УДК 004.422

В.Д. Зыков

Структура программного обеспечения системы защиты рабочего места обработки персональных медицинских данных

Рассмотрена структура программного обеспечения системы защиты рабочего места обработки персональных медицинских данных, а также требования по защите персональных медицинских данных в медицинских учреждениях.

Современные информационные технологии играют важнейшую роль в медицинской отрасли, но одной из наиболее серьезных проблем, препятствующих их повсеместному внедрению, является обеспечение защиты информации, в том числе защиты персональных данных граждан и сведений составляющих медицинскую тайну, – персональных медицинских данных. Актуальность проблемы защиты персональных медицинских данных сегодня не вызывает сомнений. Кибертерроризм, доступ физических лиц к базам персональных данных усиливают риск вторжения в сферу частной жизни и нарушения права на ее неприкосновенность. Защита персональных медицинских данных является одной из наиболее острых проблем в информатизации организаций медицинской области (таблица).

Требования Закона «О персональных данных»

Номер статьи и пункта	Содержание
Ст. 5, ч. 2, Ст. 21, ч. 4	Хранение приватных сведений должно осуществляться не дольше, чем этого требуют цели их обработки, а по достижении целей обработки или утраты необходимости в их достижении персональная информация должна быть уничтожена. Срок, в течение которого уже ставшие ненужными персональные данные должны быть уничтожены, устанавливается в три рабочих дня
Ст. 19, ч. 1	Оператор при обработке персональных данных обязан принимать необходимые организационные и технические меры, в том числе использовать шифровальные (криптографические) средства, для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения персональных данных, а также от иных неправомерных действий
Ст. 19 ч. 4	Использование и хранение биометрических персональных данных вне информационных систем персональных данных могут осуществляться только на таких материальных носителях информации и с применением такой технологии ее хранения, которые обеспечивают защиту этих данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, распространения

Согласно данным условиям необходимо выполнение следующих требований по защите персональных данных:

- идентификация и аутентификация;
- контроль доступа;
- конфиденциальность;
- контроль целостности;
- использование шифровальных (криптографических) средств [2].

Предлагаются комплексное решение по защите персональных медицинских данных в качестве базовой составляющей, использующее инфраструктуру открытых ключей и реализация следующих услуг по защите информации:

- Идентификация и аутентификация обеспечиваются сертификатами открытых ключей.
- Конфиденциальность и контроль доступа обеспечивается шифрованием.
- Контроль целостности обеспечивается электронной цифровой подписью.
- Неотказуемость – услуга, предотвращающая успешный отказ от предшествующих действий пользователя, обеспечивается использованием ЭЦП и сертификата открытого ключа.
- Журналирование.
- Гарантированное удаление остаточной информации [2].

В предлагаемом случае в комплексное решение по защите персональных медицинских данных на основе инфраструктуры открытых ключей входят следующие организационно-технические компоненты (рис. 1):

- Клиентские рабочие места, на которых осуществляется сбор, обработка, хранение и передача персональных медицинских данных.
- Оператор связи, обеспечивающий выполнение функций передачи, промежуточного хранения персональных медицинских данных и информационной поддержки документооборота.

- Автоматизированная информационная система, включающая программно-аппаратные средства защиты информации на основе инфраструктуры открытых ключей.
- Удостоверяющий центр, обеспечивающий выполнение функций выпуска и управления сертификатами открытых ключей пользователей.
- Защищенные средства для хранения цифровых сертификатов и закрытых ключей пользователей. В качестве таких средств могут выступать USB-ключи, смарт-карты, внешние носители и др.
- Каналы передачи информации.

Автоматизированная информационная система в данном случае будет иметь клиент-серверную архитектуру.

