

УДК 004.43(031)

Защита информации в медицинских информационных системах: врачебная тайна и современные информационные технологии

В. В. Домарев

Аппарат Совета национальной безопасности и обороны Украины, Киев

Резюме

Рассматриваются вопросы организации защиты конфиденциальной информации в медицинских информационных системах.

Ключевые слова: защита, конфиденциальная информация, медицинская информационная система.

Клин. информат. и Телемед. 2004. Т.1. №2. с.147–154

Введение

Информацию сегодня без преувеличения можно отнести к одному из решающих ресурсов развития медицинской сферы. Однако, в определенных случаях, информация может использоваться не только во благо, но и во вред интересам личности, общества и государства. Речь идет не только о правах граждан, юридических лиц и государства на свободное получение, распространение и использование информации, но и о необходимости защиты конфиденциальной информации и интеллектуальной собственности. Поэтому роль информационной безопасности в системе здравоохранения не только существенно возрастает, но и выходит на первый план.

Известно много случаев, когда разглашение или искажение сведений, составляющих врачебную тайну, приводило к непредсказуемым последствиям. Примером может послужить скандал в ходе предвыборной кампании на пост Президента Украины.

Актуальность проблем защиты информации в медицине и необходимость их решения сегодня уже очевидна. Однако, существующее положение дел в этой сфере можно выразить словами известного сатирика: «Все знают, что так не должно быть и все знают, как должно быть, однако, как перейти от одного к другому, не знает никто...»

Сложность решения задач защиты информации в медицинских информационных системах (МИС) характеризуется следующими факторами:

- переход на безбумажную технологию требует обеспечения юридической значимости электронных документов (при-

няты Законы Украины об электронных документах и электронном документо-обороте (N 851-IV) и об электронной цифровой подписи (N 852-IV), см. журнал «Клиническая информатика и Телемедицина», №1, 2004 г.);

- распределенное использование ресурсов МИС требует обеспечения безопасности информации на уровне разграничения доступа;
- ряд электронных документов требуют обеспечения безопасности на уровне скрытия смыслового содержания, а в некоторых случаях и недопущения несанкционированного размножения;
- работа в территориально-распределенной сети предъявляет высокие требования к аутентичности информации и источников данных;
- предъявляются высокие требования к целостности программного обеспечения (системного и прикладного), систем управления базами данных и целого ряда электронных документов (справочных, статистических, отчетных).

Медицинская информационная система как объект защиты

Медицинская информационная система (МИС) — это сложная, распределенная в пространстве система, состоящая из множества сосредоточенных (локальных) подсистем (информационных узлов), располагающих программно-аппаратны-

ми средствами реализации информационных технологий и множества средств, обеспечивающих соединение и взаимодействие этих подсистем с целью предоставления территориально удаленным пользователям широкого набора услуг из сферы информационного обслуживания.

Другими словами, МИС — организационно-техническая система, реализующая информационные технологии и предусматривающая аппаратное, программное и другие виды обеспечения, а также соответствующий персонал.

На основании анализа 40-летнего мирового опыта разработана концепция информационной системы здравоохранения (ИСЗ) [1].

Характеристики, влияющие на безопасность информации.

Рассматривая МИС с позиции защиты, полезно обратить внимание на следующие характеристики:

- категории обрабатываемой в МИС информации, высший гриф секретности информации;
- общая структурная схема и состав МИС (перечень и состав оборудования, технических и программных средств, пользователей, данных и их связей, особенности конфигурации и архитектуры и т.п.);
- тип МИС (одно-, или многопользовательская система, открытая сеть, одно-, либо многоуровневая система и т.п.);
- объемы основных информационных массивов и потоков;
- продолжительность процедуры восстановления работоспособности после сбоев, наличие средств повышения надежности и живучести и т.п.;
- технические характеристики используемых каналов связи (пропускная способность, типы кабельных линий, виды связи с удаленными сегментами МИС и пользователями и т.п.);
- территориальное расположение компонентов МИС, их физические параметры и т.п.;
- наличие других особых условий эксплуатации и др.

С точки зрения защиты информации типовые компоненты МИС рассматриваются как объекты защиты. К ним относятся:

Рабочие места пользователей и персонала МИС.

Можно выделить следующие типы рабочих мест:

- РМ пользователя дисплейного (непрограммируемого) типа с визуальным отображением информации (терминалы);
- РМ пользователя (программируемый ПК), который может функционировать в режиме обмена информацией с сопряженной ЭВМ и в автономном режиме;
- РМ оператора, предназначенное для обслуживания серверов;

• РМ программиста, предназначенное для отладки программы;

• РМ администратора, предназначенное для управления и контроля за использованием каких-либо ресурсов МИС, например, администраторы сети, базы данных, службы безопасности.

