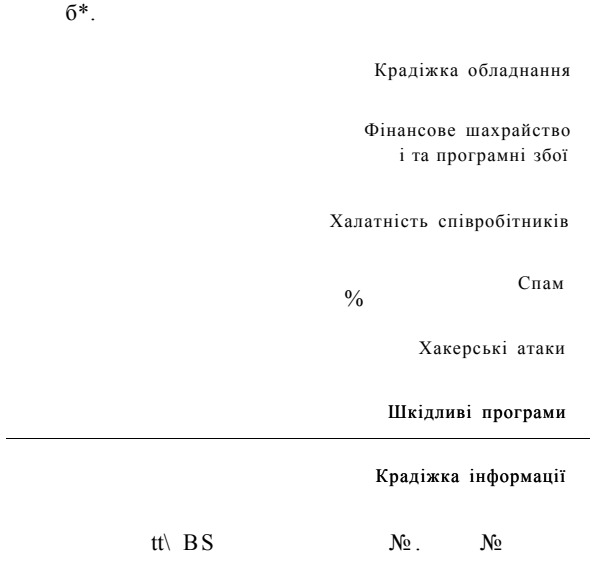

Рис. 1. Найнебезпечніші загрози IT-безпеки.

Для викрадення конфіденційної інформації у розпорядженні інсайдерів є ціла низка каналів передачі даних: поштові ресурси організації, вихід в Інтернет (веб-пошта, веб-сайт, форуми), звичайні порти робочих станцій (USB, COM, LPT), бездротові мережі (Wi-Fi, Bluetooth, IrDA). Проте самим небезпечним каналом витоку вважаються комунікаційні можливості робочих станцій, тобто стандартні порти (COM, LPT, USB), різні типи приводів (CD/DVD-RW, ZIP, Floppy), бездротові мережі і будь-які інші засоби зняття даних з персонального комп'ютера без використання корпоративної пошти і каналу Інтернет (рис. 2).

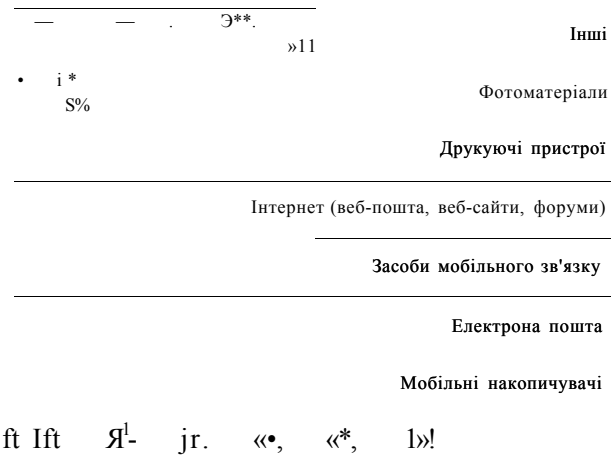

Рис. 2. Найпопулярніші канали витоку даних.

Стурбованість керівників саме цими каналами витоку продиктована, перш за все, збільшеною популярністю мобільних накопичувачів, що протягом останніх років стали дешевшими і більш поширеними.

Слід зазначити, що важливі відомості часто виявляються за межами мережевого периметру просто в результаті безвідповідальних дій персоналу Так, деякі співробітники вважають за краще брати роботу додому, або переписують грифовану інформацію (документи) на портативний накопичувач, щоб вивчити їх на своєму ноутбуку у відрядженні. Іншими словами, службовці керуються благими намірами, що на практиці можуть призвести до компрометації відомчих секретів.

Отже, саме проблема запобігання витокам на рівні робочих станцій є сьогодні однією з найзлободенніших. Мінімізувати ці ризики можна або в рамках комплексного підходу, що припускає перекриття всіх можливих каналів витоку, або шляхом реалізації автономного проекту, що дозволяє забезпечити контроль над обігом важливих відомостей тільки на рівні робочих станцій.

2. Особливості технології проектування медичних інформаційних систем і МЕП.

Існує поширена помилка, що розроблення вимог до системи - це всього лише одинична фаза, що виконується і закінчується на початку розроблення програмного продукту. Подібна ідея - етапного виконання робіт, де кожний наступний етап не починається, поки не буде завершений попередній, формувалася так званим каскадним підходом до розроблення систем, що на сьогоднішній день повністю вичерпав себе [22]. Побудова більшості сучасних медичних інформаційних систем (МІС) базується на спіральному підході.

Яким чином процес проектування впливає на зміст вимог? Вочевидь, вимоги, розроблені на самому початку проекту, так чи інакше використовуються й на його останньому етапі.

Класична V- модель [27], що описує різні стадії проекту, в основному базується на зв'язку між вимогами й їх тестуванням (рис. 3), показує зв'язок вимог і тестування на кожному етапі проекту.

Отже, вимоги у загальному випадку - це багатофункціональний документ, покликаний забезпечити взаємодію всіх учасників процесу проектування: від керівника проекту до рядового інженера.

Згідно з принципами абстракції і декомпозиції вимоги поділяються на декілька рівнів (табл. 1).

У процесі розроблення вимог потрібно чітко розмежувати область проблем і область рішень. Необхідно, щоб до проблемної області були віднесені: формулювання проблем, моделі використовування (прецеденти), призначені для користувача вимоги. Починаючи з системних вимог все повинне бути віднесено до області рішень.

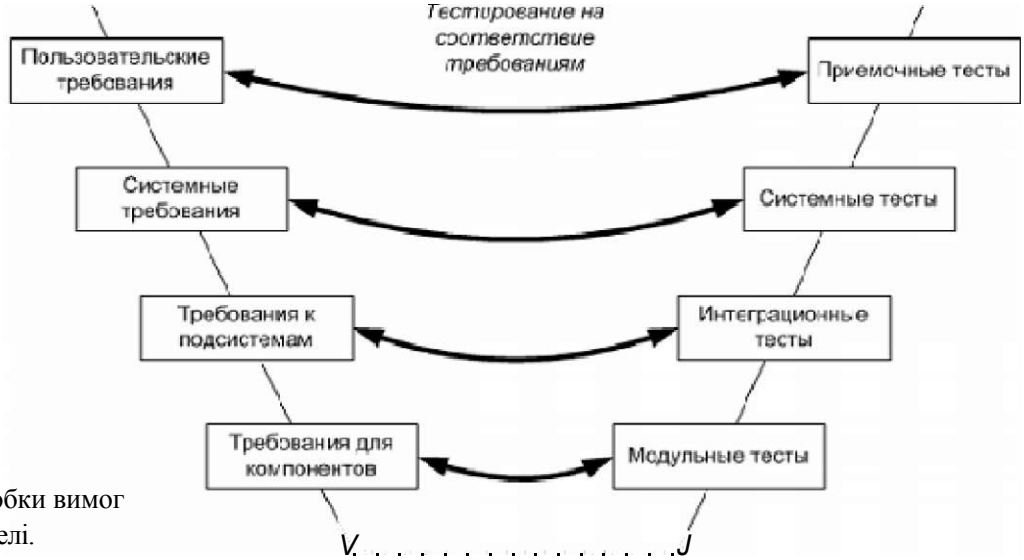

Рис. 3. Процес розробки вимог згідно V-моделі.

Таблиця 1. Область проблем та область рішень

Рівень вимог	Область	Точка зору	Мета
Вимоги користувача	Область проблем	Користувач (представник зацікавленої сторони)	Визначають - чого користувач бажає домогтися за допомогою ІС, що створюється. Слід уникати формулювання конкретних рішень
Системні вимоги	Область рішень	Аналітик	Абстрактно визначає - як система буде задовольняти вимоги користувачів. Слід уникати точного опису реалізації рішень, що пропонуються
Системні специфікації	Область рішень	Архітектор	Визначає - як архітектура системи буде задовольняти системним вимогам

Тут необхідно звернути увагу на принцип абстракції, якому слідують при описі проблемної області.

Первинне формулювання можливостей системи містить тільки те, що необхідно для визначення (опису) проблеми, і не містить нічого, що визначає конкретні рішення. Це дає свободу системним інженерам щодо знаходження найкращого рішення проблеми, оскільки інженер не зв'язаний наперед ніякими певними ідеями.

