Медицинские информационные системы

Модуль 3. Обеспечение безопасности данных в МИС.

Проблема информационной безопасности в МИС. Категории пользователей МИС. Разграничение доступа в МИС

Ланцберг Анна Вильямовна
К.т.н., доцент кафедры ИУ6 (Компьютерные системы и сети)
lantsberg_av@bmstu.ru
Каб. 801 ГК

Этапы развития концепций безопасности автоматизированных систем

- **Первый этап**: обеспечение безопасности данных механизмами, функционирующими по строго формальным алгоритмам. Программные средства защиты включались в состав операционных систем и систем управления базами данных . Слабым звеном разработанных механизмов защиты была технология разграничения доступа пользователей к данным.
- **Второй этап**: в составе операционных систем ядро безопасности реализовывалось как функционально самостоятельная подсистема управления механизмами защиты данных, которая включала технические, программные, и лингвистические средства.
- **Третий этап**: реализация принципа системности. Все средства и механизмы, используемые для защиты данных, объединяются в систему обеспечения безопасности данных, которая должна обеспечивать многоуровневую защиту данных не только от злоумышленников, но и от обслуживающего персонала АИС, а также случайных ошибок пользователей.
- **Четвертый этап:** разработка и внедрение стандартов в области информационной безопасности. Акцент сделан на безопасность баз данных

Стандартизация систем безопасности

«Критерии оценки надежных компьютерных систем» разработан Национальным центром компьютерной безопасности (NCSC —National Computer Security Center), опубликован Министерством обороны США в 1983 г.

«Руководящие документы по защите от несанкционированного доступа к информации» опубликованы Государственной технической комиссией при Президенте Российской Федерации (Гостехкомиссией) в 1992 г.

Международный стандарт **ISO/IEC 15408** опубликован в 1999 г.

ГОСТ Р ИСО/МЭК 15408-2002 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий» опубликован в 2002 г. на основе ISO/IEC 15408 . Последняя версия утверждена в 2013 г.

ГОСТ Р ИСО/МЭК 15408-2002 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий»

Выделено 11 классов функциональных требований к безопасности информационных систем:

I. аудит безопасности;
II. связь (передача данных);
III. криптографическая поддержка (криптографическая защита);
IV. защита данных пользователя;
V. идентификация и аутентификация;
VI. управление безопасностью;
VII. приватность (конфиденциальность);
VIII. защита функций безопасности объекта;
IX. использование ресурсов;
X. доступ к объекту оценки;
XI. доверенный маршрут/канал.

По защищенности процессов обработки информации все автоматизированные системы делятся на три группы

Третья группа включает в себя автоматизированные системы, в которых работает один пользователь.

Вторая и первая группы включают многопользовательские системы, в которых информация обрабатывается и хранится на носителях различного уровня конфиденциальности.

Уровни построения комплексной системы обеспечения информационной безопасности

I. Уровень прикладного программного обеспечения, отвечающего за взаимодействие с пользователем.
II. Уровень системы управления базами данных, обеспечивающего хранение и обработку данных информационной системы.
III. Уровень операционной системы, отвечающего за функционирование СУБД и иного прикладного программного обеспечения.
IV. Уровень среды доставки, отвечающего за взаимодействие информационных серверов и потребителей информации.

Основа обеспечения информационной безопасности автоматизированных систем

- **Поддержание конфиденциальности информации**
  (обеспечение пользователям доступ только к данным, для которых пользователь имеет явное или неявное разрешение на доступ)
- **Сохранение целостности данных**
  (обеспечение защиты от преднамеренного или непреднамеренного изменения информации или процессов ее обработки)
- **Обеспечение доступности**
  (обеспечение возможности авторизованным в системе пользователям доступа к информации в соответствии с принятой технологией)

Угрозы безопасности автоматизированной информационной системы

Угроза информационной безопасности автоматизированной информационной системе (АИС) - возможность воздействия на информацию, обрабатываемую в системе, приводящего к искажению, уничтожению, копированию, блокированию доступа к информации, а также возможность воздействия на компоненты информационной системы, приводящего к утрате, уничтожению или сбою функционирования носителя информации или средства управления программно-аппаратным комплексом системы.

Угроза нарушения конфиденциальности данных включает в себя любое умышленное или случайное раскрытие информации, хранящейся в вычислительной системе или передаваемой из одной системы в другую.

Угроза нарушения целостности включает в себя любое умышленное или случайное изменение информации, обрабатываемой в информационной системе или вводимой из первичного источника данных.