Компоненты средств связи (коммуникационные компоненты):

- межсетевые мосты (шлюзы, центры коммутации пакетов, коммуникационные ЭВМ) — элементы, обеспечивающие соединение нескольких сетей передачи данных, либо нескольких сегментов одной и той же сети, имеющих различные протоколы взаимодействия;
- каналы связи с узлами коммутации;
- аппаратура связи типа модем (модулятор-демодулятор), осуществляющая преобразование цифровых данных в электрические сигналы для передачи по линиям связи и обратное преобразование на приеме при обмене между удаленными друг от друга ЭВМ;
- аппаратура связи типа мультиплексор передачи данных, обеспечивающая сопряжение нескольких источников (например, нескольких ЭВМ) для передачи информации по одному каналу связи;
- каналы связи, выделенные и коммутируемые.

Вспомогательные элементы МИС:

- помещения, где расположены серверы;
- помещения, в которых размещены устройства предварительной подготовки данных;
- хранилище носителей информации;
- хранилища документов на бумажных носителях;
- служебные помещения пользователей и персонала МИС.

ЭВМ различного функционального назначения:

- центральная ЭВМ (мейнфрейм), которая осуществляет основные процедуры обработки информации в МИС;
- сервер или Host машина, предназначенная для реализации функций хранения, печати данных, обслуживания рабочих станций сети и т.п.;
- ЭВМ с функциями связанной машины, шлюза, моста между сетевыми структурами.

Проблемы организации защиты врачебной тайны

Большая концентрация массивов медицинской информации, отсутствие элементарного контроля за ее сохранностью

и относительно низкий уровень надежности технических средств вызывают серьезную тревогу в обеспечении сохранности информации.

В процессе эксплуатации МИС, накапливаемая и обрабатываемая информация является достаточно уязвимой, подверженной как разрушению, так и несанкционированному использованию. А большое число различных компонентов, операций, ресурсов и объектов МИС создает весьма привлекательную среду для различного рода вторжений и несанкционированных действий.

Основными проблемами в процессе защиты информации в МИС является:

- предотвращение утечки, хищения, утраты, искажения, подделки информации;
- предотвращение угроз безопасности информации личности, общества, государства;
- предотвращение несанкционированных действий по уничтожению, модификации, искажению, копированию, блокированию информации;
- предотвращение различных форм незаконного вмешательства в информационные ресурсы и информационные системы;
- обеспечение правового режима использования документированной информации как объекта собственности;
- защита конституционных прав граждан на сохранение личной тайны и конфиденциальности персональных данных, имеющихся в информационных системах;
- сохранение врачебной тайны, конфиденциальности документированной информации в соответствии с законодательством;
- гарантия прав субъектов в информационных процессах и при разработке, производстве и применении информационных систем, технологий и средств их обеспечения.

Следует признать, что сейчас в качестве базового уровня МИС применяются обычные (бытовые) ПК, которые в последующем объединяют с помощью дополнительного оборудования в локальные и распределенные вычислительные сети. Для защиты информации при таком подходе приходится тратить неоправданно большие средства на организацию защиты ценной информации, обрабатываемой с помощью дешевой техники. А в условиях, когда пользователи имеют доступ к нескольким серверам и обладают правами удаленной регистрации, защита настолько усложняется, что ее создание становится не по карману даже мощным фирмам и крупным медицинским центрам.

Возможно ли в таких условиях организовать защиту информации? Ответить

на этот вопрос не просто поскольку современные тенденции развития информационных технологий, делают ставку именно на открытость информационных технологий.

Угрозы информации, содержащей врачебную тайну

Наиболее распространенными путями утечки информации являются:

- хищение носителей информации и документов, получаемых в результате работы информационных систем;
- копирование информации на ПК;
- несанкционированное подключение к аппаратуре и линиям связи;
- перехват электромагнитных излучений в процессе обработки информации.

Кроме того, необходимость защиты ресурсов, программ и информации в компьютерной информационной системе от несанкционированного доступа и использования определяется наличием следующих угроз.

Системный программист — нарушает защиту. Обеспечивает себе право входа в систему. Может выявлять и обходить элементы систем защиты.

Инженер по эксплуатации — нарушает защиту технических средств. Использует автономные утилиты для доступа к файлам и для входа в систему.

Рабочие станции — наиболее доступные компоненты сетей и именно с них могут быть предприняты наиболее многочисленные попытки несанкционированных действий. С рабочих станций осуществляется управление процессами обработки информации, запуск программ, ввод и корректировка данных, на дисках рабочих станций могут размещаться важные данные и программы обработки.