Той же принцип застосовний і до системних інженерів (аналітиків), які повинні залишати свободу архітекторам для виконання їх роботи, що полягає в знаходженні кращого системного рішення для абстрактних системних вимог. Елементи реалізації, створювані на етапі функціонального моделювання на верхньому рівні вимог, не повинні містити деталей, що будуть і повинні визначатися на наступних стадіях.

Відсутність чіткого розділення між проблемами і рішеннями, може призвести до таких негативних наслідків:

- недостатнє розуміння існуючих проблем;
- неможливість визначення межі (масштаб) системи і розуміння того, який функціонал повинен до неї входити;
- домінування розробників і виконавців у дискусіях про систему, оскільки єдиний опис, існуючий для систем, описує її в термінах реалізації, а не у формулюваннях проблем;
- неможливість знаходження найкращого рішення через обмеження свободи у виборі рішення.

З урахуванням декомпозиції спрощений процес розроблення вимог представлено на рисунку 4.

Для моделей процесів використані такі графічні елементи: за допомогою кругу (овалу) позначені процеси, за допомогою прямокутника позначені дані, стрілки указують на суть операції з даними - дані читаються або записуються. Тобто рисунок 4 показує, що процес розроблення призначених для користувача вимог читає (отримує) формулювання потреб користувачів і записує (виробляє) призначені для користувача вимоги. Крім цього, процес розроблення призначених для користувача вимог виробляє і читає (використовує) модель застосування.

Процес розроблення вимог повинен обов'язково враховувати процедури перевірки виконання вимог і можливість внесення змін у хід розроблення. Відповідна схема процесу представлена на рис. 5.

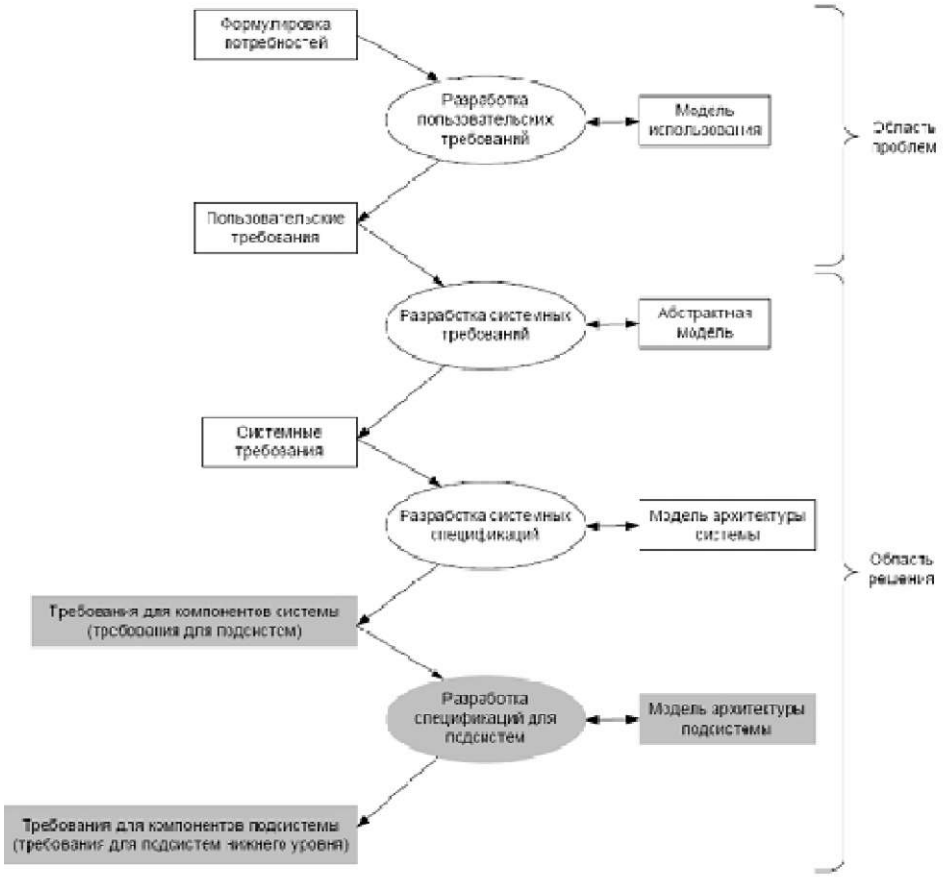

Рис. 4. Спрощений процес розроблення вимог.

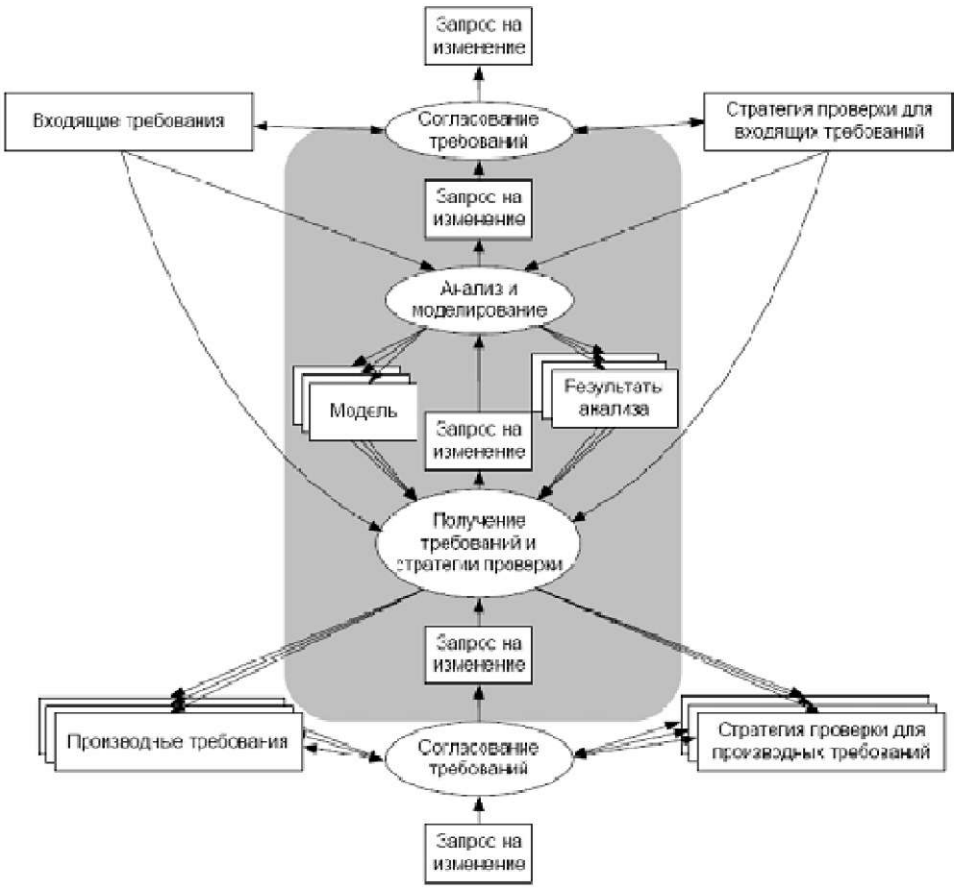

Рис. 5. Схема розроблення вимог з врахуванням запитів на змінення.

Процес починається з необхідності узгодження вхідної інформації (вимог) із замовниками, що знаходяться на рівень вище.

На другому етапі необхідно провести аналіз вхідної інформації і зрозуміти, як з неї одержати вихідну (похідну) інформацію. Як тільки похідні вимоги стають в достатній мірі сформованими, необхідно розпочинати їх узгодження з виконавцями, що працюють на наступному рівні.

Створення зв'язків між вимогами.

У контексті розроблення вимог створення й аналіз зв'язків необхідні, в першу чергу, для розуміння того, як вимоги високого рівня - загальні цілі, задачі, побажання, передбачувані очікування, потреби тощо - трансформуються у вимоги низького рівня. Отже, в основному, зв'язки потрібні між різними рівнями інформації.

