В.А. Юхимец, В.Г. Терентюк, В.А. Науринский, В.В. Куц, В.В. Яровой,
А.С. Ерёмина, А.Л. Мельник, А.С. Лисневич

АВТОМАТИЗИРОВАННАЯ МЕДИЦИНСКАЯ ИНФОРМАЦИОННАЯ СИСТЕМА. ВНЕДРЕНИЕ И ОПТИМАЛЬНЫЕ ТЕХНИЧЕСКИЕ РЕШЕНИЯ

ЧАСТЬ 1

ГУ «Национальный институт фтизиатрии и пульмонологии им. Ф.Г. Яновского НАМН Украины»
ООО «АЛТ Украина Лтд.»

Опыт внедрения Автоматизированной медицинской информационной системы (АМИС) в таком большом специализированном научно-медицинском учреждении, которым является Национальный институт фтизиатрии и пульмонологии им. Ф.Г. Яновского (НИФП НАМН), проводившегося на протяжении 2014-2016 гг. за счет бюджетного финансирования, позволяет нам высказать свои соображения относительно оптимальных технических решений этого сложного процесса. Они легли в основу технического проекта внедрения системы.

В 1-и части статьи изложены определения АМИС, задачи, которые она решает, назначение и область ее использования и основные примененные технические решения, в частности, архитектура и состав основных подсистем, логическая и функциональная архитектура системы, решения в части защиты информации.

АМИС представляет собой программно-аппаратный комплекс как совокупность программно-технических средств и баз данных, предназначенных для информатизации учреждений здравоохранения и автоматизации рабочих мест и производственных процессов, которые осуществляются на этапах предоставления медицинской помощи пациентам в лечебно-профилактическом учреждении (ЛПУ). Самыми важными функциями АМИС являются улучшение показателей предоставления медицинской помощи и создание условий для принятия управленческих решений.

Функционально АМИС состоит из 2-х взаимосвязанных компонентов: аппаратного и программного. Аппаратный компонент – это локальная компьютерная сеть в составе серверов, коммутационных узлов, кабельных сетей, сетевых рабочих станций, терминалов («тонких» клиентов), печатающих устройств, сканеров, а также программных продуктов, непосредственно обеспечивающих их функционирование. Программный компонент – это специализированный программный продукт (ПО АМИС), который работает на базе аппаратного компонента, и обеспечивает функционирование собственно автоматизированной медицинской информационной системы. В дальнейшем мы будем использовать аббревиатуру

АМИС для обозначения всего аппаратно-программного комплекса, а ПО АМИС – именно специализированного программного продукта. АМИС должна обеспечивать нужды медицинского и управленческого персонала ЛПУ в систематической информации по всем аспектам деятельности учреждения для принятия решений, способствующих достижению конечного результата – повышению качества предоставления медицинской помощи пациентам.

1. Задачи АМИС. Основными задачами внедрения АМИС в ЛПУ мы считали следующие:

- вербальное взаимодействие между врачами и другими участниками лечебно-диагностического процесса;
- накопление, сохранение, обработка и оперативная выдача информации о ходе лечебно-диагностического процесса;
- ретроспективный контроль и анализ лечебно-диагностического процесса;
- повышение управляемости ЛПУ за счет уменьшения уровня неопределенности во время формирования и принятие управленческих решений;
- повышение эффективности деятельности структурных подразделений ЛПУ при использовании иерархической системы сбора, сохранения, передачи и централизованной обработки информации, содержащейся в амбулаторной карте и истории болезни, с оперативным доступом к информации на рабочих местах (АРМ);
- повышение эффективности работы медицинского персонала, всех сотрудников медицинского учреждения за счет автоматизации трудоемких, рутинных операций (подготовка многочисленных выписок, справок, отчетов, дублирование результатов анализов, и т.п.),
- повышение достоверности данных и оперативности информационного обслуживания;
- организация информационного взаимодействия различных врачей-специалистов с возможностью более полного и оперативного обеспечения в предоставления медицинской помощи на всех этапах обслуживания пациента (профилактического, диагностического, диспансерного, стационарного, реабилитационного);
- повышение качества диагностики и лечения за счет использования экспертной поддержки принятия решения врачами с внедрением экспертной оценки их работы;
- проведение сравнительной оценки эффективности разных методов лечения на

основе накопленной базы данных;

- анализ стоимости, контроль полноты и качества диагностических и лечебных мероприятий;
- рационализация использования медицинских ресурсов (персонала, оборудования, лекарств, расходных материалов и т.п.);
- предоставление сотрудникам необходимой справочной информации по основным видам медпомощи с использованием сети Интернет;
- уменьшение затрат на медицинские услуги при отсутствии снижения качества медпомощи;
- уменьшение продолжительности медицинского обслуживания пациента за счет упрощения процедуры введения информации в электронную медицинскую карту (ЭМК);
- получение врачом полной информации о пациенте, содержащейся в ЭМК, в удобной и наглядной форме, а также справочной информации;
- повышение квалификации персонала за счет использования в работе современных информационных технологий с простым и удобным доступом к единым электронным справочникам и Базам Данных;
- сохранение конфиденциальности персональной информации пациентов и защиты ее от несанкционированного доступа;
- постоянное и надежное сохранение информации о пациентах с возможностью поиска и просмотра всех видов медицинских карт, результатов анализов, исследований, консультаций, а также историй болезней, позволяющее избежать дополнительных затрат на диагностические исследования;
- оперативное получение информации о загруженности ресурсов ЛПУ, специальных служб, персонала и оборудования для гибкого и эффективного управления работой ЛПУ;
- сокращение сроков создания и упрощение процедуры ведения форм государственной статистической отчетности, администрирование страховых медицинских случаев, отчетов о работе учреждения, и т.п.;
- уменьшение сроков и упрощение процедуры подготовки отчетных материалов о работе ЛПУ;
- использование единых процедур подготовки данных по использованию рабочего времени персоналом ЛПУ для последующего бухгалтерского учета;
- автоматизация учета материальных ресурсов ЛПУ и, в частности, лечебных средств

и товаров медицинского и немедицинского назначения.