Серверы нуждаются в особой защите. Одни — как концентраторы больших объемов информации, вторые — как элементы, в которых осуществляется преобразование данных при согласовании протоколов обмена в различных участках сети. Здесь злоумышленники, прежде всего, будут искать возможности повлиять на работу различных подсистем, используя недостатки протоколов обмена и средств разграничения удаленного доступа к ресурсам и системным таблицам. При этом, используются все воз-

можности и средства, вплоть до специальных программных закладок для преодоления системы защиты.

Каналы и средства связи. В силу большой пространственной протяженности линий связи через неконтролируемую территорию, практически всегда имеется возможность подключения к ним, либо вмешательства в процесс передачи данных со стороны злоумышленников.

Обработка информации. Возможные утечки, нарушения целостности, истинности и сохранности информации происходят в результате случайных или преднамеренных неправильных (не разрешенных) действий пользователя (санкционированного или несанкционированного для работы в данной МИС).

Можно привести и другие угрозы и каналы утечки информации, имеющие место в процессе функционирования МИС.

Степень защиты информации от неправомерного доступа и противозаконных действий зависит от качества разработки организационных и технических мер, направленных на исключение:

- доступа к аппаратуре обработки информации;
- бесконтрольного выноса персоналом различных носителей информации;
- несанкционированного введения данных в память, изменения или стирания хранящейся в ней информации;
- незаконного пользования системами обработки информации и полученными данными;
- доступа в системы обработки информации посредством самодельных устройств;
- неправомерной передачи данных по каналам связи из информационно-вычислительного центра;
- бесконтрольный ввод данных в систему;
- обработка данных по заказу без соответствующего требования заказчика;
- неправомерное считывание, изменение или стирание данных в процессе их передачи или транспортировки носителей информации.

Проблемы внедрения комплексных систем защиты

Понятие системности заключается не просто в создании соответствующих механизмов защиты, а представляет собой регулярный процесс, осуществля-

емый на всех этапах жизненного цикла МИС. При этом, все средства, методы и мероприятия, используемые для защиты информации, объединяются в целостный единый механизм — систему защиты.

К сожалению, необходимость системного подхода к вопросам обеспечения безопасности информационных технологий пока еще не находит должного понимания у владельцев современных МИС.

Сегодня стало очевидным, что специалисты из самых разных областей знаний, в том числе и медицинских, так или иначе, вынуждены заниматься вопросами обеспечения информационной безопасности (ИБ). Это обусловлено тем, что в ближайшие лет сто нам придется жить в обществе (среде) информационных технологий, куда переключаются все социальные проблемы человечества, в том числе и вопросы безопасности.

Каждый из указанных специалистов по-своему решает задачу обеспечения информационной безопасности и при этом находит свои совершенно правильные решения. Однако, как показывает практика, совокупность таких правильных решений не дает в сумме положительного результата — система безопасности в общем и целом работает неэффективно.

Если собрать всех специалистов вместе, то при наличии у каждого из них огромного опыта и знаний, создать СИСТЕМУ информационной безопасности так и не удастся. Такое положение дел обусловлено отсутствием системного подхода, который определил бы взаимные связи (отношения) между существующими понятиями, определениями, принципами, способами и механизмами защиты.

Специфическими особенностями решения задачи создания систем защиты являются:

- неполнота и неопределенность исходной информации о составе МИС и характерных угрозах;
- многокритериальность задачи, связанная с необходимостью учета большого числа частных показателей (требований) системы защиты информации (СЗИ);
- наличие как количественных, так и качественных показателей, которые необходимо учитывать при решении задач разработки и внедрения СЗИ;
- невозможность применения классических методов оптимизации.

Решение задачи обеспечения информационной безопасности во многом зависит от разработки модели представления системы защиты, которая на основе научно-методического аппарата, позволяла бы решать задачи создания, использования и оценки

