ГОСУДАРСТВЕННЫЙ СТАНДАРТ УЗБЕКИСТАНА

ИНФОРМАЦИОННАЯ ТЕХНОЛОГИЯ

Требования к базам данных и обмену информацией между органами государственного управления и государственной власти на местах

Узбекское агентство стандартизации, метрологии и сертификации

Ташкент

Предисловие

1 РАЗРАБОТАН Центром развития и внедрения компьютерных и информационных технологий UZINFOCOM

2 ВНЕСЕН Узбекским агентством связи и информатизации (УзАСИ)

3 УТВЕРЖДЁН И ВВЕДЕН В ДЕЙСТВИЕ постановлением Узбекского агентства стандартизации, метрологии и сертификации (агентство «Узстандарт») от 04.10.2007 № 05-52

4 ВВЕДЕН ВПЕРВЫЕ

Информация о введении в действие (прекращении действия) настоящего стандарта и изменений к нему на территории Узбекистана публикуется в указателе, издаваемом агентством «Узстандарт»

Содержание

ГОСУДАРСТВЕННЫЙ СТАНДАРТ УЗБЕКИСТАНА

АХБОРОТ ТЕХНОЛОГИЯСИ
Маълумотлар базалари ва жойлардаги давлат бошқаруви ҳамда давлат ҳокимияти органлари ўртасида ахборот алмашишига қўйиладиган талаблар

ИНФОРМАЦИОННАЯ ТЕХНОЛОГИЯ
Требования к базам данных и обмену информацией между органами государственного управления и государственной власти на местах*

Information technology
Databases and state authorities information exchange by information between organ of state management and state authorities on places requirements

Дата введения 2008-01-01
2018-01-01

1 Область применения

Настоящий стандарт устанавливает основные требования к базам данных на стадиях разработки, эксплуатации и технического сопровождения программного обеспечения баз данных и при обмене информацией между информационными системами органов государственного управления и государственной власти на местах.

Требования, установленные настоящим стандартом, обязательны для применения во всех органах государственного управления и государственной власти на местах.

2 Нормативные ссылки

В настоящем стандарте использованы ссылки на следующие нормативные документы:

ГОСТ 19.101-77 Единая система программной документации. Виды программ и программных документов

ГОСТ 34.321-96 Информационные технологии. Система стандартов по базам данных. Эталонная модель управления данными

(Исключен, Изм. № 1)

O‘z DSt 1047:2003 Информационные технологии. Термины и определения

O‘z DSt 1092:2009 Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи

---

* **С изменением № 1, утвержденным постановлением агентства «Узстандарт» от 03.01.2013 № 05-42**

(Измененная редакция, Изм. № 1)

O‘z DSt 1105:2009 Информационная технология. Криптографическая защита информации. Алгоритм шифрования данных

(Измененная редакция, Изм. № 1)

O‘z DSt 1985:2010 Информационная технология. Виды комплектность и обозначение документов при создании информационных систем

(Включен дополнительно, Изм. № 1)

Примечание – При пользовании настоящим стандартом целесообразно проверить действие ссылочного стандарта на территории Узбекистана по соответствующему указателю стандартов, составленному по состоянию на 1 января текущего года, и по соответствующим информационным указателям, опубликованным в текущем году. Если ссылочный документ заменен (изменен), то при пользовании настоящим стандартом следует руководствоваться замененным (измененным) стандартом. Если ссылочный документ отменен без замены, то положение, в котором дана ссылка на него, применяется в части, не затрагивающей эту ссылку.

3 Термины, определения и сокращения

3.1 В настоящем документе применены следующие термины с соответствующими определениями по O’z DSt 1047:

3.1.1 алгоритм: Упорядоченный конечный набор четко определенных правил для решения задач за конечное число шагов.

3.1.2 аутентификация: Проверка и подтверждение подлинности определенных реквизитов или идентификаторов, предъявляемых субъектом.