Використовування зв'язків може надати такі вигоди:

1. Упевненість у досягненні цілей. Встановлення зв'язків і формалізація їх контролю призводить до чіткого розуміння того, як саме досягаються цілі.

2. Можливість оцінки впливу змін. Існування зв'язків між вимогами дає можливість проводити різного роду аналіз впливу змін, що вносяться.

3. Можливість оцінки внеску підрядників і субпідрядників, тобто оцінювання частини роботи, що за проектом її виконують інші організації.

4. Можливість контролю ходу проекту й оцінювання обсягів виконаної роботи. Зазвичай буває дуже важко оцінити виконану вами роботу як частину загального обсягу робіт за проектом, тим більше якщо сама робота полягає в написанні і редагуванні документів. Використовування зв'язків дозволяє достатньо точно вимірювати прогрес навіть на ранніх етапах проекту.

5. Можливість зіставляти витрати і вигоду (визначати економічну ефективність, доцільність). Однозначний зв'язок між вимогами і певними компонентами системи дозволяє визначати витрати з передбачуваним позитивними ефектом від їх реалізації.

Зв'язки між вимогами зазвичай мають тип «багато хто до багато кого» (рис. 6). Одна вимога нижнього рівня може бути пов'язана з декількома вимогами вищого рівня, і навпаки. В простому ж випадку зв'язки можуть встановлюватися між різними вимогами, але одного рівня.

Стрілки на лініях зв'язку на рисунку 6 проставляються виходячи з конкретного правила - стрілка завжди указує напрям до джерела інформації. Іншими словами, якщо одна інформація «витікає» з іншої, то зв'язок повинен бути направлений від першого до другого. Для такого правила є дві причини:

- зазначений формат стрілки часто відповідає хронологічному порядку появи інформації - зв'язок завжди указує на інформацію, що існувала раніше;
- дуже часто це відповідає також і правам на володіння інформацією: одній людині належать зв'язки, що «витікають» з документа, іншій - ті, що тільки входять.

Для підтримки процесу роботи з вимогами застосовуються різні методи аналізу зв'язків між вимогами (табл. 2).

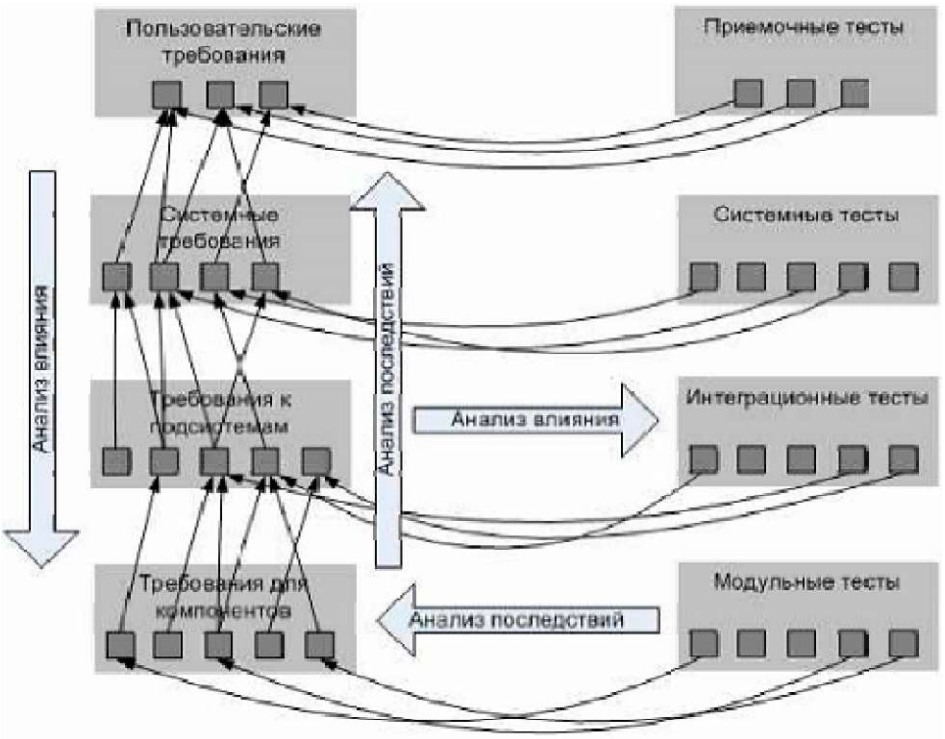

Рис. 6. Зв'язки між вимогами.

Таблиця 2. Методи аналізу зв'язків вимог

Метод аналізу	Опис	Процес, що підтримується
Аналіз впливу	Аналіз вхідних зв'язків з метою відповіді на питання: «Що станеться якщо змінити дану вимогу?»	Процес змін
Аналіз наслідків	Аналіз вихідних зв'язків з метою відповіді на питання: «Нам це дійсно потрібно?»	Аналіз економічної доцільності
Аналіз покриття	Аналіз зв'язків з метою відповіді на питання «Все враховано?» Як правило використовується для оцінювання прогресу роботи	Проектування. Звітування

Аналіз впливу дає можливість оцінити, на які інші елементи проекту (нижнього рівня) вплине зміна в даному конкретному елементі. А оскільки часто вплив одного елемента на інші має відносний характер, тому кожного разу внесення зміни, якщо це необхідно, призводить до детальнішого аналізу того, чи торкнеться дана зміна інших елементів проекту чи ні, і якщо торкнеться, то наскільки сильно.

Аналіз наслідків працює в протилежному напрямку аналізу зв'язків. Аналізуються елементи нижнього рівня, наприклад, зміст вимоги, частина специфікації або результат тесту, а потім за допомогою зв'язків перевіряється його відповідність одному з елементів вищого рівня.

Елементи нижніх рівнів, якщо вони не мають ніяких зв'язків «вгору», ймовірно, лише збільшують витрати і не приносять ніякої користі.

Для аналізу вхідних зв'язків застосовують аналіз покриття (рис 7). Він дозволяє перевірити зв'язок вимог високого рівня зі специфікаціями найбільш низьких рівнів і тестами. Відсутність таких зв'язків свідчить про те, що вимога не буде задоволена (виконана) або протестована. Проте й наявність зв'язків, самих по собі, не дає гарантії, що вимога буде задоволена і протестована. Для переконання в останньому слід додати знання і досвід проектувальника системи.

Аналіз покриття також застосовується для оцінювання прогресу роботи - того, наскільки системні