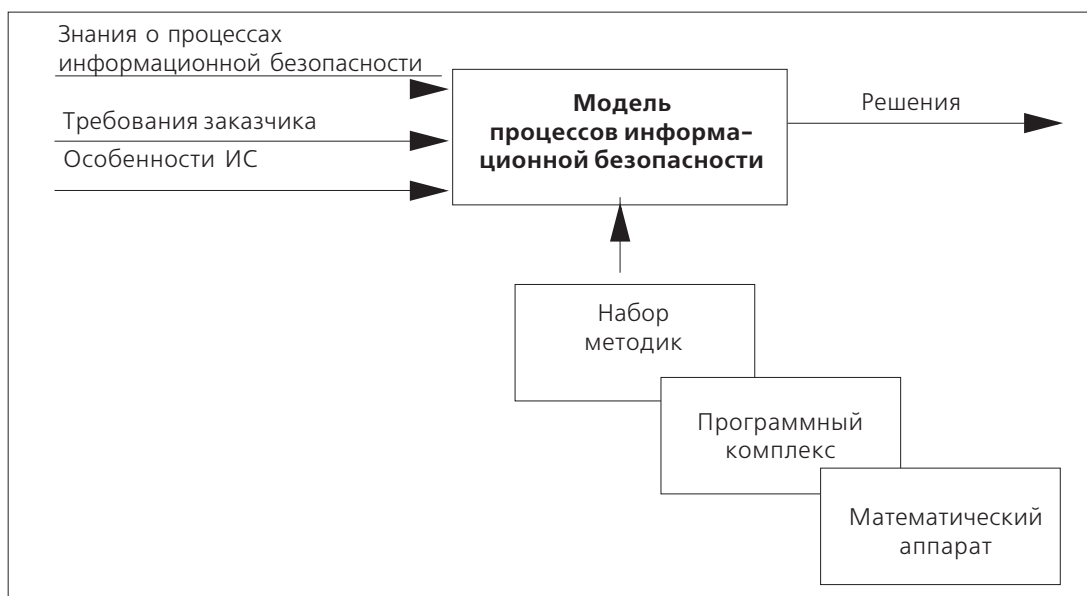


Рис. 1. Упрощенное представление модели информационной безопасности.

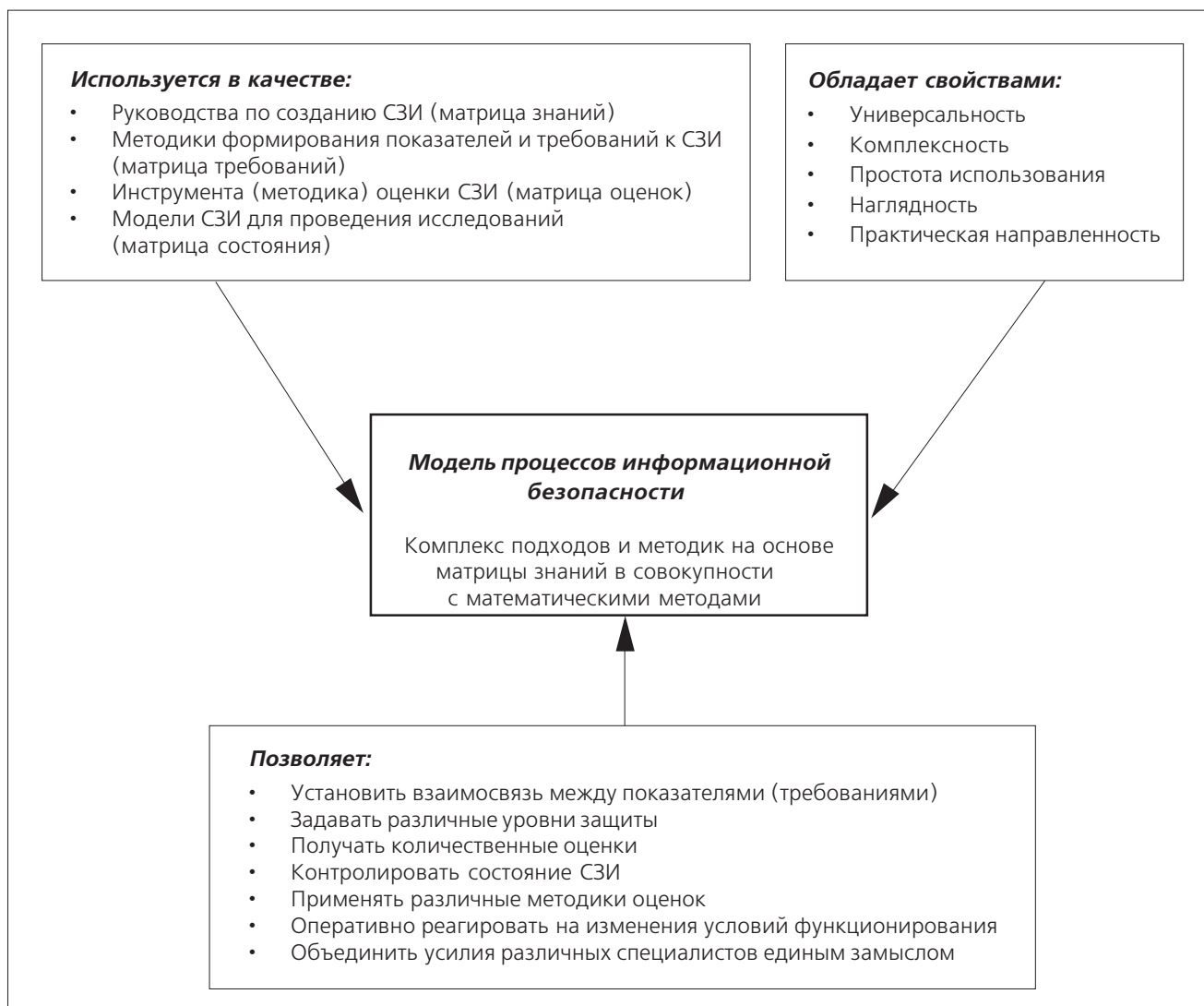


Рис. 2. Свойства модели информационной безопасности.