Источники угроз информации в АИС

Внешние источники:

- умышленные, деструктивные действия лиц с целью искажения, уничтожения или хищения программ, данных и документов системы, причиной которых являются нарушения информационной безопасности защищаемого объекта;
- искажения в каналах передачи информации, поступающей от внешних источников, циркулирующих в системе и передаваемой потребителям, а также недопустимые значения и изменения характеристик потоков информации из внешней среды и внутри системы;
- сбои и отказы в аппаратуре вычислительных средств;
- вирусы и иные деструктивные программные элементы, распространяемые с использованием систем телекоммуникаций, обеспечивающих связь с внешней средой или внутренние коммуникации распределенной системы баз данных;
- изменения состава и конфигурации комплекса взаимодействующей аппаратуры системы за пределы, проверенные при тестировании или сертификации системы.

Источники угроз информации в АИС

Внутренние источники:

- системные ошибки при постановке целей и задач проектирования автоматизированных информационных систем и их компонент, допущенные при формулировке требований к функциям и характеристикам средств обеспечения безопасности системы;
- ошибки при определении условий и параметров функционирования внешней среды, в которой предстоит использовать информационную систему и, в частности, программно-аппаратные средства защиты данных;
- ошибки проектирования при разработке и реализации алгоритмов обеспечения безопасности аппаратуры, программных средств и баз данных;
- *ошибки и несанкционированные действия пользователей, административного и обслуживающего персонала в процессе эксплуатации системы;*
- недостаточная эффективность используемых методов и средств обеспечения информационной безопасности в штатных или особых условиях эксплуатации системы.

Категории пользователей МИС

Группы лиц	Категории
Администраторы МИС	Категория I
Администраторы подсистем или баз данных МИС	Категория II
Пользователи МИС	Категория III
Пользователи, являющиеся внешними по отношению к конкретной МИС	Категория IV
Лица, обладающие возможностью доступа к системе передачи данных	Категория V
Сотрудники ЛПУ, имеющие санкционированный доступ в служебных целях в помещения, в которых размещаются ресурсы МИС, но не имеющие права доступа к ресурсам	Категория VI
Обслуживающий персонал ЛПУ (охрана, работники инженерно-технических служб…)	Категория VII
Уполномоченный персонал разработчиков МИС, имеющий право обслуживать и модифицировать компоненты МИС	Категория VIII

Специфика медицинской информации

- *Пациент имеет доступ ко всей медицинской информации, относящейся к нему*
- *Вся медицинская информация должна обрабатываться оперативно*
- *Медицинская информация разбивается на множество частей, обрабатываемых разными специалистами, в том числе лаборантами, медицинскими сестрами, врачами и регистраторами*
- *Информация является многогранной, носит всесторонний характер: персональные данные, статистические данные, сведения о ходе лечения.*
- *Отсутствует регламент взаимодействия медицинских сотрудников, пациентов и доверенных лиц*

>>>>>Велика вероятность возникновения угроз несанкционированного получения доступа к данным, утраты информации и ее искажения

Объекты МИС, подлежащие защите

- ✓ *Вычислительная мощность файлового сервера*
- ✓ *Информация в базе данных СУБД*
- ✓ *Резервные копии из базы данных СУБД*
- ✓ *Архивные копии файлового сервера*
- ✓ *Целевые данные операционной системы, СУБД, АРМ, администратора МИС и начальника информационной безопасности*
- ✓ *Сбор, обработка, хранение и передача информации в МИС*
- ✓ *Программные и аппаратные средства обеспечения функционирования МИС*

Наиболее вероятные нарушения информационной безопасности

- *Утечка данных (нарушение конфиденциальности)*
- *Полное или частичное получение доступа к базе данных*
- *Получение злоумышленниками доступа к информации*
- *Утрата данных (физическое разрушение носителей информации и/или стирание информации при непосредственном доступе к данным или через интерфейс системы)*
- *Несанкционированное внесение изменений в данные (через интерфейс системы или при прямом доступе к базе данных)*
- *Отказ функционала МИС (из-за повреждений целостности системы)*
- *Некорректное функционирование МИС (в результате несанкционированного изменения ее модулей)*

Информационная безопасность МИС достигается с помощью комплексного применения ***организационных мер, программных и технических средств защиты.***

Этапы построения системы защиты МИС

I. *Сбор сведений о существующих системах, хранящих персональные сведения*
II. *Моделирование угроз безопасности*
III. *Разработка технических заданий по обеспечению безопасности МИС*
IV. *Проектирование системы защиты информации*
V. *Разработка организационно-распорядительной документации, которая регламентирует процессы обработки и защиты сведений*
VI. *Поставка, установка и настройка средств защиты информации*
VII. *Проведение аттестации информационных систем согласно требованиям безопасности*

Важные мероприятия, реализуемые на этапах I и II

- Анализ безопасности архитектурных решений и их программных реализаций в СУБД
- Анализ безопасности взаимодействия с внешними компонентами
- Исследование вопросов сопряжения с программным обеспечением промежуточного уровня

Анализ безопасности архитектурных решений и их программных реализаций в СУБД

- идентификация и аутентификация субъектов (пользователей) системы,
- технологии реализации дискреционной, мандатной и ролевой моделей доступа к ресурсам системы,
- реализацию аудита действий пользователей.