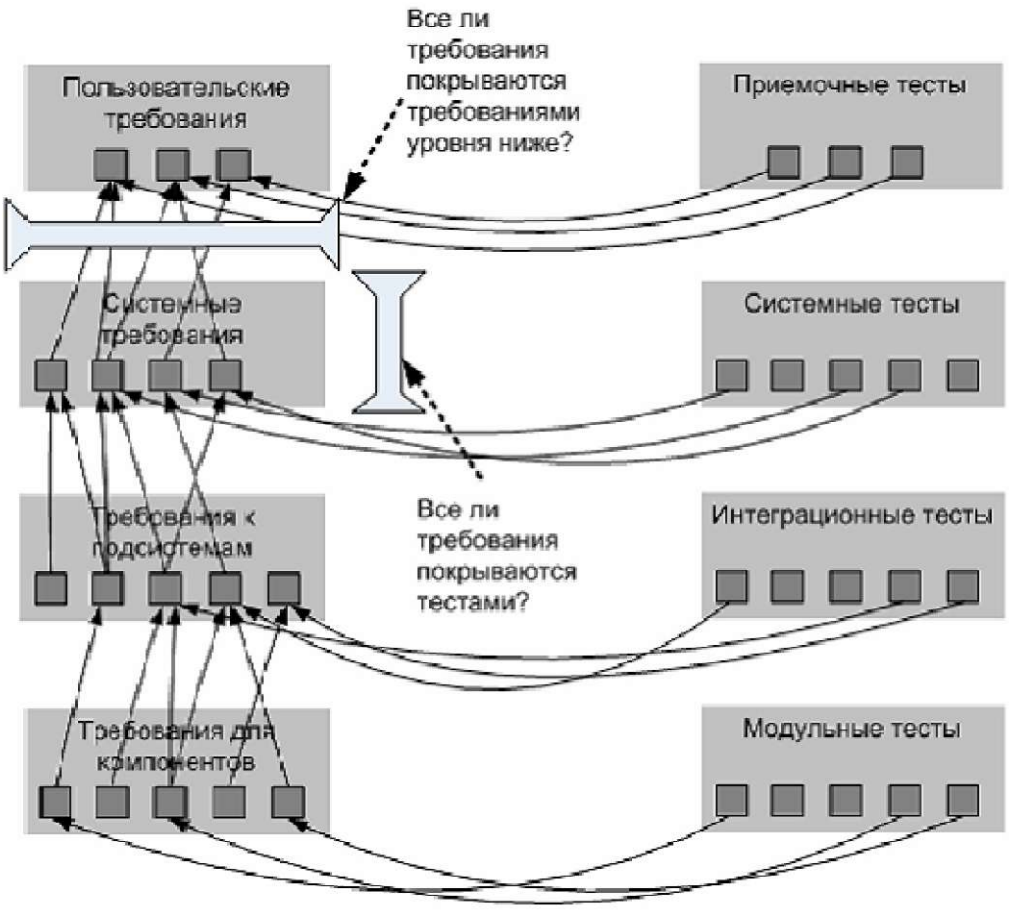

Рис. 7. Аналіз покриття.

інженери просунулися в задоволенні вимог користувачів.

У процесі розроблення кожна системна вимога зв'язується з тими призначеними для користувача вимогами, для задоволення яких вона і призначена. Відмітимо таке: якщо установка зв'язків відбувається безпосередньо в процесі написання системних вимог, то потребує невеликих додаткових витрат у порівнянні з тим, коли встановленням зв'язків займаються вже після призначення вимог як для користувача, так і системних.

Той же самий принцип може бути використаний для вимірювання прогресу розроблення планів тестування. Відсоток готових планів тестування може бути визначений як відсоток покриття вимоги тестами.

Розглянуті типи аналізу зв'язків дозволяють зробити висновок про їх ключове значення в процесі роботи з вимогами.

Роль вимог в сфері забезпечення безпеки ІС.

Не існує складних систем, що були б безпечними. Складність - головний ворог безпеки; вона практично завжди виражається в кількості додаткових засобів, можливостей і параметрів, доступних користувачу програми.

Наприклад, є ІС з 20 параметрами, кожен з яких може бути включено або вимкнено, що припускає наявність більше мільйона різних конфігурацій програми. Для переконання в працездатності ІС слід протестувати декілька найбільш очікуваних комбінацій параметрів. А для переконання в безпеці системи необхідно оцінити кожну з мільйона можливих конфігурацій і перевірити стійкість цих конфігурацій до кожного з можливих видів атак. Останнє звичайно неможливо. Зазвичай кількість параметрів ІС набагато перевищує 20, крім того, слід враховувати змінне середовище.

Отже, абсолютно безпечних систем не існує.

Тому важливо знати, що слід захистити та які загрози є актуальними для даної ІС.

Як приклад невдалої системи захисту можна привести протокол захищених електронних транзакцій (Secure Electronic Transaction - SET), який застосовується для захисту електронних платежів, виконуваних в Internet за допомогою кредитних карт. Одна з особливостей протоколу SET полягає в шифруванні номера кредитної карти, щоб зловмисник, що перехопив номер, не міг його скопіювати. Друга ж особливість, коли навіть продавець не бачить номера кредитної карти покупця, набагато менш вдала.

Деякі продавці використовують номери кредитних карт для пошуку відомостей про покупця або для стягування з нього додаткових зборів. Системи електронної комерції були засновані на припущенні про те, що у продавця є доступ до номера кредитної карти покупця. Зрозуміло, заборонити цей доступ нереально. В результаті в специфікації протоколу включена можливість відправляти в зашифрованому вигляді номер кредитної карти двічі - до банку і до продавця, щоб у продавця теж був номер кредитної карти покупця.

Навіть не дивлячись на наявність такої можливості, протокол SET побудовано на вирішення абсолютно іншої проблеми. В більшості випадків номери кредитних карт крадуть зовсім не під час їх передачі від покупця продавцю. Їх крадуть з бази даних продавця. SET же захищає інформацію тільки під час її передачі.

Наведений приклад демонструє необхідність системного підходу до побудови системи безпеки ІС. Неможливо кожен засіб безпеки розглядати окремо, необхідно врахувати його вплив на всю систему в цілому. І найголовніше - як і у випадку розроблення функціоналу ІС, при розробці системи безпеки слід чітко визначити, для чого це робиться, які саме ресурси підлягають захисту і який рівень безпеки повинен бути забезпечений. Неконтрольоване підвищення рівня захисту окремих об'єктів може призвести до знищення рівня безпеки системи в цілому.

Аутентифікація користувачів.

Згідно з визначенням, аутентифікація користувача (АК) - це перевірка того, чи дійсно користувач є тим, за кого він себе видає.

Фахівці з інформаційної безпеки класифікують різні методи аутентифікації відповідно до відмітних характеристик. Існують три типи чинників аутентифікації.

Надійнішою та зручнішою у застосуванні вважається технологія аутентифікації, що заснована на вживанні ЕЦП. Для цього вимагається спочатку одержати цифровий сертифікат ключа електронного підпису.

Електронний цифровий підпис - один із сервісів безпеки, що допомагає вирішувати завдання цілісності, доступності та невідмовності авторства. Для повноцінного функціонування електронного цифрового підпису необхідне створення розвиненої інфраструктури, що відома як інфраструктура відкритих ключів або PKI (public key infrastructure). Під цим терміном розуміється повний комплекс програмно-апаратних засобів, а також організаційно-технічних заходів, необхідних для функціонування технології з відкритими ключами. Основним компонентом інфраструктури є власне система управління цифровими ключами і сертифікатами. Асиметрична криптографія допомагає вирішувати завдання забезпечення конфіденційності, аутенти-

фікації, цілісності і достовірності інформації. Розглянемо деякі з понять докладніше.

В асиметричній криптографії застосовується два типи відмінних один від одного ключів. Перший, публічний ключ, використовується для того, щоб виконати "публічні операції" (наприклад, шифрування, перевірку і підтвердження достовірності ЕЦП). Другий - відповідно, закритий ключ - використовується для "закритих операцій" (наприклад, розшифрування, генерація ЕЦП). Тобто, все, що зашифровано за допомогою публічного ключа, може бути розшифровано за допомогою закритого або секретного ключа. Така система дозволяє не тільки уникнути необхідності ділитися секретною (ключовою) інформацією з іншими користувачами, але і забезпечити таку важливу властивість інформації, як невідмовність користувача від авторства. Оскільки тільки власник закритого ключа в змозі реалізувати відповідні процедури.

Інфраструктура відкритих ключів, що базується на застосовуванні сертифікатів (визначають власників закритих ключів і їх повноваження), дозволяє співвідносити публічні ключі з їх власниками. Це безумовно важливо, оскільки при криптографічному перетворенні повідомлення вирішальним чинником є наявність публічного ключа, що належить легальному одержувачу, а не будь-якій «підставній» особі. Отже, технологія PKI по суті є способом безпечного розподілу публічних ключів. За аналогічною схемою після отримання підписаного документа є можливою перевірка ідентичності особи, яка підписала документ.

Іншими, не менш важливими складовими асиметричної криптографії є управління закритими ключами, а також питання зберігання ключів.

По суті, єдиний спосіб гарантувати цілісність електронного документа полягає в тому, щоб підписати кожне повідомлення електронним цифровим підписом, оскільки критично важливою властивістю ЕЦП є невідмовність. Іншими словами, якщо підписаний документ одержано, то підписуюча особа не може пізніше заперечувати факт підписання документа. Отже, відправник не може відмовитися від досконалої дії. Така властивість дозволяє використовувати документи, підписані за допомогою ЕЦП, як доказову базу в суді, і забезпечує нескасованість посланих по електронній пошті замовлень або розпоряджень.