2. Назначение АМИС. Исходя из приведенных задач, АМИС предназначена для комплексной автоматизации ЛПУ и должна осуществлять поддержку лечебно-диагностических мероприятий, обеспечивать информационную поддержку работы медицинских работников ЛПУ, осуществлять поддержку бизнес-планирования и оптимизации всех производственных процессов ЛПУ и осуществлять информационную поддержку оценки их эффективности. АМИС, без ухудшения заданных характеристик, имеет возможность адаптации к любым изменениям в лечебно-диагностическом процессе, методах управления, принципах учета и т.п., в частности, организационной структуры ЛПУ, системы кодирования ЭМК, форм статистической и другой отчетности и периодичности их предоставления, количественного и качественного состава диагностического и другого оборудования, формата и структуры файлов обмена данными со смежными системами. Адаптация обеспечивается за счет процедур администрирования и конфигурирования ПО АМИС, модификации документальных и отчетных форм.

3. Область использования АМИС. АМИС используется для хранения всего необходимого набора данных, которые могут появляться в ЛПУ в процессе предоставления медицинской помощи пациентам. Структура построения массива данных разрабатывается в соответствии с мировыми стандартами, что гарантирует дальнейшую интеграцию и двустороннюю передачу данных в другие медицинские Базы данных или реестры. АМИС должна поддерживать автоматический режим работы с диагностическим и лабораторным медицинским оборудованием, соответствующем международным стандартам обмена и управления медицинскими данными DICOM3 и/или ASTM1394.

4. Основные технические решения. Далее приводятся основные технические решения, которые были применены нами при внедрении АМИС в НИФП НАМН, и на практике доказали свою жизнеспособность и практическую целесообразность.

4.1. Архитектура и состав основных подсистем. Компонентная структура АМИС схематично изображена на рисунке 1. Она построена на принципе системы управления обработкой транзакций. Такая система характеризуются большим количеством изменений в Базе данных (БД). Изменения вводятся интенсивно, большим количеством пользователей. Произвольное число пользователей может одновременно обращаться к одним и тем же данным, но только один из них имеет возможность изменять их в данный момент времени. Построенная система гарантирует, что только один Пользователь в каждый конкретный момент времени может изменить любые конкретные данные.

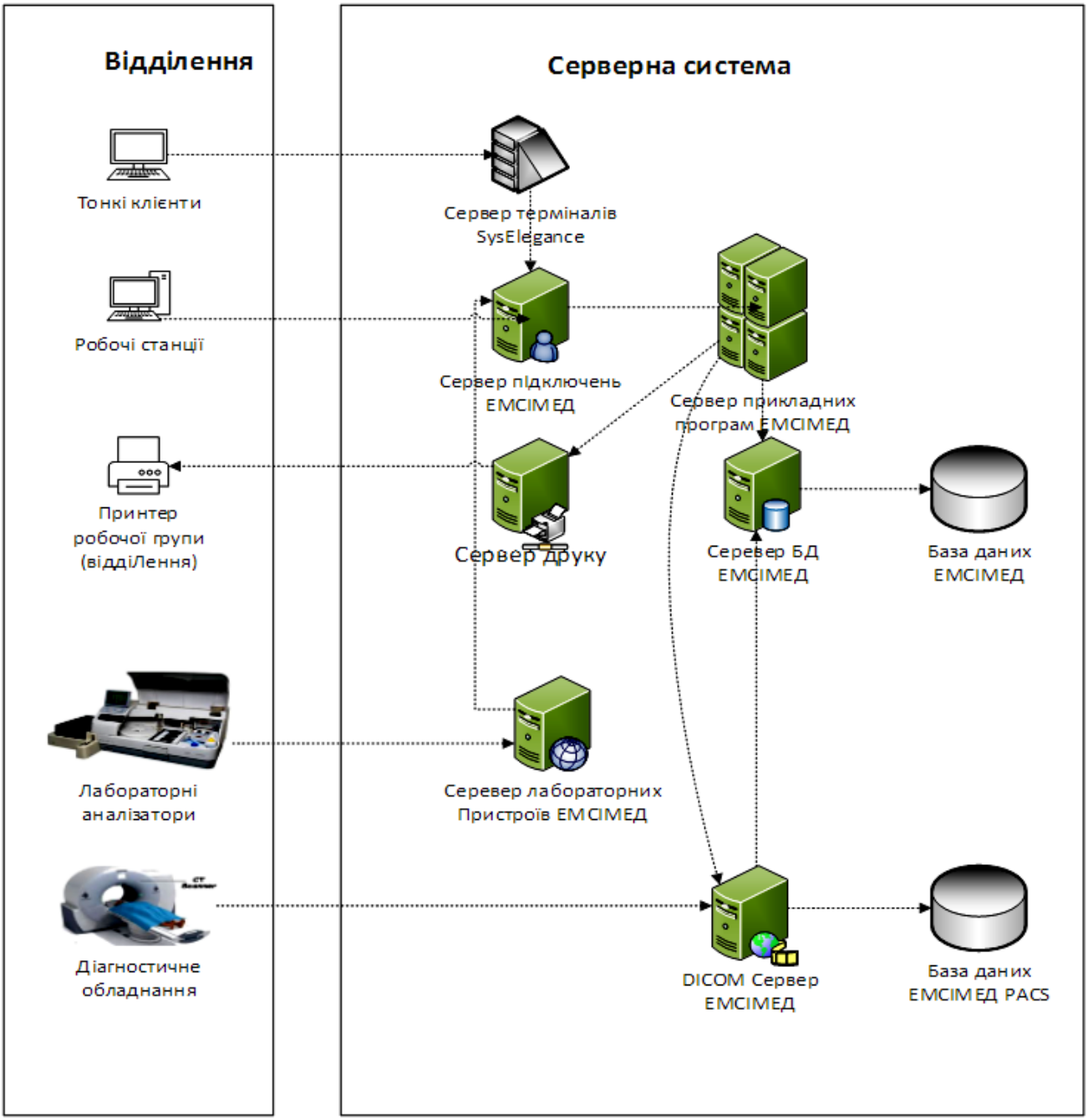

Рисунок 1. Компонентная структура АМИС.