Технологии реализации дискреционной, мандатной и ролевой моделей доступа к ресурсам системы

- В процессе исследования **дискреционной модели** доступа важно обратить внимание на особенности реализации системных привилегий и привилегий доступа к объекту системы, в частности, механизмы предоставления и отзыва привилегий. Основа дискреционной модели – матрицы доступа, где строки – это субъекты (пользователи), столбцы – объекты (файлы)

- Важнейший вопрос при проведении исследования реализации **мандатной модели** управления доступом — технология присваивания и изменения меток для объектов и субъектов. Реализация разграничения доступа на уровне кортежей предполагает наличие специального столбца с меткой доступа.

- Ролевая модель доступа широко распространена в мировой практике обеспечения защищенных технологий обработки баз данных.
  Роль — это поименованный набор привилегий, который может быть предоставлен пользователю или другой роли; по сути, языковое средство для автоматизации работы администратора по разграничению доступа.

- **Представление** — это поименованная динамически поддерживаемая сервером выборка из одной или нескольких таблиц. Оператор SELECT, определяющий выборку, ограничивает видимые пользователем данные. Кроме того, представление позволяет эффективно ограничить данные, которые пользователь может модифицировать.

Аудит действий пользователя

Аудит – автоматическое ведение протоколов действий пользователей системы.

В СУБД средство ведения аудита реализовано в виде набора возможностей, управляемых языковыми средствами системы, или независимой утилиты.

Средства аудита выполняют фиксацию информации об активности пользователей системы в словаре данных или в файле операционной системы — журнале аудита.

Информация о настройках системы аудита хранится в специальном конфигурационном файле.

Файл настройки или параметры команды активизации аудита определяют перечень событий, которые фиксируются системой аудита.

Анализ безопасности взаимодействия с внешними компонентами

- вопросы сопряжения с элементами операционной системы — анализ управляющих и информационных потоков вниз
- вопросы сопряжения с программным обеспечением промежуточного уровня (прослушивающие процессы, HTTP-серверы, мониторы транзакций и т. п.) — анализ управляющих и информационных потоков вверх
- возможности пользователей СУБД несанкционированно осуществлять чтение и запись в файлы и устройства операционной системы, включая возможность модификации записей аудита, осуществляемых во внешние файлы

Исследование вопросов сопряжения с программным обеспечением промежуточного слоя

1) выявление портов взаимодействия с внешним программным обеспечением и механизмов их активизации и переназначения (внутренние и внешние);
2) устойчивость к перегрузкам каналов с шумовым трафиком и вставкам ложных пакетов;
3) возможности внутреннего и внешнего управления активизацией и перенастройкой параметров протоколов ODBC и JDBC;
4) анализ алгоритмов и технологий линейного шифрования трафика межсерверного обмена и взаимодействия клиентского программного обеспечения с серверами баз данных.

Меры обеспечения информационной безопасности МИС. Программные компоненты

Защита от несанкционированного доступа	Развертывание средств авторизации
	Использование систем мониторинга сетей
	Применение систем обнаружения и предотвращения вторжений (IDS/IPS)
	Внедрение систем предотвращения утечек конфиденциальной информации (DLP)
	Применение технологии децентрализованного хранения данных (блокчейн)
	Установка антивирусного программного обеспечения и развертывание межсетевых экранов (файерволов)
Криптографические средства защиты	Использование алгоритмов шифрования данных
	Внедрение электронной цифровой подписи
Системы аутентификации	Внедрение парольной защиты
	Подпись сертификатами
	Доступ по биометрическим данным
Инструментальные средства анализа систем защиты	Программное обеспечение для мониторинга

Меры обеспечения информационной безопасности МИС. Технические компоненты

Системы бесперебойного питания	Установка и обслуживание источников бесперебойного питания
	Резервирование нагрузки
	Установка генераторов напряжения
Средства предотвращения взлома корпусов и кражи оборудования	Электронные ключи, смарт-карты (дополнение к парольной защите)
Средства контроля доступа в помещение	Исполнительные турникеты (шлагбаумы, турникеты и т.д.)
	Средства идентификации: карты, брелоки, биометрия и т.д.
	Считыватели (картридеры)
	Панели для ввода с клавиатуры
	Устройства биометрической аутентификации
	Контроллеры и концентраторы
	Индивидуальное ПО

Меры обеспечения информационной безопасности МИС. Организационные компоненты

- Исключение злоумышленного проникновения на территорию и в помещения посторонних лиц
- Организация работы с сотрудниками в плане доступа к информации
- Организация работы с документами и документированной информацией
- Организация использования технических средств сбора, обработки, накопления и хранения конфиденциальной информации
- Организация работ по анализу внутренних и внешних угроз конфиденциальной информации
- Организация работы по проведению контроля за работой персонала с конфиденциальной информацией

Спасибо за внимание!