Важливою областю вживання асиметричної криптографії є також аутентифікація. Наприклад, при вході в операційну систему Microsoft Windows за смарт-картою користувач відправляє запит на аутентифікацію, підписаний своїм закритим ключем. У відповідь він отримує від сервера реквізити для посвідчення особи (ticket granting ticket - "квиток, що надає квиток" в - термінології Kerberos), що зашифровані за допомогою його відкритого ключа і для розшифрування яких знову потрібно застосувати закритий ключ. Асиметрична криптографія є невід'ємною частиною протоколу мережної аутентифікації TLS/SSL.

Хоча кожен з додатків по-своєму використовує відкритий і закритий ключі, всі вони виходять з одного положення - кожен користувач, кожен учасник обміну інформацією є єдиним володарем свого закритого ключа.

Для забезпечення безпеки закритих ключів сьогодні найчастіше використовуються такі підходи:

• програмні сховища (Software token) призначені для зберігання закритих ключів на диску комп'ютера, найчастіше - в зашифрованому вигляді. Прикладами реалізації даного підходу є криптопровайдер Microsoft Enhanced CSP, що входить до складу операційної системи Microsoft Windows або браузер Mozilla/Netscape;

• апаратні пристрої (hardware token) призначені для зберігання закритих ключів і виконання криптографічних операцій, що вимагають використовування закритого ключа. Найпоширенішими в СНД представниками пристроїв даного класу є смарт-карти і USB-ключі eToken PRO, що побудовані з використанням мікросхем смарт-карти;

• репозитарії (credentials repository) - виділені сервери, призначені (часто спеціалізоване апаратне забезпечення) для централізованого зберігання закритих ключів декількох користувачів. Для того, щоб виконати операцію з використанням свого закритого ключа (наприклад, підписати електронний лист) користувач повинен спочатку аутентифікуватися та передати дані для оброблення на сервері, а потім отримати результат.

Враховуючи вразливість програмних сховищ закритого ключа все частіше стали використовувати апаратні пристрої з криптографічними можливостями. Завдяки виконанню криптографічних операцій, апаратні пристрої забезпечують вищий рівень захисту ключової інформації, оскільки закриті ключі ніколи не експортуються з пристрою. Основна проблема згаданої раніше системи захисту полягає в тому, що закритий ключ імпортується в небезпечне середовище локального комп'ютера. Розв'язати цю проблему можливо лише застосувавши відчужуваний пристрій, здатний апаратно виконувати криптографічні операції.

Отже, зовнішній носій повинен бути оснащений мікропроцесором, здатним зашифрувати і відправити назад повідомлення, послане на цей пристрій локальним комп'ютером користувача.

Припустимо, що користувач підключає апаратний пристрій з криптографічними можливостями на інфіковану вірусом машину і вводить пароль для авторизації у вікні, що з'явилося на екрані монітора. Існує вірогідність того, що вірус може підмінити собою користувача і, діючи від його імені, використовувати апаратний пристрій (токен) для підпису повідомлення. Проте реалізація такої атаки обмежена в часі - її можна виконати тільки на час фізичного підключення токена до комп'ютера.

В обговорюваному типі токенів закритий ключ зберігається в захищеній пам'яті пристрою і ніколи не покидає її. Тому скористатися ним для проведення криптографічних перетворень можна тільки у разі отримання зловмисником фізичного доступу до пристрою. Якщо зловмисник зуміє одержати токен легального користувача, виникне загроза компрометації інформації, що зберігається в його пам'яті. Безпека в цьому випадку забезпечується лише ступенем фізичного захисту пристрою. У простих токенів він мінімальний, тому зламати і витягнути ключову інформацію не складає серйозних труднощів. Проте відзначимо, що для злому захисту часто необхідно зруйнувати сам токен або просто вкрасти його, а, значить, напад буде знайдений легальним користувачем. Звичайно, іноді користувач сам може втратити свій токен. У такому разі він повинен негайно повідомити про це адміністратора безпеки (або іншу особу, що відповідає за інформаційну безпеку), який відкличе загублені сертифікати і виконає інші роботи згідно регламенту.

На додаток до перерахованих ризиків і загроз, існує потенційно більш руйнівний тип нападу на апаратні токени - атака на побічні канали (side channel attack). Діставши фізичний доступ до токена той, що атакує, може одержати інформацію про закриті ключі користувача, вимірявши такі показники, як час і потужність, витрачені в ході виконання токеном криптографічних перетворень. Можливо подібний вид атаки видасться неправдоподібним, проте він є високоефективним способом прочитування закритого ключа, до того ж таким, що не пошкоджує сам пристрій.

Описані загрози обумовлюють необхідність наявності у пристрої розширеного функціоналу, що об'єднує криптографічні можливості з можливостями технологій для забезпечення посиленого захисту проти такого роду атак, зокрема пов'язаних з фізичним доступом (табл. 3).

Таблиця 3. Фактори аутентифікації

Фактор	Переваги	Слабкі сторони	Приклади
Щось відоме користувачу, наприклад пароль	Мала вартість реалізації, переносимість	Доступність активній розвідці. Неможливість виявлення таких атак. Паролі або легко вгадати, або важко запам'ятати. Висока вартість обробки забутих паролів	Пароль, персональний ідентифікаційний код, комбінація сейфа
Щось, чим володіє користувач	Найважче для атаки	Висока вартість. Може бути втрачений або вкрадений. Ризик відмови апаратурній частині. Не завжди переносимо	Розпізнавальний знак, смарт-карта, секретні дані, вбудовані у файл або пристрій, механічний ключ
Щось властиве користувачу	Найлегше з точки зору виконання аутентифікації	Висока вартість. Загроза дистанційного відтворення. Ризик втрати відомостей особистого характеру. Характеристика не може бути змінена. Помилкове відхилення законних користувачів. Характеристика може бути пошкоджена.	Відбитки пальців, малюнок сітківки ока, розпізнавання голосу, фотодокумент

Зауважимо, що сам процес аутентифікації складний. Складно також зробити систему достатньо чутливою, щоб вона відкидала сторонніх користувачів і при цьому час від часу не відкидала своїх. Також можуть бути визнані непридатними внаслідок фізіологічних змін і тілесних пошкоджень і біометричні показники.

3. Підсистема підтримки ЕЦП.

Персональний електронний медичний паспорт громадянина України має бути підтриманим технологією електронного цифрового підпису з використанням сертифікованих державною службою спеціального зв'язку та захисту інформації (ДССЗЗІ) України, криптографічних засобів захисту інформації.

Основні вимоги до засобів ЕЦП, що використовуються в системі:

- обчислення хеш-функції відповідно до ДСТУ 34311;
- вироблення та перевірка електронного цифрового підпису відповідно до ДСТУ 4145-2002 та ДСТУ 34310;

- можливість вироблення декількох електронних цифрових підписів для одного документа;
- робота з сертифікатами відкритих ключів і списками відкликаних сертифікатів у форматі X.509 v3, склад полів яких відповідає вимогам Закону України "Про електронний цифровий підпис";
- відповідність нормам Законів України "Про електронний цифровий підпис" і "Про електронні документи та електронний документообіг";
- можливість управління сертифікатом згідно із законом України "Про електронний цифровий підпис" і забезпечення підтримки запитів до центру сертифікації ключів (ЦСК) у форматі, що відповідає рекомендаціям PKCS;
- надання доступу до каталогу відкритих сертифікатів акредитованих ЦСК (АЦСК);
- надання доступу до служби часу;
- можливість використання апаратних носіїв ключових даних (смарт-карти, Secure Token).

До складу підсистеми АСЗЕЗ-ЕЦП повинні входити такі модулі:

- модуль взаємодії з базами даних сертифікатів користувачів ЕЦП акредитованих центрів сертифікації ключів;
- центри реєстрації абонентів АЦСК у регіоні.

Варіанти отримання ключів ЕЦП респондентами.

Запропоновані два варіанти:

1. Респонденти можуть користуватися ЕЦП від будь-якого акредитованого центру сертифікації ключів. Інакше кажучи, респондент звертається та отримує посилений сертифікат в АЦСК.

