Проблемы информационной безопасности в медицинских информационных системах

Фохт Игорь Анатольевич, Горбунов Павел Александрович
Институт программных систем РАН, Исследовательский центр медицинской информатики, Россия, г. Переславль-Залесский, e-mail: vogt@interin.ru

В докладе представлены результаты теоретических исследований и практических разработок Исследовательского центра медицинской информатики Института программных систем Российской академии наук (ИПС РАН) в области обеспечения информационной безопасности в медицинских информационных системах.

Keywords: информационная безопасность, сохранность данных, несанкционированный доступ, медицинская информационная система.

ВВЕДЕНИЕ

Особенностью медицинской информации является ее конфиденциальность. Права граждан на конфиденциальность информации о факте обращения за медицинской помощью и иных передаваемых ими при обращении за медицинской помощью сведений, на информированное добровольное согласие как предварительное условие для медицинского вмешательства и отказ от него установлены Основами законодательства РФ об охране здоровья граждан от 22.07.93 №5488-1 (Постановление Правительства Российской Федерации. Основы законодательства Российской Федерации об охране здоровья граждан, 22.07.1993 №5488-1). Сведения, с которыми оперирует медицинская информационная система, являются персональными данными и могут составлять врачебную тайну.

Кроме того, база данных медицинской информационной системы (МИС) содержит критически важную информацию, от которой, зачастую, может зависеть жизнь человека, поэтому ключевым фактором при создании МИС должно стать обеспечение целостности базы данных и возможность слежения за состоянием системы и ее безопасностью.

Таким образом, особое внимание должно уделяться обеспечению защиты информации в МИС – разделению доступа пользователей ПО к различным фрагментам данных и защите информации от несанкционированного доступа, а также от утраты и искажения данных.

1. ОСНОВНЫЕ ПРОБЛЕМЫ И НАПРАВЛЕНИЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Информационная безопасность (ИБ) при функционировании медицинской информационной системы обеспечивается за счет взаимоувязанного комплексного использования организационных мер, программных и технических средств защиты.

Перечислим основные направления возможных нарушений ИБ:

- Утечка данных (нарушение конфиденциальности).
- Утрата данных.
- Несанкционированная модификация данных.

При включении в МИС средств обеспечения информационной безопасности необходимо помнить, что наращивание требований по ИБ неизбежно накладывает ограничения на доступность данных для пользователей МИС. Есть три вектора информационной безопасности:

- конфиденциальность,
- целостность,
- доступность данных.

И обеспечение ИБ должно строиться на компромиссе меж ними, обеспечивая приемлемый уровень безопасности наряду с приемлемыми для работы пользователей ограничениями в части санкционирования использования ресурсов и сервисов МИС.

2. ТЕХНИЧЕСКИЕ СРЕДСТВА ЗАЩИТЫ ДАННЫХ МИС

К техническим средствам обеспечения защиты данных относятся программно-аппаратные решения, обеспечивающие сохранность носителей информации:

- На уровне устройств хранения. RAID-технологии (зеркалирование, RAID5 и т.д.).
- На уровне БД (Standby, архивирование оперативных журналов).

3. ОРГАНИЗАЦИОННЫЕ МЕРЫ ПО СОХРАННОСТИ ДАННЫХ МИС

В качестве организационного мероприятия по предотвращению утраты данных рекомендуется резервное копирование. Защита от утечки данных во время резервного копирования обеспечивается следующими мерами:

- двойным шифрованием с разделением доступа к ключам и данным,
- регламентом резервного копирования и хранения резервных копий БД, разделяющим полномочия копирующего, паролирующего и хранящего копию,
- разделением прав доступа - администратор БД имеет доступ только к базе данных, не имея доступа к файлам, администратор системы имеет доступ к файлам, но не имеет прямого доступа к БД проекта.

Рекомендуются мероприятия по предотвращению нарушения конфиденциальности, а также вредоносного изменения информации, в случае проникновения в систему постороннего лица с несвойственными ему полномочиями. Данные мероприятия призваны обеспечить выполнение требований инструкции по парольной защиты информации:

- Проведение инструктажа с пользователями МИС о недопустимости хранения своего пароля в доступном месте, а также сообщения его посторонним лицам.
- Профилактическая смена паролей пользователей раз в 2 месяца.
- Запрещение использования в качестве паролей для входа в систему общеизвестных слов – названия системы, названия ЛПУ, своего ФИО и т.д.
- Запрещение использования в качестве паролей для входа в систему «простых» паролей – содержащих одинаковые символы, отличающихся от прошлых номером и т.д.