3.1.3 база данных; БД: Совокупность данных, организованных по определенным правилам, предусматривающим общие принципы описания, хранения и манипулирования данными, независимо от прикладных программ.

3.1.4 браузер: Клиентская программа для работы в WWW.

3.1.5 данные: Информация, являющаяся объектом обработки в телекоммуникационных системах.

3.1.6 дешифрование: Процесс, противоположный шифрованию и связанный с восстановлением исходного текста из зашифрованного при отсутствии ключа шифрования.

3.1.7 доступность информации: Состояние информации и её носителя, при котором обеспечивается беспрепятственное и своевременное получение пользователями предназначенной для них информации.

3.1.8 Интернет, сеть Интернет: Глобальная информационная система, которая:

- логически связана унитарным адресным пространством, основанном на IP-протоколе или на его перспективных расширениях/последователях;

- может поддерживать коммуникации, используя Transmission Control Protocol/ Internet Protocol (TCP/IP) или его расширения/последователи и/или IP-совместимые протоколы;

- предоставляет, использует или делает доступными (для всех или конфиденциально) сервисы высоко уровня, основанные на коммуникациях и связанной с ними инфраструктуре, здесь определенной.

2 Глобальное (всемирное) множество независимых компьютерных сетей, соединенных между собой для обмена информацией по стандартным открытым протоколам.

3 Совокупность общедоступных информационно-телекоммуникационных сетей, взаимодействие между которыми обеспечивается применением межсетевого протокола с одноименным названием.

3.1.9 информатизация: Организационный социально-экономический и научно-технический процесс создания условий для удовлетворения информационных потребностей юридических и физических лиц в информации, с использованием информационных ресурсов, информационных технологий и информационных систем.

3.1.10 информационная безопасность: Совокупность свойств информации и поддерживающей инфраструктуры быть защищенной от случайных или преднамеренных воздействий естественного или искусственного характера.

3.1.11 клиент-сервер: Общий способ описания услуг и модель пользовательских процессов (программ) для этих услуг.

Примечание - Выполнение задачи разделяется на две части: инициирование запросов системой конечного пользователя (клиентской частью) и ответ на них серверной частью (хранилищем ресурсов). Под системой "клиент-сервер" понимают совокупность клиентов, серверов и сети в целом.

3.1.12 конфиденциальность информации: Состояние информации и носителя, при котором обеспечиваются предотвращение несанкционированного ознакомления с ней или несанкционированного документирования (снятия копий).

3.1.13 криптографический метод защиты информации: Метод защиты информации, основанный на принципе её шифрования и кодирования. Криптографический метод может быть реализован как программными, так и аппаратными средствами.

3.1.14 несанкционированный доступ к информации; НСД: Доступ субъекта к объекту или информации в нарушение установленных в системе правил разграничения доступа.

3.1.15 обеспечение программное; ПО: Совокупность программ системы обработки информации и программных документов, необходимых для эксплуатации этих программ.

3.1.16 обмен данными электронный: Электронная передача информации с одного компьютера на другой с использованием согласованного стандарта структуризации информации.

3.1.17 пользователь (потребитель) информации: Субъект, обращающийся к информационной системе или посреднику за получением необходимой ему информации (информационных продуктов) и пользующийся ею (ими).

3.1.18 продукт программный: Программные средства, предназначенные для поставки, передачи, продажи пользователю.

3.1.19 протокол: Совокупность правил и соглашений, регламентирующих формат и процедуру передачи данных между двумя или несколькими независимыми устройствами или процессами.

3.1.20 сервер: 1 Совокупность аппаратного и программного обеспечения (программа-сервер), позволяющая компьютеру предоставлять услуги другому компьютеру. Компьютеры работают с программой-сервером с помощью программ-клиентов.

2 Программа для сетевого компьютера, позволяющая предоставлять услуги одного компьютера другому.