Изменения вносятся с помощью механизма транзакций. Трансакция представляет собой набор изменений, рассмотренных, как единое целое. Если одно из изменений не может быть выполнено, то и все другие изменения, выполненные в транзакции, будут отменены для сохранности целостности данных. Одновременно АМИС имеет элементы оперативной аналитической обработки накапливаемой информации и принимает решение на основе ее анализа. АМИС работает на основе СУБД SQL и имеет архитектуру " клиент-сервер". Единая

БД общего использования размещается на отказостойкой подсистеме обработки транзакций и сохранения данных, включающей сервер БД и дисковый массив с расщеплением дисков, которая размещена в ЛПУ и обеспечивает доступ к этой БД с автоматизированных рабочих мест (АРМ) пользователей, подключенных к локальной сети.

Пользователями АМИС являются все медицинские работники из числа уполномоченных сотрудников ЛПУ, которые работают на автоматизированных рабочих местах (АРМ), входящих в состав АМИС. На АРМ пользователей установленное клиентское лицензионное программное обеспечение для работы с АМИС. АМИС поддерживает работу с различными типами АРМ пользователей, в частности: настольный компьютер, ноутбук, «тонкий» клиент, а также с различными путями организации рабочих сеансов пользователей, в частности: работа в обычном и терминальном режиме, включая возможность работы на бездисковых АРМ.

Средствами передачи информации между клиентом и сервером БД в АМИС является локально-вычислительная сеть (ЛВМ) с пропускной способностью оптоволоконной магистрали 1 Гбит/сек, функционирующая на основе стека транспортных протоколов TCP/IP. Связь с клиентами обеспечивается с помощью ЛОМ и сервера программных приложений. Доступ к БД обеспечивается с помощью сервера программных приложений через специализированные интерфейсы программирования доступа (ADO).

АМИС исключает непосредственный доступ клиента к БД. Вся переданная и полученная клиентом информация передается в зашифрованном виде. Алгоритм шифрования SSL (от 40 до 128 Бит) используется в случае установления серверу программных приложений с помощью транспортного туннеля через Kerberos. В АМИС возможен вход только авторизованных клиентов с предоставлением каждому клиенту соответствующих регламентированных прав на просмотр определенной информации и выполнение определенных операций в системе.

Программное обеспечение клиента включает клиентский модуль, базирующийся на графическом интерфейсе (GUI). Все прочее программное обеспечение, которое включает правила и логику обработки данных, хранится на сервере программных приложений и сервере БД.

Задачи сервера БД:

- управление информационной БД, с которой совместно работают группы Пользователей;
- управление доступом к БД;

- защита информации с помощью средств архивации/восстановления;
- централизованное задание для всех приложений обработки данных глобальной целостности данных;
- обеспечение высокой скорости обработки запросов.

Задачи клиентского модуля (клиентской программы, запускаемой пользователем на своем АРМ):

- представление интерфейса пользователя;
- управление логикой приложения;
- выполнение логики приложения;
- проверка допустимости данных;
- запрос и получения информации о сервере БД.

4.2. Логическая и функциональная архитектура системы. В основе архитектуры АМИС лежит многоуровневая схема прикладных программ баз данных. Сервер баз данных реализован на базе программного обеспечения Microsoft (MS) SQL Server 2012 SE на сервере под управлением операционной системы (ОС) MS Windows Server 2012 R2. Сама база хранит данные системы, триггеры, сохраненные процедуры и SQL-запросы, которые обеспечивают доступ к этим данным и им целостность. Выполнение COM+ модулей системы на COM+ сервере под управлением MS Windows Server обеспечивает MS DTC-сервис. Он также руководит SQL-транзакциями. Архитектура системы представлена следующими COM + модулями:

- диспетчер SQL-запросов обеспечивает доступ к запросам, хранящимся в БД, вызывает SQL-сервер для их выполнения и передает результаты в виде ADO Recordset вызова модуля;
- прикладной сервис выполняет аутентификацию пользователя, поддерживает сессию пользователя и авторизацию при доступе к ресурсам системы, а также вызывает диспетчер SQL-запросов.

Сокет-сервер системы реализован как Windows-сервис. Осуществляя поддержку соединения с клиентом в сетевой среде TCP/IP, он обеспечивает получение запросов и передачу данных между прикладным сервисом АМИС и клиентской частью. Также сокет-сервер может сериализировать или десериализировать данные в формате XML или ADTG и зашифровать/дешифровать трафик в соответствии с проколом SSL.

На рабочем месте сотрудника ЛПУ работает клиентский модуль – часть ПО, и модуль

обновления версий. Клиентский модуль АМИС обеспечивает пользователя возможностью выполнения всех операций по вводу данных в систему, их первоначальной проверки на допустимость и непротиворечивость, передачи их на сервер, а также получения информации с сервера БД и ее представления в удобном для просмотра и анализа виде.

Подсистема соединения выполняет: поддержку соединения (в том числе удаленного) с сервером соединений АМИС, сериализацию/десериализацию данных, шифрование/дешифрование трафика, принудительное управление клиентскими SQL-транзакциями.

На сервере данных DICOM (сервере PACS) хранится база данных DICOM (за исключением изображений) и работает MS SQL сервер. Прикладной сервис DICOM реализован как Windows-сервис, который выполняет запросы к БД DICOM и осуществляет доступ к хранилищу изображений, расположенному на том же компьютере или реализованном в виде сетевого ресурса. Клиентский модуль взаимодействует непосредственно с DICOM-сервером.

Бизнес-логика системы распределена на несколько уровней и оптимизирована с точки зрения минимизации трафика между клиентскими модулями и сервером подключений. Основная ее часть реализована в виде триггеров, сохраненных процедур и SQL-запросов, которые выполняются на SQL-сервере.