2. Респонденти, за бажанням, зможуть отримати на платній основі комплекти ключів ЕЦП і сертифікатів до них безпосередньо в МОЗ України. У такому випадку МОЗ повинен користуватися послугами будь-якого АЦСК (можливо, створеного як підприємство державної форми власності при МОЗ). За другим варіантом, на базі МОЗ розгортаються центри реєстрації абонентів (ЦРА) всіх АЦСК або МОЗ користується послугами будь-якого одного АЦСК, що працює на його базі.

4. Розподілені бази даних.

При розробці архітектури системи виникає питання про ступінь концентрації ресурсів ІС, особливо це питання торкається систем управління базами даних (СУБД).

Історично першими з'явилися зосереджені ІС, в яких дані зберігалися й оброблялися засобами одного сервера або кластера серверів (рис. 8). Проте в міру розвитку телекомунікаційних технологій виявилися недоліки даної архітектури. Вона непогано працює в обмеженому масштабі, наприклад, в рамках одного офісу або декількох видалених робочих груп-філіалів, пов'язаних з головним підприємством.

Подібна архітектура погано піддається масштабуванню. При зростанні системи може настати момент, коли витрати на модифікацію і супровід такої системи стають порівнянними з витратами на створення нової системи. Окрім застосування зосередженої схеми ІС в глобальних мережах створює критичні точки відмови, наприклад, пошкодження каналів зв'язку внаслідок стихійної біди може призвести до недоступності важливих ресурсів для цілого регіону.

Подібні проблеми розв'язуються шляхом децентралізації ресурсів і використовування розподіленої архітектури ІС (рис. 9).

Останні півтора десятиліття ознаменувалися великим прогресом в області побудови розподілених ІС, зокрема розподілених СУБД.

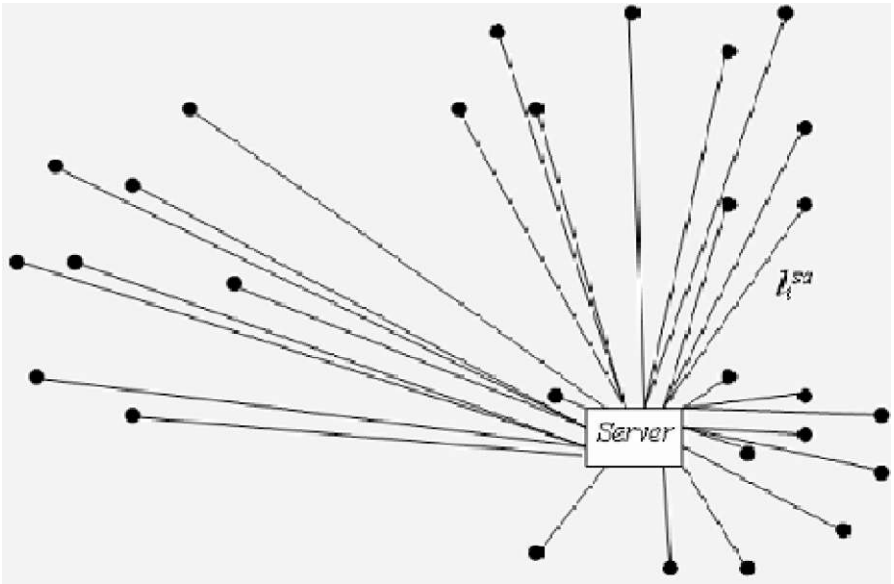

Рис. 8. Зосереджена ІС.

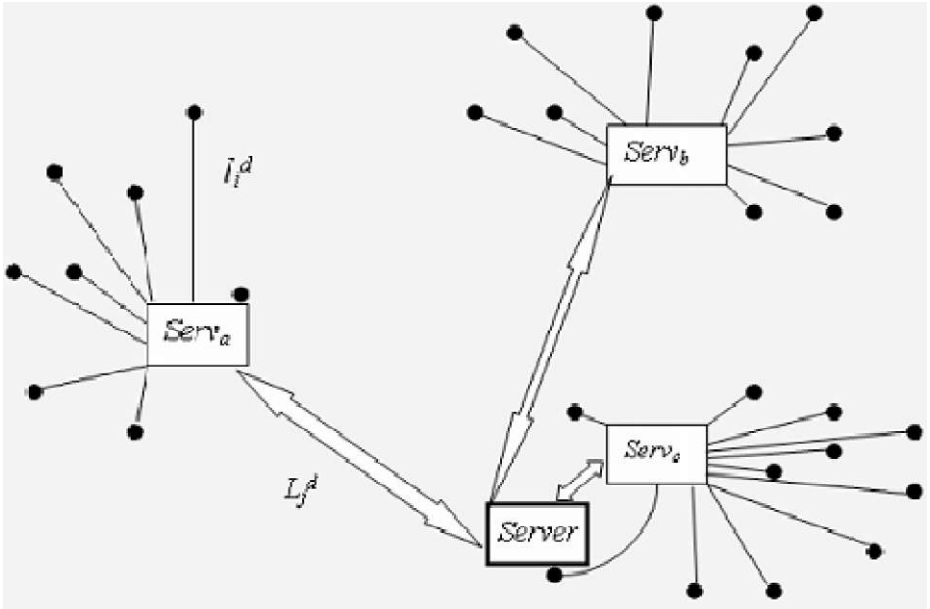

Рис. 9. Розподілена ІС.

Під розподіленою (Distributed DataBase - DDB) зазвичай розуміють базу даних, що включає фрагменти з декількох баз даних, які розташовуються на різних вузлах мережі комп'ютерів, і, можливо управляються різними СУБД. Розподілена база даних виглядає, з погляду користувачів і прикладних програм, як звична локальна база даних. В цьому значенні слово "розподілена" відображає спосіб організації бази даних, але не зовнішню її характеристику ("розподіленість" бази даних невидима ззовні).

Можливі однорідні і неоднорідні розподілені бази даних. В однорідному випадку кожна локальна база даних управляється однією і тією ж СУБД. В неоднорідній системі локальні бази даних можуть відноситися навіть до різних моделей даних. Мережна інтеграція неоднорідних баз даних - це актуальна, проте дуже складна проблема. Багато рішень відомі на теоретичному рівні, але поки не вдається справитися з головною проблемою - недостатньою ефективністю інтегрованих систем.

Основним завданням інтеграції неоднорідних БД є надання користувачам інтегрованої системи глобальної схеми БД, представленої в деякій моделі даних, і автоматичне перетворення операторів маніпулювання БД глобального рівня в операторів, зрозумілих відповідним локальним СУБД.

При суворій інтеграції неоднорідних БД локальні системи БД втрачають свою автономність. Після включення локальної БД у федеральну систему всі подальші дії з нею, включаючи адміністрування, повинні проводитися на глобальному рівні. Оскільки користувачі часто не погоджуються втрачати локальну автономність, бажаючи проте мати нагоду працювати зі всіма локальними СУБД на одній мові і формулювати запити з одночасною вказівкою різних локальних БД, розвивається напрям МУЛЬТІ-БД. В системах МУЛЬТІ-БД не підтримується глобальна схема інтегрованої БД і застосовуються спеціальні способи йменування для доступу до об'єктів локальних БД. Як правило, в таких системах на глобальному рівні допускається тільки вибірка даних, що дозволяє зберегти автономність локальних БД.

Як правило, інтегрувати доводиться неоднорідні БД, розподілені в обчислювальній мережі. Це в значній мірі ускладнює реалізацію. Додатково до власних проблем інтеграції доводиться вирішувати всі проблеми, властиві розподіленим СУБД: управління глобальними транзакціями, мережну оптимізацію запитів тощо. Дуже важко домогтися ефективності.

Як правило, для зовнішнього представлення інтегрованих і МУЛЬТІ-БД використовується (іноді розширена) реляційна модель даних. Останнім часом все частіше пропонується використовувати об'єктно-орієнтовані моделі, але на практиці поки основою є реляційна модель. Тому, зокрема, включення в інтегровану систему локальної реляційної СУБД істотно простіше і ефективніше, ніж включення СУБД, заснованої на іншій моделі даних.