Примечание - Обслуживаемые компьютеры сообщаются с сервер-программой при помощи пользовательской программы (клиент-программы).

3 Вычислительная машина (система), управляющая определенным видом ресурсов сети.

Примечание - Различают файл-сервер, сервер приложений, факс-серверы, почтовые, коммуникационные, веб-серверы и др.

3.1.21 сеть корпоративная вычислительная: Информационно-вычислительная сеть, объединяющая локальные сети отдельных предприятий (фирм, организаций, акционерных обществ и т.п.) корпорации в масштабе как одного государства, так и нескольких государств.

3.1.22 сеть сетей всемирная, паутина всемирная, World Wide Web: Гипертекстовая система поиска ресурсов в Интернете и доступа к ним.

Примечание - World Wide Web предоставляет набор услуг Интернета, позволяющий просмотреть данные, хранящиеся в компьютерах этой сети, через систему связывающих их гиперссылок.

3.1.23 сеть Ethernet: Широковещательная компьютерная сеть, имеющая архитектуру Ethernet.

3.1.24 система информационная: 1 Система для подготовки, отправления, получения, хранения или иной обработки сообщений данных. 2 Организационно упорядоченная совокупность информационных ресурсов, информационных технологий и средств связи, позволяющая осуществлять сбор, хранение, поиск, обработку и пользование информацией. 3 Любая система, связанная с накапливанием, хранением или обработкой информации.

3.1.25 средство криптографической защиты информации (СКЗИ): Средство, осуществляющее криптографическое преобразование информации для обеспечения ее безопасности.

3.1.26 целостность информации (данных): Состояние информации (данных) и носителя, при котором обеспечиваются неделимость и предотвращение несанкционированного или преднамеренного уничтожения, искажения, утечки, хищения, подделки, подмены в целом и её отдельных составных частей.

3.1.27 шифрование: Совокупность обратимых преобразований информации (данных) в соответствии с криптографическим алгоритмом и ключом для надежного сокрытия ее истинного содержания.

3.2 В настоящем стандарте применены следующие сокращения:

БД - база данных.
ИР – информационный(ые) ресурс(ы).
ИС – информационная система.
КС – корпоративная сеть.

ПО – программное обеспечение.

СКЗИ – средства криптографической защиты информации.

СУБД – система управления базой данных.

ЭЦП – электронная цифровая подпись.

API - Application Programming Interface – Интерфейс программирования приложений.

ASCII – American Standard Code for Information Interchange - Американский стандартный код для обмена информацией.

DMZ - Demilitarized Zone - демилитаризованная зона — технология обеспечения защиты информационного периметра, при которой сервера, отвечающие на запросы из внешней сети, или направляющие туда запросы, находятся в особом сегменте сети.

FTP – File Transfer Protocol – Протокол передачи файлов.

HTTP – Hypertext Transfer Protocol - Протокол передачи гипертекста.

HTTPS – Расширение протокола HTTP.

IETF – Internet Engineering Task Force - Открытое международное сообщество проектировщиков, учёных, сетевых операторов и провайдеров.

IMAP – Internet Message Access Protocol – интернет-протокол прикладного уровня для доступа к электронной почте.

ISO - International Organization for Standardization - Международная организация по стандартизации.

MIME – Multipurpose Internet Mail Extensions - стандарт, описывающий передачу различных типов данных по электронной почте.

OSI - Open Systems Interconnection Reference Model — модель взаимодействия открытых систем — абстрактная модель для сетевых коммуникаций и разработки сетевых протоколов.

PNG – Portable Network Graphics – растровый формат хранения графической информации, использующий сжатие без потерь.

SGML – Standard Generalized Markup Language – стандартный общий язык разметки.

SMTP – Simple Mail Transfer Protocol - простой протокол передачи почты.

SQL – Structured Query Language – язык структурированных запросов.

SVG – Scalable Vector Graphics – масштабируемая векторная графика.