Архитектура АМИС распределяется на 3 уровня (рисунок 2):

- **клиентский (уровень презентации).** Предназначен для отображения бизнес-контента. На рабочем месте пользователя системы работает клиентский модуль и модуль обновления версий. Клиентский модуль обеспечивает возможность выполнения всех операций по вводу данных в систему, их первоначальной проверке на допустимость и непротиворечивость, передачу их на сервер, а также получение информации с сервера данных и ее представление в удобном для просмотра и анализа виде;

- **уровень приложений (бизнес-логики)**. Состоит из сервиса подключений (сокет-серверу) и прикладных функциональных приложений АМИС, развернутых на COM+. Сокет-сервер системы реализован как Windows-сервис и обеспечивает получение запросов, передачу данных между прикладным сервисом АМИС и клиентским модулем, мониторинг трафика клиентских соединений и ведения протокола запросов. Бизнес-логика системы представлена следующими COM+ модулями:

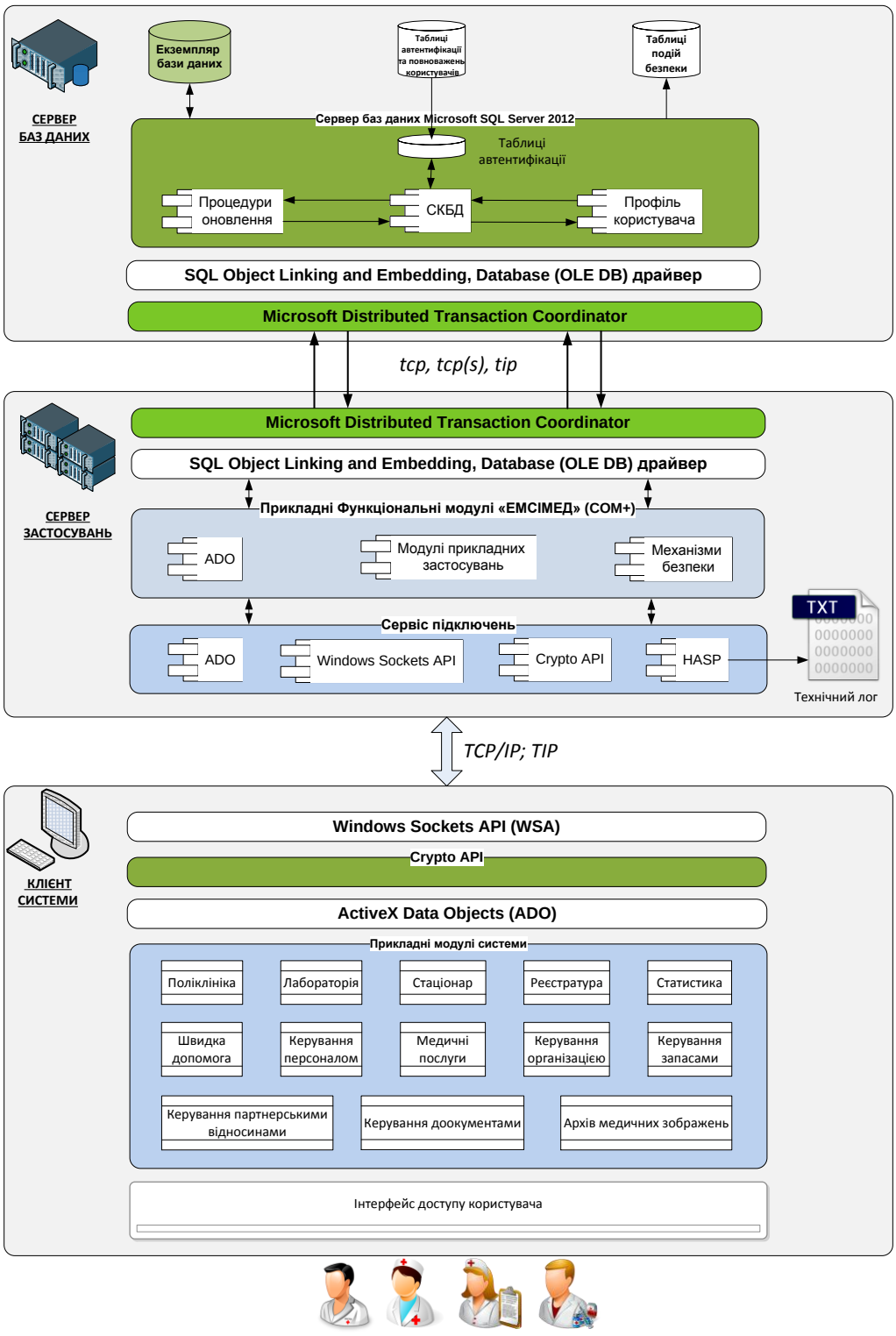

Рисунок 2. Архитектура системы.

- диспетчер SQL-запросов обеспечивает доступ к запросам, которые хранятся в БД, вызывает SQL-сервер для их выполнения и передает результаты в виде ADO Recordset

вызванному модулю;

- прикладной сервис АМИС, выполняющий аутентификацию пользователя, поддерживает сессию пользователя и авторизацию при доступе к ресурсам системы, а также вызывает диспетчер SQL-запросов;

- уровень базы данных. Данный уровень представлен в виде многоуровневой схемы прикладных программ баз данных. Сама база хранит данные системы, триггеры, сохраненные процедуры и SQL-запорсы, которые обеспечивают доступ к этим данным и их целостность. Выполнение COM+ модулей системы обеспечивается MS DTC-сервисом, к функциям которого относится управление SQL-транзакциями.