Виділяють [23] 12 властивостей або якостей ідеальної DDB:

- локальна автономія (local autonomy);
- незалежність вузлів (no reliance on central site);
- безперервні операції (continuous operation);
- прозорість розташування (location independence);
- прозора фрагментація (fragmentation independence);

• прозоре тиражування (replication independence);
• оброблення розподілених запитів (distributed query processing);
• оброблення розподілених транзакцій (distributed transaction processing);
• незалежність від устаткування (hardware independence);
• незалежність від операційних систем (operationg system independence);
• прозорість мережі (network independence);
• незалежність від баз даних (database independence).

Локальна автономія. Ця якість означає, що управління даними на кожному з вузлів розподіленої системи виконується локально. База даних, розташована на одному з вузлів, є невід'ємним компонентом розподіленої системи. Будучи фрагментом загального простору даних, вона, в той же час, функціонує як повноцінна локальна база даних; управління нею виконується локально і незалежно від інших вузлів системи.

Незалежність від центрального вузла. В ідеальній системі всі вузли рівноправні і незалежні, а розташовані на них бази є рівноправними постачальниками даних в загальний простір даних. База даних на кожному з вузлів самодостатня - вона включає повний власний словник даних і повністю захищена від несанкціонованого доступу.

Безперервні операції. Цю якість можна трактувати як можливість безперервного доступу до даних (відоме "24 години на добу, сім днів на тиждень") в рамках DDB незалежно від їх розташування і незалежно від операцій, виконуваних на локальних вузлах. Цю якість можна виразити гаслом "дані доступні завжди, а операції над ними виконуються безперервно".

Прозорість розташування - означає повну прозорість розташування даних. Користувач, що звертається до DDB, нічого не повинен знати про реальне, фізичне розміщення даних у вузлах інформаційної системи. Всі операції над даними виконуються без урахування їх місцезнаходження. Транспортування запитів до баз даних здійснюється вбудованими системними засобами.

Прозора фрагментація. Трактується як можливість розподіленого (тобто на різних вузлах) розміщення даних, що логічно є єдиним цілим. Існує фрагментація двох типів: горизонтальна і вертикальна. Перша означає зберігання рядків однієї таблиці на різних вузлах (фактично, зберігання рядків однієї логічної таблиці в декількох ідентичних фізичних таблицях на різних вузлах). Друга означає розподіл стовпців логічної таблиці по декількох вузлах.

Прозорість тиражування. Тиражування даних - це асинхронний (в загальному випадку) процес перенесення змін об'єктів початкової бази даних в бази, розташовані на інших вузлах розподіленої системи. В даному контексті прозорість тиражування означає можливість перенесення змін між базами даних засобами, невидимими користувачу розподіленої системи. Дана властивість означає, що тиражування можливе і досягається внутрішньосистемними засобами.

Оброблення розподілених запитів. Ця властивість DDB трактується як можливість виконання операцій вибірки над розподіленою базою даних, сформульованих в рамках звичного запиту на мові SQL. Тобто операцію вибірки з DDB можна сформулювати за допомогою тих же мовних засобів, що і операцію над локальною базою даних.

Оброблення розподілених транзакцій. Трактується як можливість виконання операцій оновлення розподіленої бази даних, не руйнуючи цілісність і узгодженість даних. Ця мета досягається вживанням двохфазового або двофазного протоколу фіксації транзакцій (two-phase commit protocol), що став фактичним стандартом обробки розподілених транзакцій. Його вживання гарантує злагоджену зміну даних на декількох вузлах в рамках розподіленої (або, як її ще називають, глобальної) транзакції.

Незалежність від устаткування. Ця властивість означає, що вузлами розподіленої системи можуть виступати комп'ютери будь-яких моделей і виробників - від мейнфреймів до "персоналок".

Незалежність від операційних систем. Ця якість випливає з попереднього і означає різноманіття операційних систем, що управляють вузлами розподіленої системи.

Прозорість мережі. Доступ до будь-яких баз даних може здійснюватися по мережі. Спектр підтримуваних конкретною СУБД мережних протоколів не повинен бути обмеженням системи з розподіленими базами даних. Дана якість формулюється максимально широко - в розподіленій системі можливі будь-які мережні протоколи.

Незалежність від баз даних. Ця якість означає, що в розподіленій системі можуть мирно співіснувати СУБД різних виробників, і можливі операції пошуку і оновлення в базах даних різних моделей і форматів.

Виходячи з визначення Дейта, можна розглядати DDB як слабозв'язну мережну структуру, вузлами якої є локальні бази даних. Локальні бази даних ав-

тономні, незалежні і самовизначаються; доступ до них забезпечується СУБД, в загальному випадку від різних постачальників. Зв'язки між вузлами - це потоки тиражованих даних. Топологія ББВ варіюється в широкому діапазоні - можливі варіанти ієрархії, структур типу " зірка" тощо. В цілому топологія ББВ визначається географією інформаційної системи і спрямованістю потоків тиражування даних.

Порівняння безпеки і надійності розподілених і зосереджених систем.

Порівняємо зосереджену і розподілену системи з погляду надійності і безпеки.

Під надійністю розумітимемо властивість системи зберігати в часі у встановлених межах значення всіх параметрів, що характеризують здатність виконувати необхідні функції в заданих режимах і умовах вживання, технічного обслуговування і транспортування.

Багато систем не є абсолютно надійними, тобто властивість надійності системи має місце на кінцевому інтервалі часу, після закінчення якого відбувається відмова в роботі. Тривалість інтервалу безвідмовної роботи залежить від дуже великого числа чинників, передбачити які нереально, тому відмову звичайно вважають випадковою подією.

Надійність прийнято характеризувати вірогідністю відмови в роботі (або вірогідністю безвідмовної роботи) протягом певного відрізка часу. Іншою характеристикою надійності системи є середній час напрацювання на відмову.

Під безпекою розуміють стан захищеності системи від потенційно і реально існуючих загроз, або відсутність таких загроз. Система знаходиться в стані безпеки, якщо дія зовнішніх і внутрішніх чинників не приводить до погіршення або неможливості її функціонування. Загрози можуть бути різного роду, зокрема загроза фізичного руйнування.

У контексті створення та функціонування МЕП цікавими є інформаційні загрози. До них відносяться загрози отримання системою недостовірної вхідної інформації, спотворення внутрішньосистемної інформації, а також просочування інформації про функціонування системи.

Інформаційна безпека - стан захищеності інформаційного середовища суспільства, що забезпечує її формування, використовування і розвиток на користь громадян, організацій, держави.

Всі фізичні елементи будь-якої системи є потенційно ненадійними і уразливими з погляду безпеки.

Ненадійність елементів системи, що здійснюють переробку інформації, може полягати в повній відмові від переробки, в зміні функції (стабільному отриманні невірних результатів), в збоях (періодичному виникненні помилок).

Ненадійність елементів, що здійснюють передачу інформації, може полягати в повному припиненні передачі, в односторонньому припиненні передачі (для двонаправлених каналів), у виникненні випадкових помилок при передачі (перешкод).

Порушення безпеки елементів системи, що здійснюють оброблення інформації, може полягати як в навмисних діях зловмисників, що викликають відмову в роботі, зміна функцій (постійна або одинична), так і в несанкціонованому доступі до інформації (НСД).

Порушення безпеки елементів системи, що здійснюють передачу інформації, може полягати у втручанні, що призводить до повного припинення передачі, до одностороннього припинення передачі (для двонаправлених каналів), до заміни одних повідомлень на інші. Також може мати місце НСД.

Отже, проблеми надійності і безпеки багато в чому споріднені. Вони пов'язані з втручанням у функціонування системи. Відмінність полягає в тому, що ненадійність визначається фізичними, природними чинниками і не пов'язана з чиєюсь метою. Небезпечність визначається, в основному, "людським чинником" - наявністю зловмисників і/або безтурботних співробітників. Але одна з проблем безпеки - просочування інформації при несанкціонованому доступі - не має аналога серед проблем надійності.

Кожний чинник з погляду надійності, якщо його розглядати ізольовано, виконує позитивну або негативну роль. Наприклад, збільшення кількості ненадійних елементів в системі за інших рівних умов виконує негативну роль. Під іншими рівними умовами тут розуміється незмінність архітектури (з'єднань і розподілу функцій) системи, незмінність параметрів елементів тощо. Якщо ж архітектуру змінити, наприклад, застосовувати додаткові елементи для дублювання (резервування), то надійність, навпаки, підвищується.