VPN – Virtual Private Network – виртуальная частная сеть.

VRML – Virtual Reality Modeling Language – язык моделирования виртуальной реальности.

W3C - World Wide Web Consortium - консорциум "Всемирной паутины" – сети Интернет.

XHTML – Extensible Hypertext Markup Language – расширяемый язык разметки гипертекста.

XML - Extensible Markup Language - расширяемый язык разметки.

4 Основные требования к управлению данными при обмене информацией между информационными системами

4.1 Информационные системы

Информационная система может быть размещена на одной или нескольких компьютерных системах. Если информационная система размещена на нескольких компьютерных системах, то она будет рассматриваться как распределенная информационная система.

Данные поступают в информационную систему и исключаются из нее, и эти взаимодействия могут осуществляться или людьми, или процессами.

Управление данными в настоящем стандарте касается организации и управления постоянными данными. Постоянные данные - это данные, которые хранятся в информационной системе в течение определенного периода времени. Система, которая выполняет функцию организации и управления постоянными данными, называется системой управления данными.

[ГОСТ 34.321].

4.2 Обмен данных в информационной системе

4.2.1 Обмен данных в информационной системе позволяет нескольким пользователям работать с одной и той же информацией, хранящейся в базе данных.

В настоящем стандарте под обменом данных понимается движение и, как результат, объединение информации. Наиболее актуальные и типичные аспекты обмена данными следующие:

- обмен данными между территориально удаленными друг от друга точками ввода информации;
- обмен данными между системами учета с разным назначением (бухгалтерский учет, оперативный учет, управленческий учет);
- обмен данными в системе «поставщик-покупатель», «заказчик-исполнитель» и т.д.;

Общими требованиями, предъявляемые к системам обмена данными, являются обеспечение единичного ввода информации (данных), используемой в одной или нескольких базах данных, соблюдение общих правил целостности базы данных, устойчивость системы к сбоям и защищенность от несанкционированного доступа.

4.2.2 При обмене критически важными данными между информационными системами должен быть использован защищенный канал связи, основанный на протоколе HTTPS или с применением виртуальной частной сети (VPN).

4.2.3 При передаче конфиденциальной информации должны использоваться средства криптографической защиты информации (СКЗИ). В случае передачи электронных документов, данные документы должны быть заверены электронной цифровой подписью (ЭЦП) выданной сертифицированным центром регистрации

ключей Республики Узбекистан. При этом должен использоваться единый алгоритм шифрования данных, отвечающий стандарту O’z DSt 1105.

4.2.4 При обмене не критически важной (публичной) информацией использование СКЗИ не обязательно.

4.3 База данных и схема

Постоянные данные в среде базы данных заключают в себе схему и базу данных. Схема - это описания содержания, структуры и ограничения целостности, используемые для создания базы данных. База данных - это набор постоянных данных, определенных с помощью схемы.

Система управления данными использует определения данных в схеме, чтобы предоставлять возможность доступа и управлять доступом к данным в базе данных.

4.4 Средство моделирования данных

Схему разрабатывают в соответствии с совокупностью правил структурирования данных. Каждая совокупность правил структурирования данных может иметь связанную с ней совокупность правил манипулирования данными, определяющую процессы, которые должны быть выполнены над структурированными данными.

Правила структурирования данных и правила манипулирования данными - это средства моделирования данных.

Язык баз данных используется, чтобы определить схему согласно правилам структурирования данных и процессы в соответствии со связанными с ними правилами манипулирования данных.

Примерами классов средства моделирования данных являются реляционный, сетевой и иерархический классы. Правила структурирования данных для двух средств моделирования данных в различных классах должны быть похожими, как, например, для сетевого и реляционного, но связанные с ними средства манипулирования данными могут отличаться.