ПО АМИС интегрирует в себе прикладной сервер Windows Server Application Role, систему управления базами данных Microsoft SQL Server 2012 R2, функциональные модули ПО АМИС, которые инсталлируются в систему поодиночке, и дополнительные компоненты. Клиентский модуль АМИС инсталлируется отдельно на АРМ пользователя системы и терминальные серверы. Прикладной сервер Windows Server Application Role состоит из Windows Sockets API, Crypto API и серверных процессов для выполнения COM-программ. Доступ сервера к COM-данным в базе данных выполняется через OLE DB и MS DTC, которые предоставляют единый интерфейс для импорта программных пакетов. Система управления базами данных Microsoft SQL Server 2012 состоит из диспетчера, модуля управления потоками Workflow и интерфейса администрирования СУБД SQL Server Management Studio. Прикладные функциональные модули ПО АМИС состоят из разработанных на базе ADO серверных COM-приложений в соответствии с необходимыми выполняемыми задачами. Клиентские COM-приложения, которые устанавливаются на клиентской стороне под управлением ОС Windows, реализуют функциональный интерфейс доступа пользователя в соответствии со своим назначением.

Дополнительные компоненты предназначены для осуществления внутренних и внешних соединений прикладных серверов.

4.3. Решения относительно защиты информации. Защита информации в АМИС является многоуровневой и обеспечивается как стандартными средствами серверной операционной системы, так и средствами ПО АМИС и антивирусной защиты.

4.3.1. Защита на уровне операционной системы с применением Active Directory. На момент начала внедрения АМИС в институте уже существовала ЛВС с доменными принципами управления сетью, которая включала:

- единое хранилище объектов управления, к которым относятся пользователи, компьютеры, серверы, принтеры, информация службы доменных имен, и т.п.;
- гибкое управление объектами, а именно: создание, редактирование, удаление, установление политик безопасности пользователей и рабочих станций, управление правами доступа, аудит доступа к объектам;
- централизованное управление всеми объектами с одного рабочего места;
- гибкое определение политик безопасности, прав и параметров рабочего места для пользователей, которые используют учетные записи в службе каталогов, в соответствии с правилами групповых политик;
- группирование объектов управления службы каталогов в соответствии с местом нахождения, организационной структурой объекта и т.п., с возможностью частичного делегирования прав для администрирования выделенной группы объектов;
- единая аутентификация и авторизации пользователей в службе каталогов;
- предоставление авторизованным пользователям соответствующих прав доступа согласно групповым политик к прикладным подсистемам унифицированных коммуникаций и инфраструктурных систем.

4.3.2. Защита на уровне ПО АМИС:

- создание списка пользователей согласно штатного расписания;
- определение перечня групп пользователей и присвоение функций к отдельным группам;
- добавление пользователей к группам в соответствии с полномочиями;
- определение перечня профилей врачей для доступа к формам первичной документации;
- распределение доступа пользователей к отдельным отчетам;
- вся информация между рабочим местом пользователя и сервером прикладных программ передается с помощью защищенного транспортного протокола с шифрованием с помощью ключей HASP;
- использование сеансных ключей.

4.3.3. Архитектура средств защиты от несанкционированного доступа. Средства защиты являются совокупностью функций в составе следующих компонентов:

- серверной операционной системы Windows Server 2012 R2;
- клиентской операционной системы Microsoft Windows 2000/XP/7/8;

- сервера приложений Windows Server Application Role;
- сервера баз данных Microsoft SQL Server 2012;
- прикладных функциональных модулей АМИС.

Компоненты средств защиты системы АМИС предназначены для реализации функций защиты информации, которая обрабатывается средствами АМИС, от несанкционированного доступа.

На уровне внутренних прикладных приложений средства защиты обеспечивают:

1) идентификацию и аутентификацию пользователей по группам безопасности и функциональным ролями в рамках АМИС;

2) авторизацию полномочий пользователей и процессов в рамках их транзакций при попытках доступа к рабочим, серверным и технологическим процессам и объектам БД;

3) протоколирование и аудит событий в системе;

4) защита собственных компонентов от несанкционированной модификации, блокирования и отказов;

5) доступность рабочих, серверных и технологических процессов АМИС в рамках транзакций пользователей;

6) криптографическая защита информационного трафика между сокет-сервером АМИС и клиентским модулем.

Сервер приложений – это компонент АМИС, предназначенный для управления приложениями, которые разрабатываются на платформе COM+. Он состоит из сервиса подключений АМИС Socket Server и рабочих процессов, выполняющих COM-программы. Доступ сервера к данным в базе данных осуществляется по OLE DB-схеме и MS DTS. Инструмент ADO предоставляет среду разработки для программирования на языке COM.

В то время, как сервер приложений АМИС обеспечивает полный контроль над внутренними приложениями, его функции служат только базисными функциями для использования приложений, управляемых клиентом. Поэтому в рамках данного документа рассматриваются лишь функции безопасности, обеспечиваемые ядром системы обеспечения фундаментальной политики безопасности и некоторых служб безопасности, которые будут использоваться во внутренних приложениях АМИС.

Основное назначение средств защиты:

- защита COM-приложений, для которых реализуется доступ средствам сервера приложений;

- обеспечение аудита;
- управление пользователями и авторизацией;
- идентификация и аутентификация пользователей;
- управление и интеграция COM-процессов;
- управление защитой.

Сервер баз данных Microsoft SQL Server 2012 – это компонент АМИС, предназначенный для хранения информации из COM-приложений, таблиц аутентификации и полномочий пользователя, таблиц событий безопасности. Средства защиты Microsoft SQL Server 2012 представляют собой набор механизмов безопасности относительно обеспечения конфиденциальности, целостности и доступности информации, которая хранится и обрабатывается в базах данных, а также наблюдаемость (управляемость) SQL Server 2012 в целом.

Существуют три категории прав на уровне базы данных. Это право на администрирование (DBA), право на управление ресурсами (RESOURCE), право на доступ (CONNECT). Некоторые пользователи могут вообще не иметь никаких прав, связанных с конкретной базой данных:

1. Пользователь, имеющий право на доступ (CONNECT), имеет возможность получать и модифицировать данные в базе. Он может модифицировать те объекты, которыми владеет.

2. Пользователь, имеющий имеет право на управление ресурсами (RESOURCE), в дополнение к тем прав, которые имеют пользователи с правом на доступ, может создавать новые объекты.