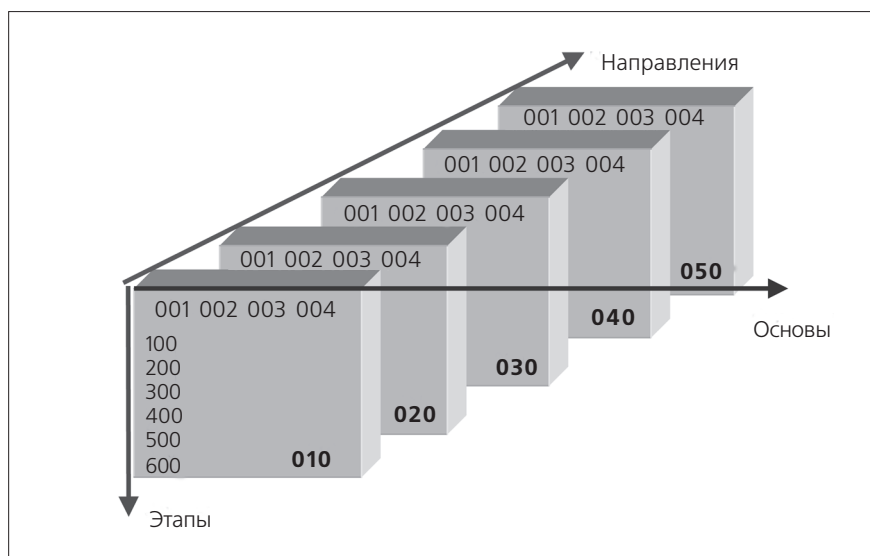


Рис. 3. Группы составляющих модели информационной безопасности.