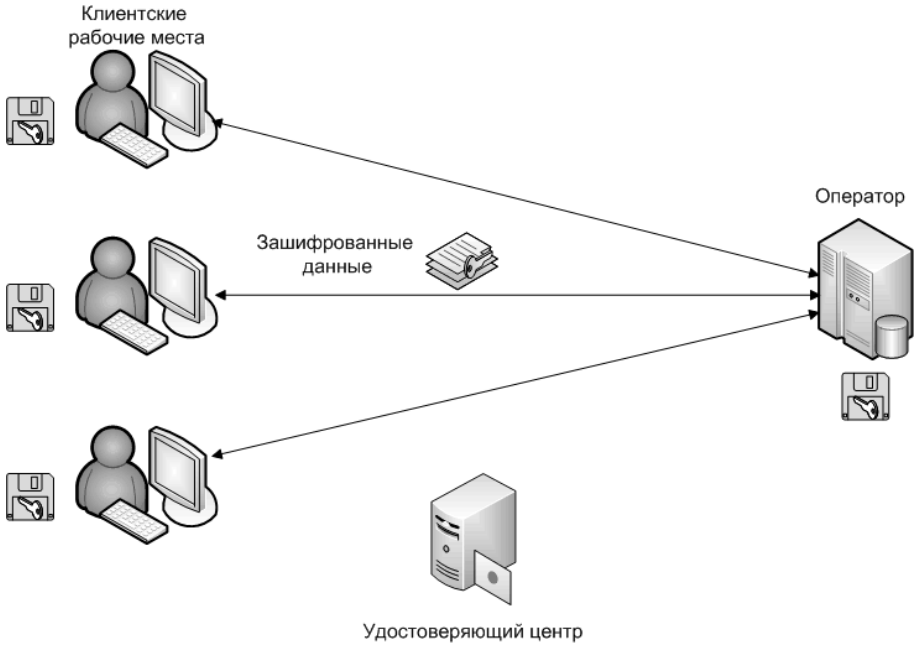

Рис. 1. Компоненты решения по защите персональных медицинских данных

Предлагается система защиты рабочего места обработки персональных медицинских данных, состоящая из следующих модулей: контроля доступа; транспортного; журналирования; криптографического; хранения данных; гарантированного удаления остаточной информации (рисунок 2). Функциональные требования к каждому модулю строго определены.

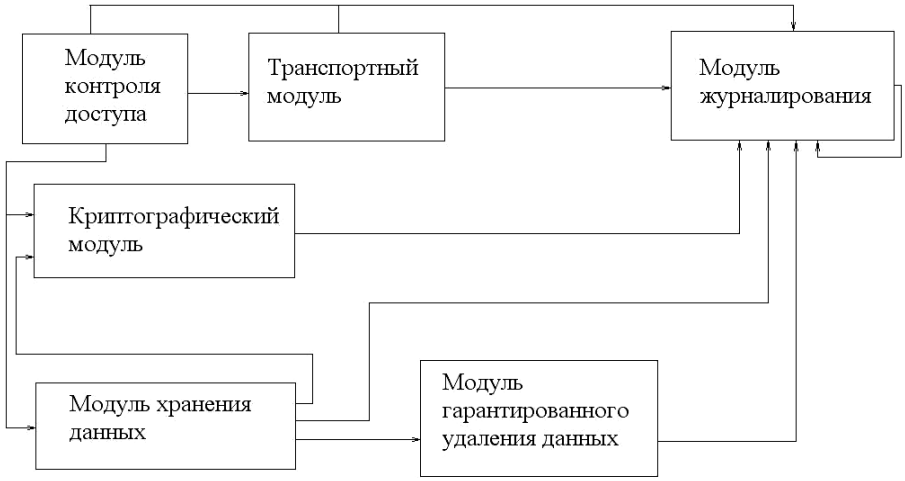

Рис. 2. Структура системы защиты рабочего места обработки персональных медицинских данных

Очевидно, что предложенное комплексное решение устанавливает защищенную среду функционирования персональных медицинских данных, а также удовлетворяет требованиям Федерального закона «О персональных данных». В настоящее время данный проект по защите персональных медицинских данных реализуется на базе лечебно-профилактических учреждений города Томска.

Литература

1. Федеральный закон Российской Федерации от 27 июля 2006 года № 152-ФЗ «О персональных данных».

2. Зыков В.Д. Требования к системам защищенного электронного документооборота // Научная сессия ТУСУР–2007.

Зыков Владимир Дмитриевич
ГОУ ВПО «Томский государственный университет систем управления и радиоэлектроники»
Аспирант кафедры комплексной информационной безопасности электронно-вычислительных систем
Эл. почта: email: zvd@udcs.ru.

V.D. Zykov

The structure of protection system software for the workplace processing personal medical data

In this clause the structure of protection system software for the workplace processing personal medical data and requirements on protection of personal medical data in medical institutions are described in detail.