3. Пользователь, имеющий имеет право на администрирование базы данных (DBA) в дополнение к тем прав, которые имеют пользователи с правом на управление ресурсами, обладает следующими возможностями: удалять базу данных и любые объекты независимо от того, кто ими владеет; раздавать и менять права доступа других пользователей к базе данных в целом и к отдельным объектам.

Защита данных в Microsoft SQL Server 2012 базируется на привилегиях (разрешенных действиях), предоставляемых пользователям (или группам пользователей), которые имеют идентификаторы на конкретные объекты базы данных (например, таблицы).

Контроль за доступом к информации осуществляет сервер базы данных. Пользователь не имеет доступа непосредственно к файлам БД. Он не знает, как и где хранятся эти файлы. При выполнении запроса пользователя сервер получает его от сервера приложений АМИС,

определяет имя пользователя, и по внутренней информации определяет, может ли данное лицо выполнить этот запрос. Если такое право имеется, сервер выполняет обработку запроса, если нет – пользователю присылается сообщения об ошибке.

Назначение средств защиты в структуре Microsoft SQL Server 2012:

- защита таблиц данных, доступ к которым реализуется со стороны сервера приложений АМИС;
- обеспечение аудита;
- управление защитой;
- хранение личных данных пациентов в БД в зашифрованном виде.

Прикладные функциональные модули ПО АМИС – это компоненты системы, разработанные на COM-платформе сервера приложений в соответствии с необходимыми задачами (Поликлиника, Лаборатория, Стационар, Регистратура, Статистика, Управление персоналом, Медицинские услуги, Управление организацией, Управление запасами, Управление партнерскими отношениями, Управление документами, Архив медицинских изображений, Администрирование, Scientific), которые реализуют функциональный интерфейс доступа пользователя согласно своему назначению.

Назначение средств защиты в структуре прикладных функциональных модулей ПО АМИС:

- защита прикладных модулей, доступ к которым реализуется со стороны сервера приложений АМИС;
- обеспечение аудита;
- резервирование и архивирование данных;
- управление защитой.

4.3.4. Внешние интерфейсы средств защиты. Для каждого из видимых извне интерфейсов описаны следующие пункты:

- тип интерфейса (отношение к функциям защиты);
- протокол/метод использования (например, сетевой протокол, транзакция, запрос);
- целевая функция интерфейса.

В таблицах 1-4 отображены интерфейсы определенных выше компонентов:

1) внешние интерфейсы уровня презентации;
2) внешние интерфейсы сервиса подключения;
3) внешние интерфейсы COM+ исполнений;

4) внешние интерфейсы уровня баз данных.

Таблица 1. Внешние интерфейсы средств защиты АМИС (уровень презентации)

Название интерфейса	**Протокол/Метод использования**	**Целевая функция**
Windows Sockets API	TCP/IP	Подключение оборудования Логика проверки ввода
Crypto API	Security Support Provider Interface	Шифрование трафика
ADO	Activex COM+	Презентация данных

Таблица 2. Внешние интерфейсы средств защиты АМИС (сервис подключений)

Название интерфейса	**Протокол/Метод использования**	**Целевая функция**
Windows Sockets API	TCP/IP	Поддержка сессий клиента
Crypto API	Security Support Provider Interface	Шифрование трафика
ADO	Activex COM+	Сжатие трафика
HASP	IPX TCP/IP Netbios	Контроль лицензий MCMed

Таблица 3. Внешние интерфейсы средств защиты АМИС (COM+ исполнение)

Название интерфейса	**Протокол/Метод использования**	**Целевая функция**
ADO	Activex COM+	Бизнес логика
SQL OLE DB	Microsoft Data Access Components	Аутентификация пользователя (login) Проверка прав доступа пользователя (авторизация)
MS DTC	Transaction Internet Protocol	Управление транзакциями Протоколирование операций

Таблица 4. Внешние интерфейсы средств защиты (уровень базы данных)

Название интерфейса	**Протокол/Метод использования**	**Целевая функция**
MS DTC	Transaction Internet Protocol	Управление распределенными транзакциями
SQL OLE DB	Microsoft Data Access Components	Унифицированный доступ к хранилищу данных

4.3.5. Средства защиты прикладных приложений:

Activex Data Objects

Назначение модуля и описание взаимодействия с другими модулями	Интерфейс программирования приложений для доступа к данным, разработанный компанией Microsoft (MS Access, MS SQL Server) и основанный на технологии компонентов Activex. ADO позволяет представлять данные из разных источников (реляционных баз данных, текстовых файлов, и т.п.) в объектно-ориентированном виде.
Тип	Модуль не реализовывает функции безопасности, а лишь предоставляет помощь в транспортировке данных к функциям безопасности.

Windows Sockets API

Назначение модуля и описание взаимодействия с другими модулями	WSA представляет собой техническую спецификацию, которая определяет, как сетевое программное обеспечение Windows будет получать доступ к сетевым сервисам, в том числе, TCP/IP. API определяет стандартный интерфейс между клиентским приложением и внешним стеком протоколов TCP/IP.
Тип	Модуль не реализовывает функции безопасности, а лишь предоставляет помощь в транспортировке данных к функциям безопасности.

Crypto API

Назначение модуля и описание взаимодействия с другими модулями	Интерфейс программирования приложений, который обеспечивает Windows-приложения стандартным набором функций для работы с криптопровайдером. CryptoAPI поддерживает работу с асимметричными и симметричными ключами, а также может работать с электронными сертификатами. Набор поддерживаемых криптографических алгоритмов зависит вот конкретного криптопровайдера. Интерфейс Crypto API разделен на 5 функциональных групп: 1. Базовые криптографические функции: • функции шифрования / дешифрования данных; • функции хеширования и получения цифровой подписи данных; • функции инициализации криптопровайдера и работы с полученным контекстом; • функции генерации ключей; • функции обмена ключами. 2. Функции кодирования/декодирования.