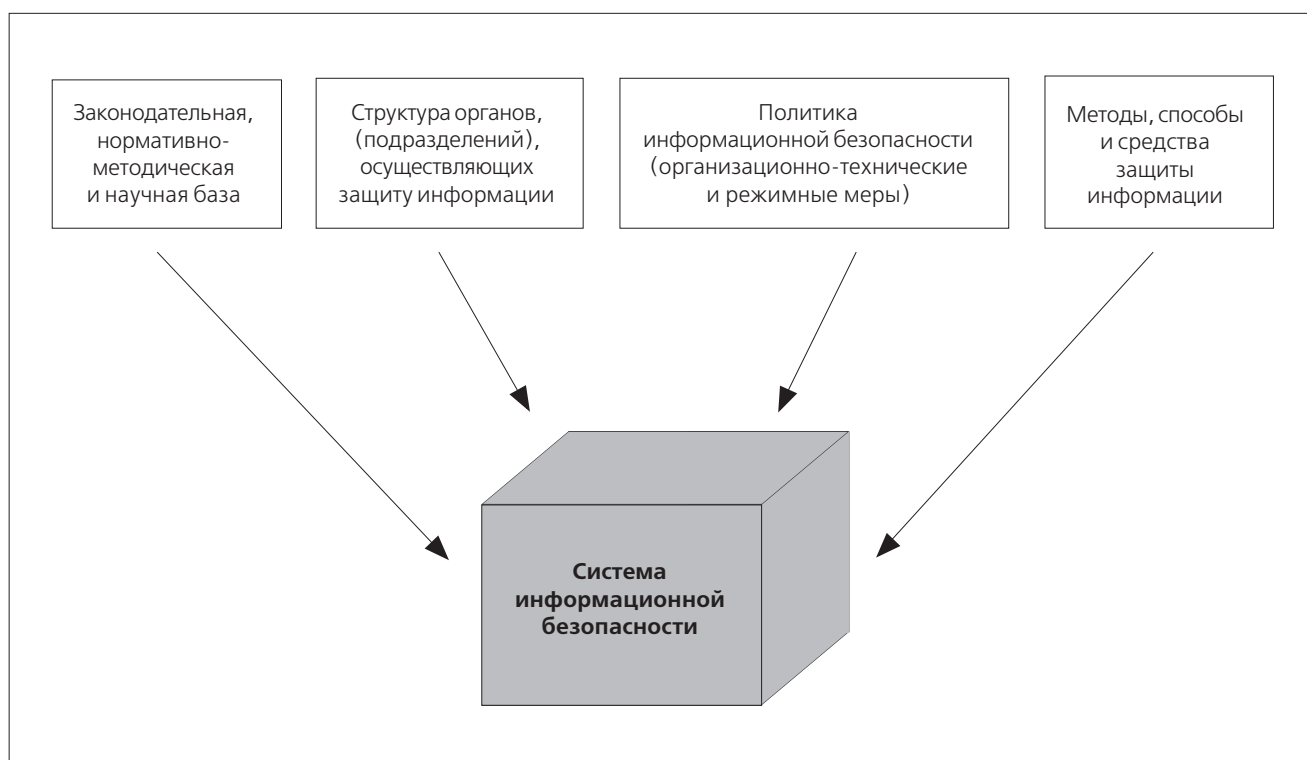


Рис. 4. Основы информационной безопасности.

эффективности СЗИ для проектируемых и существующих МИС.

Основной задачей такой модели является научное обеспечение процесса создания системы информационной безопасности за счет правильной оценки эффективности принимаемых решений и выбора рационального вариан-

та технической реализации системы защиты информации.

В упрощенном виде модель СЗИ представлена на рис.1.

Требования к модели:

Такая модель должна удовлетворять следующим требованиям (рис. 2.):

Использоваться в качестве:

- руководства по созданию СЗИ;
- методики формирования показателей и требований к СЗИ;
- инструмента (методика) оценки СЗИ;
- модели СЗИ для проведения исследований (матрица состояния).

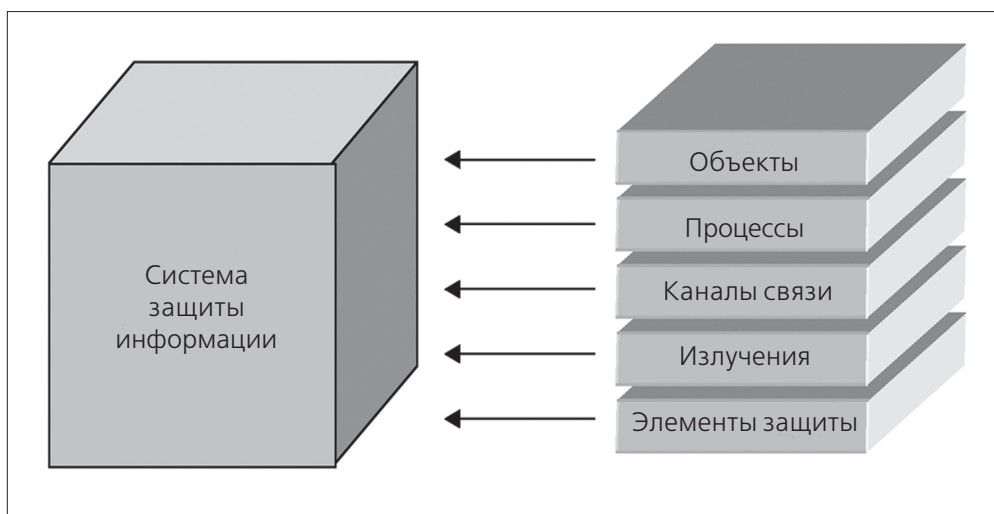


Рис. 5. Направления информационной безопасности.