Лінії зв'язку з об'єктами в зосередженій системі мають більшу, ніж в розподіленій системі, довжину. Це, поза сумнівом, негативний чинник. Звичайно із збільшенням довжини лінії збільшується кількість перешкод, збільшується вартість передачі, збільшуються можливості зловмисників по зніманню інформації або по її спотворенню. Цей загальний висновок не залежить від природи лінії зв'язку - дротовий, оптоволоконний, радіозв'язок, зв'язок з використанням супутників тощо. Конструкція лінії зв'язку визначає тільки вид залежності та числові характеристики параметрів надійності і безпеки.

При проектуванні системи завжди доводиться шукати компроміс між різними чинниками, з математичної точки зору - вирішувати оптимізаційну задачу. Її сутність у тому, що можна забезпечити будь-яку необхідну надійність системи, але збільшення надійності супроводжується збільшенням її собівартості. Причому збільшується як вартість проектування і реалізації, так і вартість експлуатації (функціонування).

Те ж можна сказати і про безпеку. Заходи щодо безпеки мають ще одну негативну рису: спричинення додаткових незручностей користувачам системи, мінімальне з яких - необхідність введення логіна та пароля.

Разом з архітектурою технічних засобів для відмовостійкості розподіленої системи велику роль має методика побудови алгоритмів. Вона повинна бути розрахована на можливі збої або розузгодження в роботі вузлів системи (при програмуванні в зосереджених системах можливість збою звичайно не враховується).

Висновки. Розглянуті особливості технологій проектування МІС і МЕП на сучасному етапі. Виділені обов'язкові етапи проектування, що пов'язані з аутентифікацією користувачів, забезпеченням конфіденційності інформації, підтримкою ЕЦП, забезпеченням селективного доступу до інформації тощо. Показано, що в жодному світовому проекті не приділено належної уваги коректному вирішенню зазначених проблем.

Досліджені питання сумісності існуючих БД з МЕП. Показано, що необхідними елементами досягнення сумісності є єдність структури медичних документів; уніфікація класифікацій діагнозів, станів здоров'я, архетипів, шаблонів та принципів аналізу інформації; стандартів медичних дій в усіх медичних закладах; впровадження стандартизованого апаратного та програмного забезпечення, а також синхронізація з іншими серверами.

Література

1. Браун П. Приватность в век терабайтов и терроризма / Питер Браун // В мире науки. - 2008. - № 12. - С. 20-21.
2. Ванчаков Н. Б. Практические основы защиты информации. Технические методы и средства : производственно-практическое издание / Н. Б. Ванчаков, 3. А. Н. Григорьев. - Калининград : КЮИ МВД России, 2000. - 198 с.
3. Голубев Д. Л. Распределенные центры обработки данных / Голубев Д. Л. // Jet Info. - 2006. - № 5. - С. 3-16.
4. Горбатов В. С. Основы технологии PKI / В. С. Горбатов, О. Ю. Полянская. - М. : Горячая линия - Телеком, 2004 - 246 с.
5. Гребнев В. Направление правового регулирования вопросов использования ЕЦП / В. Гребнев, А. Скиба // Правове, нормативне та метрологічне забезпечення систем захисту інформації в Україні. - 2003. - N° 6. - С. 6-10.
6. ДСТУ 3396 0-96 Захист інформації. Технічний захист інформації. Основні положення.
7. ДСТУ 3396.2-97 Захист інформації. Технічний захист інформації. Терміни та визначення.
8. Закон України "Про інформацію" від 02.10.1992 № 2657-XII.
9. Закон України "Про захист інформації в автоматизованих системах" від 05.07.1994 № 80/94-ВР .
10. Закон України «Про електронний цифровий підпис» від22.05.2003 № 852-IX.
11. Меняев М. Ф. Информационные технологии управления : учебное пособие. Кн. 3 : Системы управления организацией / Меняев М. Ф. - М. : Омега-Л, 2003. - 462 с.
12. Методы и средства обработки информации : труды Третьей Всерос. науч .-техн. конф., 6-8 октября 2009 г, Москва / МОН РФ, РАН [и др.]. - М. : МГУ имени М. В. Ломоносова, 2003. - 481 с.
13. Миков А. И. Система оперирования распределёнными имитационными моделями сетей телекоммуникаций / Миков А. И., Замятина Е. Б., Фатыхов А. Х. // Методы и средства обработки информации : труды Первой Всерос. науч.-техн. конф., 1-3 октября 2003 г., Москва / МОН РФ, РАН [и др.]. - М. : МГУ имени М. В. Ломоносова, 2003. - С. 437-443.
14. Мялковский Д. Организационно-технические вопросы построения и функционирования национальной системы ЭЦП / Д. Мялковский, А. Скиба // Правове, нормативне та метрологічне забезпечення систем захисту інформації в Україні. - 2003. - №> 6. - С. 11-15.
15. Наказ ДСТСЗІ СБ України №> 50 від 10.05.06 "Правила посиленої сертифікації".
16. НД ТЗІ 1.1-002-99 Загальні положення щодо захисту інформації в комп'ютерних системах від несанкціонованого доступу.
17. НД ТЗІ 1. 1-003-99 Термінологія в галузі захисту інформації в комп'ютерних системах від несанкціонованого доступу.
18. НД ТЗІ 2.5-004-99 Критерії оцінки захищеності інформації в комп'ютерних системах від несанкціонованого доступу.
19. НД ТЗІ 3.6-001-2000 Технічний захист інформації. Комп'ютерні системи. Порядок створення, впровадження, супроводження та модернізації засобів технічного захисту інформації від несанкціонованого доступу.
20. Окинавская хартия глобального информационного общества (Окинава, 22 июля 2000 года) // Дипломатический вестник. - 2000. - №> 8. - С. 51-56.
21. Олифер В. Г. Сетевые операционные системы : учебное пособие / В. Г. Олифер, Н. А. Олифер. - СПб. : Питер, 2007. - 538 с.
22. Панасенко С. П. Основы криптографии для экономис-

тов : учеб. пособие для вузов / Панасенко С. П., Батура В. П., Гагарина Л. Г. - М. : Финансы и статистика, 2005. - 174 с.

23. Постанова КМУ від 13.06.2004 №№ 903 „Порядок акредитації центру сертифікації ключів".

24. Постанова КМУ від 28.10.2004 №> 1454 „Порядок обов'язкової передачі документованої інформації".

25. Правила посиленої сертифікації, затверджені наказом ДСТСЗІ СБ України від 10.05.06 №> 50.

26. Скиба В. Ю. Руководство по защите от внутренних угроз информационной безопасности / В. Ю. Скиба, В. А. Курбатов. - СПб. : Питер, 2008. - 321 с.

27. Смит Р. Э. Аутентификация: от паролей до открытых ключей / Ричард Э. Смит. - М. : Вильямс, 2002. - 432 с.

28. Танненбаум Э. Компьютерные сети / Танненбаум Э. - СПб. : Питер, 2002. - 992 с.

29. Фергюсон Н. Практическая криптография / Н. Фергюсон, Б. Шнайер. - М. : Вильямс, 2005. - 424 с.

30. Kuhn D. R. Introduction to Public Key Technology and the Federal PKI Infrastructure. NIST SP 800-32 / D. R. Kuhn, C. H. Vincent, W. P. Polk, S. J. Chang // National Institute of Standards and Technology : U.S. Government publication. - 2001. - 54 p.

31. Lee A. Guideline for Implementing Cryptography in the Federal Government, NIST SP 800-21 / Lee A. // National Institute of Standards and Technology, 1999. - Режим доступу: http://csrc.nist. gov/publications/nistpubs/800-21/800-21.pdf,

32. Lyons-Burke K. Federal Agency Use of Public Key Technology for Digital Signatures and Authentication. NIST Special Publication 800-25 / Lyons-Burke K. - 2000. - Режим доступу: http ://csrc. nist. gov/publications/nistpubs/800-12.

33. Mitchell C. PKI standards. Information Security Technical Report, 5 / Chris Mitchell // London : Institute of Electrical Engineers, 2000. - 17 p.