	3. Функции работы с сертификатами. 4. Многоуровневые функции обработки криптографических сообщений. 5. Низкоуровневые функции обработки криптографических сообщений.
Тип	Реализация функций безопасности: • «управление ресурсами (объектами защиты)»

HASP

Назначение модуля и описание взаимодействия с другими модулями	Аппаратно-программная система, предназначенная для защиты программ и данных от нелегального использования, пиратского тиражирования, несанкционированного доступа к данным, а также для аутентификации пользователей при доступе к защищенным ресурсам. Основой ключей HASP является специализированная микросхема ASIC (Application Specific Integrated Circuit), которая имеет уникальный для каждого ключа алгоритм работы. Принцип защиты заключается в том, что в процессе выполнения защищенная программа запрашивает подключенный к компьютеру ключ HASP. Если HASP возвращает правильный ответ и работает по заданному алгоритму, программа выполняется нормально. В противном случае она может завершиться, переключиться в демонстрационный режим или заблокировать доступ к отдельным функциям программы.
Тип	Реализация функций безопасности (реализует декларативную безопасность КЗЗ): • «идентификация и аутентификация»; • «управление ресурсами (объектами защиты)»; • «обеспечение аудита»

SQL OLE DB

Назначение модуля и описание взаимодействия с другими модулями	Набор программных COM-интерфейсов, предназначенный для доступа к разным источникам данных, таким как реляционные и нереляционные данные, текстовые и графические данные, архивы электронных сообщений, файловая система и бизнесы-объекты. Состоит из следующих компонентов: потребители (consumers), провайдеры данных (data providers) и сервисные компоненты (service components). Любой компонент ПО, использующий интерфейсы OLE DB, является потребителем. Потребители могут обращаться к данным через Activex Data Objects, представляющем собой высокоуровневый интерфейс к OLE DB. Провайдер данных –

	это компонент ПО, выполняющий манипуляции с данными. Провайдер данных выполняет следующие функции: 1. получение от потребителя запросов на получение или модификацию данных; 2. получение данных из БД или их модификация в БД; 3. возвращение данных потребителю. Провайдер сервисов реализует расширенный функционал, не поддерживаемый обычными провайдерами данных, например, сортировку и фильтрацию данных, обработку транзакций и SQL-запросов, и т.п. Сервисный компонент может обращаться к хранилищу данных непосредственно или с помощью соответствующего провайдера данных.
Тип	Модуль не реализовывает функции безопасности, а лишь предоставляет помощь в транспортировке данных к функциям безопасности.

MS DTC

Назначение модуля и описание взаимодействия с другими модулями	Координатор распределенных транзакций – составная часть служб компонентов Windows Component Services. В Component Services также включена технология COM+. COM+ используется при необходимости нетранзакционной передачи сообщений, а MS DTC – при необходимости транзакционной передачи. Служба выполняет сложные процедуры взаимодействия и проверки ошибок с целью обеспечения необходимой последовательности выполнения операций.
Тип	Модуль не реализовывает функции безопасности, а лишь предоставляет помощь в транспортировке данных к функциям безопасности.

COM+

Назначение модуля и описание взаимодействия с другими модулями	Стандарт создания ПО на основе взаимодействующих компонентов, каждый из которых может использоваться во многих программах одновременно. Служит основой для OLE, Activex-объектов и элементов управления Activex. COM+ предоставляет средства безопасности, которые используются для защиты COM-приложений. COM+ позволяет руководить защитой как с помощью атрибутов Component Services, так и программно, вызывая в коде специальные API-функции. Механизмы безопасности COM+ включают: • декларативная ролевая безопасность; • программная ролевая безопасность; • службы аутентификации;

	• делегирование прав. Ролевая безопасность является основным средством безопасности приложений COM+. Используя роли, можно автоматически создавать политику авторизации, указывая, кому какие ресурсы будут доступны. Ролевую безопасность можно применять программно, если приложение нуждается в более детальном контроле доступа.
Тип	Реализация функций безопасности (реализует декларативную безопасность КЗЗ): • «идентификация и аутентификация»; • «управление пользователями и их авторизацией»

SQL Server Management Studio

Назначение модуля и описание взаимодействия с другими модулями	Компонент СУБД SQL Server 2012, предназначенный для доступа, налаживание, управление и администрирование всех компонентов Microsoft SQL Server 2012. Предназначен для разработки и администрирования объектов баз данных и налаживания соответствующих объектов служб Analysis Services. Позволяет выполнять налаживание политики идентификации для группы пользователей и политики безопасности для всех компонентов Microsoft SQL Server 2012.
Тип	Реализация функций безопасности (реализует декларативную безопасность КЗЗ): • «идентификация и аутентификация»

SQL Server Logon

Назначение модуля и описание взаимодействия с другими модулями	Встроенный в СУБД графический интерфейс введения учетных данных администратора. Для процедуры авторизации взаимодействует с SQL Server Authentication Service.
Тип	Реализация функций безопасности (реализует декларативную безопасность КЗЗ): • «идентификация и аутентификация»

Transact SQL

Назначение модуля и описание	Транзакции к базе данных, предназначенные для работы с пользователями и группами. Позволяет создавать новых пользователей и группы, определяя для каждой из них

взаимодействия с другими модулями	политику безопасности. Для каждого пользователя настраивается доступ к соответствующим объектам защиты и порядок выполнения операций с ними.
Тип	Реализация функций безопасности (реализует декларативную безопасность КЗЗ): • «идентификация и аутентификация»; • «управление пользователями и авторизацией»

СУБД Logfile

Назначение модуля и описание взаимодействия с другими модулями	Отслеживание и протоколирование событий, которые происходят в SQL Server 2012, осуществляется подсистемой аудита. SQL Server 2012 позволяет настроить автоматический аудит событий. Подсистема аудита предоставляет возможность определять конкретные события или группы событий, относительно которых нужно проводить наблюдение. Модуль аудита имеет возможность определить формат журнала регистрации событий (SQL-таблицы, текстовый файл) и место его хранения.
Тип	Реализация функций безопасности (реализует декларативную безопасность КЗЗ): • «обеспечение аудита»