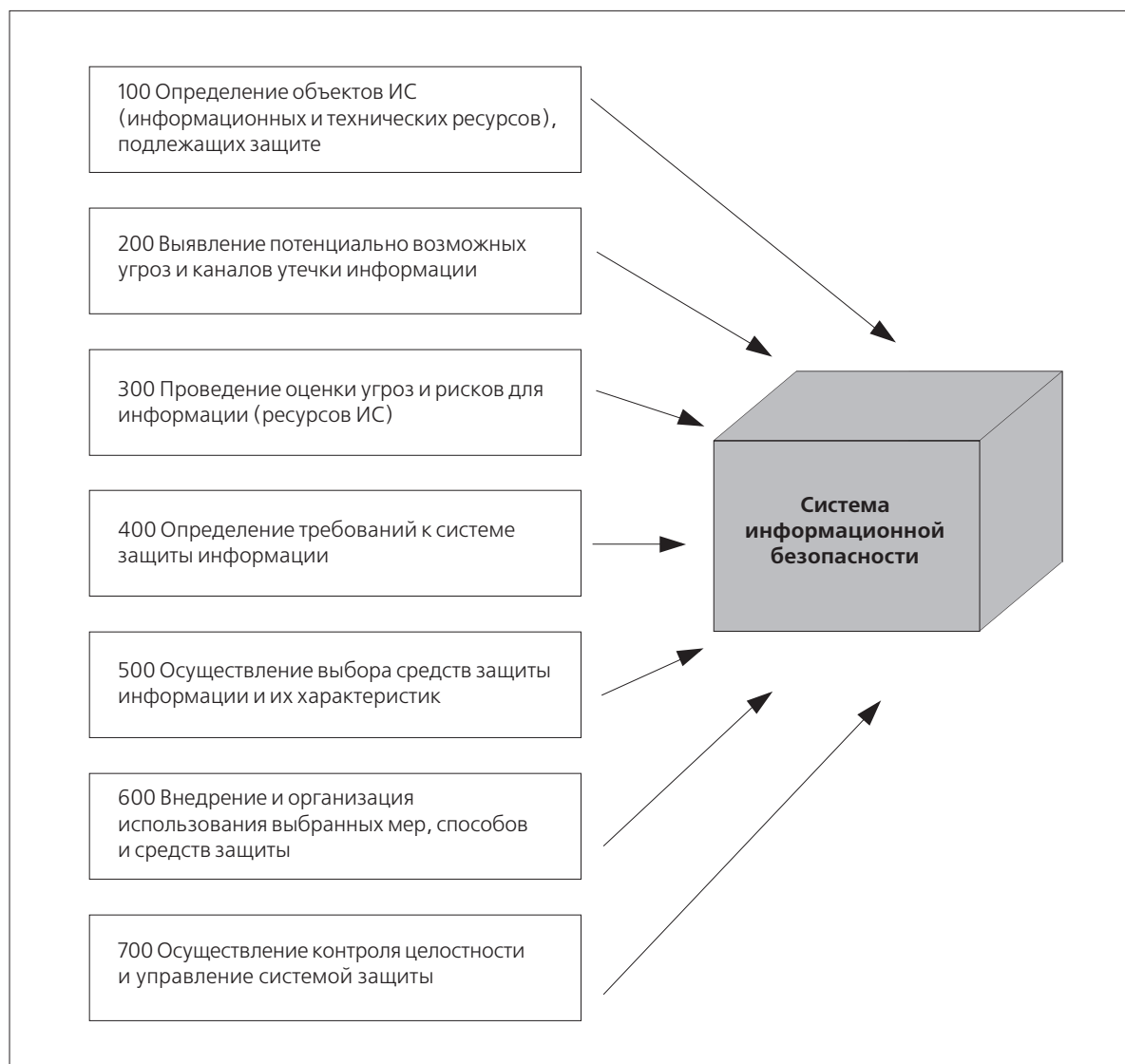


Рис. 6. Этапы создания систем защиты информации.

Обладать свойствами:

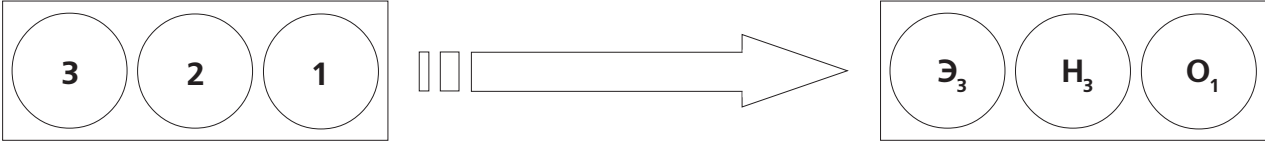
- универсальность;
- комплексность;
- простота использования;
- наглядность;
- практическая направленность;
- быть самообучаемой (возможность наращивания знаний);

• функционировать в условиях высокой неопределенности исходной информации.

Позволять:

- установить взаимосвязь между показателями (требованиями);
- задавать различные уровни защиты;

- получать количественные оценки;
- контролировать состояние СЗИ;
- применять различные методики оценок;
- оперативно реагировать на изменения условий функционирования;
- объединить усилия различных специалистов единым замыслом.



300 – Проведение оценки уязвимости и рисков (показатель №3 блока «ЭТАПЫ»);
020 – Защита процессов программ (показатель №2 блока «НАПРАВЛЕНИЯ»);
001 – Нормативная база (показатель №1 блока «ОСНОВЫ»).