4. ПРОГРАММНЫЕ СРЕДСТВА ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ МИС (на примере ИНТЕРИН Promis)

При функционировании МИС информационная безопасность данных обеспечивается специальными программными средствами – подсистемой информационной безопасности. Основная функциональность:

- Организация санкционированного доступа к данным.
- Мониторинг «опасных» событий.
- Управление свойствами пользователя МИС.
- Ведение журналов безопасности.

Организация санкционированного доступа к данным относится к общесистемным механизмам. Остальные функции возложены на специализированный АРМ администратора информационной безопасности МИС.

Организация санкционированного доступа к данным

Полномочия пользователя МИС по доступу к той или иной информации определяются конфигурацией рабочего места пользователя и задаются выделенными ему привилегиями.
Привилегии определяются:

- Типовой ролью – описывает полномочия группы пользователей одной специализации (метапользователя), обладающих одинаковыми правами по отношению к информации.
- Элементарными привилегиями – привилегии, которые вносят дополнительные коррективы в стандартное меню какой-либо типовой роли.

Привилегии пользователю выделяет администратор информационной безопасности. Он же обладает полномочиями на изменение и удаление привилегий.

Конфигурация рабочего места задается:

1. Содержанием системного меню, доступного данному пользователю.
2. Содержимым Рабочего стола пользователя (в зависимости от того, какие информационные объекты с какими разрешенными над ними действиями) размещены на его Рабочем столе.

Входными параметрами для медицинской информационной системы являются, прежде всего:

- идентификатор пользователя – вводится при запуске системы ИНТЕРИН Promis (имеет длину до 30 разрешенных символов),
- пароль пользователя – вводится при запуске системы ИНТЕРИН Promis (имеет длину не менее 8 разрешенных символов).

Этими идентификаторами определяется конфигурация рабочего места, которое получит пользователь, независимо от того, где физически расположен компьютер, с которого он запускает систему (в пределах VLAN и имеющийся доступ в системе защиты от несанкционированного доступа). Эти же параметры определяют, какие из разделов МИС доступны данному пользователю (на просмотр или на редакцию).

Мониторинг «опасных» событий

Мониторинг работы МИС реализуется предоставлением списка открытых сеансов (сессий). Выбрав любую, администратор информационной безопасности может либо подробно ознакомиться со свойствами данного пользователя, либо, в случае возникновения каких-либо сомнений в правомерности его действий, принудительно завершить сеанс.

Управление свойствами пользователя МИС

АРМ администратора информационной безопасности предоставляет средства для мониторинга и управления свойствами каждого пользователя МИС.

АРМ обеспечивает отслеживание текущих ролей, показывает имя пользователя в СУБД Oracle, профиль (Oracle), табличное пространство БД, временное табличное пространство, статус – состояние учетной записи пользователя (открыта, заблокирована, просрочен пароль и их комбинации), дату блокировки (если запись была заблокирована), дату истечения пароля и дата создания учетной записи.

Управление свойствами пользователя заключается в предоставлении возможности изменения/наделения его ролями, а также принудительного завершения срока действия пароля и блокировки его учетной записи.

Журналы безопасности

Журналы безопасности ведутся в отношении выделенных «опасных событий» - действий, которые могут повлиять на общую информационную безопасность системы.
АРМ администратора информационной безопасности обеспечивает ведение журналов:

- Ошибки входа (попытки ошибочных входов в МИС).
- Новые пользователи (регистрация новых пользователей).
- Измененные пользователи (пользователи, свойства которых изменялись).
- Удаленные пользователи (пользователи, которые были удалены).
- Предоставление доступа (предоставление доступа пользователям к АРМ/роли).
- Запрещение доступа (запрещение доступа пользователям к АРМ/роли).
- Запуск АРМ (какие АРМы запускались).
- Снятие подписи с документа.

Данные журналов могут быть представлены в отсортированном или отфильтрованном по любому параметру виде. Допускается задание временнОго промежутка. По каждому журналу может быть сформирован и напечатан соответствующий отчет.

5. ОПЫТ ВНЕДРЕНИЯ И ЭКСПЛУАТАЦИИ

При разработке медицинских информационных систем Технологии ИНТЕРИН изначально применялись отдельные фрагменты средств информационной защиты в виде общесистемных механизмов и средств СУБД.

В отдельный самостоятельный блок подсистема информационной безопасности была выделена в рамках реализации специализированного медицинского программного обеспечения для автоматизации деятельности ведомственной амбулатории Главного управления Банка России по Вологодской области в 2005 году.

В докладе описана подсистема информационной безопасности, которая была запущена в промышленную эксплуатацию почти год назад. Опыт ее использования позволяет делать выводы о правильности избранной концепции и примененных технологических решений.