Модуль авторизации СУБД

Назначение модуля и описание взаимодействия с другими модулями	Структурный компонент SQL Server Management Studio, обеспечивающий применение соответствующих политик доступа к объектам защиты после прохождения администратором процедуры авторизации. В рамках подсистемы размежевания доступа взаимодействует с sys.credentials.
Тип	Реализация функций безопасности (реализует декларативную безопасность КЗЗ): • «идентификация и аутентификация»

sysadmin

Назначение модуля и описание взаимодействия с другими модулями	Роль системного администратора, которая автоматически создается во время инсталляции компонентов СУБД Microsoft SQL Server 2012, и позволяет осуществлять администрирование SQL Server 2012 и просмотр журналов регистрации событий. Системный администратор может изменять права доступа к объектам лишь под учетной записью sysadmin.
Тип	Реализация функций безопасности (реализует декларативную

	безопасность КЗЗ): • «идентификация и аутентификация»; • «обеспечение аудита»; • «управление пользователями и авторизацией»

dtexec

Назначение модуля и описание взаимодействия с другими модулями	Структурный компонент Integration Services, осуществляющий контроль за работой всех модулей СУБД Microsoft SQL Server 2012 и использующийся для удаленного доступа к консоли управления. Для защиты от неавторизованных действий имеет возможность настроить усиленную аутентификацию (с использованием ЭЦП) и установить пароль на выполнение отдельных действий (доступ к консоли, журналам регистрации событий).
Тип	Реализация функций безопасности (реализует декларативную безопасность КЗЗ): • «управление пользователями и авторизацией»

Database Engine (Защищенные объекты и разрешения)

Назначение модуля и описание взаимодействия с другими модулями	Структурные компоненты службы Database Engine СКБД Microsoft SQL Server 2012, предназначенные для управления ресурсами базы данных. Позволяют создавать защищенные ресурсы и определять порядок доступа к ним. Имеют встроенные механизмы налаживания условий, во время которых будет осуществляться блокирование/разблокирование ресурсов и контроль за их выполнением.
Тип	Реализация функций безопасности (реализует декларативную безопасность КЗЗ): • «разграничение доступа к ресурсам»

Plug-In

Назначение модуля и описание взаимодействия с другими модулями	Модернизация структурных компонентов СУБД Microsoft SQL Server 2012 выполняется путем инсталляции отдельных плагинов и их соответствующей настройки. Для этого в составе Microsoft SQL Server 2012 используется компонент Slipstream, котрый обеспечивает добавление новых плагинов и их конфигурацию или удаление без остановки работы основных компонентов СУБД.
Тип	Реализация функций безопасности (реализует декларативную безопасность КЗЗ): • «модернизация компонентов»

Просмотр журналов аудита

Назначение модуля и описание взаимодействия с другими модулями	Microsoft SQL Server 2012 предоставляет средства просмотра журналов аудита. Для просмотра журналов аудита с помощью встроенных в SQL Server 2012 средств пользователь должен быть членом в определенной роли sysadmin уровня сервера.
Тип	Реализация функций безопасности (реализует декларативную безопасность КЗЗ): • «обеспечение аудита»

SQL Server 2012 Data Recovery Tool

Назначение модуля и описание взаимодействия с другими модулями	В процессе функционирования Microsoft SQL Server 2012 могут возникать следующие типы отказов, которые приводят к прерыванию предоставления услуг: • невозможность запуска сервера; • сервер не отвечает на запросы участников. В случае, если отказы связаны с повреждением компонентов SQL Server 2012 вследствие отказов компонентов среды функционирования (повреждение компонентов ОС Windows, повреждение носителей данных), требуется повторная инсталляция SQL Server 2012. В прочих случаях отказы могут быть устранены без повторной инсталляции SQL Server 2012. Для этого Microsoft SQL Server 2012 предоставляет пользователю, который является членом роли sysadmin (SA), следующие инструменты: Использование службы резервного восстановления работы SQL Server 2012 Data Recovery Tool, которая позволяет загрузить последнюю удачную конфигурацию СУБД и восстановить объекты БД из резервной копии.
Тип	Реализация функций безопасности (реализует декларативную безопасность КЗЗ): • «восстановление после сбоев»

SQL Server 2012 Native Client

Назначение модуля и описание взаимодействия с другими модулями	SQL Server 2012 Native Client представляет собой клиентское приложение к СУБД Microsoft SQL Server 2012 и используется как дополнительный интерфейс доступа системного администратора к консоли управления SQL Server 2012. SQL Server 2012 Native Client устанавливается в качестве отдельного ПО в ОС Windows и использует механизмы безопасности

	операционной системы. Для идентификации в системе взаимодействует с SQL Server Logon, а во время администрирования может взаимодействовать с другими компонентами SQL Server 2012.
Тип	Реализация функций безопасности (реализует декларативную безопасность КЗЗ): • «идентификация и аутентификация»; • «управление пользователями и авторизацией»

SQL Server 2012 Server Audit

Назначение модуля и описание взаимодействия с другими модулями	Server Audit представляет собой структурный компонент СУБД Microsoft SQL Server 2012, отвечающий за сбор, хранение и работу с журналами регистрации событий. Модуль осуществляет накопление событий, которые поступили от компонентов и служб Microsoft SQL Server 2012, их структурирование и надежное сохранение. Системный администратор имеет возможность формировать индивидуальные отчеты или использовать стандартные табличные отчеты с помощью служб Reporting Services.
Тип	Реализация функций безопасности (реализует декларативную безопасность КЗЗ): • «обеспечение аудита»

4.3.6. Функциональный профиль защищенности АМИС.

АМИС, введенная в НИФП НАМН, получила экспертное заключение Государственной службы специальной связи и защиты информации на соответствие требованиям нормативных документов системы технической защиты информации в Украине с уровнем гарантий Г-2, и положительное заключение Государственного учреждения "Медицинский центр телемедицины МЗ Украины".

Продолжение статьи читайте в следующей **ЧАСТИ 2**.