Этапы	Основа >>>	010				020				003				004				005			
		Защита объектов ИС				Защита процессов и программ				Защита каналов связи				ПЭМИ				Управление системой защиты			
		База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства	База	Структура	Меры	Средства
		011	012	013	014	021	022	023	024	031	032	033	034	041	042	043	044	051	052	053	054
100	Определение информации, подлежащей защите																				
200	Выявление угроз и каналов утечки информации																				
300	Проведение оценки уязвимости и рисков																				
400	Определение требований к СЗИ																				
500	Осуществление выбора средств защиты																				
600	Внедрение и использование выбранных мер и средств																				
700	Контроль целостности и управление защитой																				

Рис. 7. Матрица защиты информации.

Описание подхода к формированию модели информационной безопасности

Как составить такое представление об информационной безопасности, чтобы охватить все аспекты проблемы? Человек получает наиболее полное представление об интересующем его явлении, когда ему удастся рассмотреть это нечто неизвестное со всех сторон, в трехмерном измерении. Исходя из этого, предлагается рассмотреть три «координаты измерений» — три группы составляющих модели ИБ (рис. 3.).

1. Из чего состоит (ОСНОВЫ).
2. Для чего предназначена (НАПРАВЛЕНИЯ).

3. Как работает (ЭТАПЫ).

В качестве ОСНОВ (рис. 4.) или составных частей СИСТЕМЫ рассматриваются:

- законодательная, нормативно-правовая и научная база;
- структура и задачи органов (подразделений), обеспечивающих безопасность информации;
- организационно-технические и режимные меры и методы (политика информационной безопасности);
- программно-технические способы и средства.

Далее, руководствуясь принципом «разделяй и властвуй», выделяются основные НАПРАВЛЕНИЯ обеспечения безопасности информационных технологий (рис. 5.):

- защита объектов информационных систем;
- защита процессов, процедур и программ обработки информации;
- защита каналов связи;
- подавление побочных электромагнитных излучений;
- управление системой защиты.

Проведенный анализ существующих методик (последовательностей) работ по созданию СЗИ позволяет выделить ЭТАПЫ создания систем защиты (рис. 6.):

- определение информационных и технических ресурсов, а также объектов МИС(!) подлежащих защите;

- выявление множества потенциально возможных угроз и каналов утечки информации;
- проведение оценки уязвимости и рисков информации (ресурсов МИС) при имеющемся множестве угроз и каналов утечки;
- определение требований к системе защиты информации;
- осуществление выбора средств защиты информации и их характеристик;
- внедрение и организация исполнения выбранных мер, способов и средств защиты;
- осуществление контроля целостности и управление системой защиты.

Для наглядности и простоты использования указанной модели применяется так называемая матрица знаний (рис. 7.) Содержание каждого из элементов МАТРИЦЫ описывает взаимосвязь составляющих системы защиты информации (СЗИ). Комплекс вопросов создания и оценки СЗИ рассматривается путем анализа различных групп элементов матрицы, в зависимости от решаемых задач. Например, отдельно можно оценить качество нормативной базы, или защищенность каналов связи, или качество мероприятий по выявлению каналов утечки информации и т.д. В общем случае основным содержанием элементов матрицы является ответ на вопрос: «Какие из мероприятий по защите информации, кем и как выполняются?».

Литература

1. Майоров О. Ю., Белов Л.Б., Неженский С. А. Информационные системы здравоохранения (госпитальные информационные системы) — дань моде или необходимость (технико-экономическое обоснование внедрения программного комплекса «С-Госпиталь®»). // *Клин. информат. и Телемед.*, 2004, т.1, с. 1–12.
2. Домарев В. В. Защита информации и безопасность компьютерных систем. — К.: ТИД ДиаСофт, 1999. — 480 с.
3. Домарев В. В. Безопасность информационных технологий. Методология создания систем защиты. — К.: ТИД ДиаСофт, 2002. — 688 с.
4. Домарев В. В., «Безопасность информационных технологий. Системный подход», К.: ТИД ДиаСофт, 2004. — 900 с.

Интернет-ресурс

1. <http://www.domarev.kiev.ua>

Protection of the information in medical information systems: medical secret and modern information technologists

V. V. Domarev

The Department of National Safety and Defenses Council of Ukraine, Kiev

Abstract

The questions of organization of protection of the confidential information in medical information systems are considered.

Keywords: protection, confidential information, medical information system.

Захист інформації в медичних інформаційних системах: лікарська таємниця і сучасні інформаційні технології

В. В. Домарев

Апарат Ради національної безпеки і оборони України, Київ

Резюме

Розглядаються питання організації захисту конфіденційної інформації в медичних інформаційних системах.

Ключові слова: захист, конфіденційна інформація, медична інформаційна система.

Переписка

к.т.н. В. В. Домарев

Апарат Совета национальной безопасности и обороны Украины
ул. Каменева, 8
Киев, 01133, Украина,
e-mail: dvv@rainbow.gov.ua
<http://www.domarev.kiev.ua>