4.5 Поддержка управления данными

4.5.1 Требования, накладываемые информационными системами на управление данными, которые не зависят от конкретных требований информационной системы хранения и манипулирования данными, следующие:

- поддержка жизненного цикла информационных систем;
- управление конфигурацией информационных систем, управление версиями и варианты;

- параллельная обработка;
- управление транзакциями базы данных;
- проектирование производительности;
- идентификация объектов данных;
- расширение средства моделирования данных;
- поддержка для различных средств моделирования данных в интерфейсе пользователя;
- ведение контрольных журналов;
- восстановление распределенной базы данных;
- реструктуризация логических данных;
- реорганизация физической памяти.

Управление данными обеспечивает обобщенные средства удовлетворения этих требований так, чтобы не было необходимости разрабатывать конкретные решения для каждой информационной системы.

4.5.2 Управление конфигурацией, управление версиями и варианты

Деятельность по управлению изменениями, осуществляемыми в конфигурации информационной системы за какой-то период времени, называется управлением конфигурацией. Следует идентифицировать дискретные версии системной конфигурации в конкретные моменты времени, а также продолжать следить за конфигурацией, которая принадлежит каждой конкретной версии.

Когда информационная система находится в различных фазах жизненного цикла, то для параллельного существования в различных формах могут потребоваться постоянные данные и процессы, которые являются частью информационной системы.

Две формы процесса могут считаться различными вариантами. Это означает, что каждый вариант удовлетворяет различным требованиям (таким, как различие внутренних представлений памяти) и ни один вариант не предназначен для того, чтобы изменять другой.

4.5.3 Параллельная обработка

Информационная система является ресурсом, который может быть распределен между несколькими пользователями одновременно. Пользователь может инициировать запрос на услуги системы управления данными, которыми можно управлять более целесообразно, если доступ к данным может быть сделан одновременно. Среда управления данными должна гарантировать выполнение отдельного намерения каждого пользователя таким образом, чтобы он согласовывался с его восприятием данных.

Параллельные взаимодействия не должны влиять друг на друга, а параллельная обработка не должна влиять на целостность данных.

4.5.4 Управление транзакцией базы данных

Транзакция базы данных определяется как ограниченная последовательность взаимодействий базы данных, которые вместе образовывают логическую единицу работы. В случаях обновления базы данных транзакция базы данных является последовательностью шагов обновления, которые из-

меняют содержание базы данных из одного непротиворечивого состояния в другое.

Требования к управлению транзакциями базы данных следующие:

- следствия всех изменений должны оставаться в базе данных после завершения транзакции базы данных или ни одни из них не остаются;

- после завершения работы транзакция базы данных оставляет базу данных в непротиворечивом состоянии;

изменения, осуществленные транзакцией базы данных, должны быть невидимы для любой другой параллельной транзакции базы данных и наоборот;

- заблокированная один раз система должна гарантировать, что результаты транзакции базы данных переживают любые последующие отказы.

Параллельное выполнение нескольких транзакций базы данных должно быть эквивалентным в том смысле, что выполнение их параллельно является таким же самым, как если бы они выполнялись последовательно.

4.5.5 Проектирование производительности

Необходимо создавать возможности для улучшения производительности любой информационной системы: прикладной системы, системы словарей или системы, в которой интегрируются обе системы.

Основой получения таких улучшений является накопление статических данных о частоте использования процессов и частоте доступа и изменений в объектах данных.

4.5.6 Идентификация объектов

Каждый объект в среде базы данных должен быть уникальным. Это должно быть достигнуто путем присвоения каждому объекту уникального имени с использованием вложенной иерархии пространств имен.

Для того чтобы дать уникальное имя в среде базы данных, может потребоваться, чтобы имена были определены с помощью имен во внешнем пространстве имен.

Именем может быть имя, назначенное пользователем или системой управления данными.

Требование именования существует для прикладных систем, систем словарей и других типов информационной системы. Если имеется более чем одна среда базы данных в компьютерной системе, тогда требуется, чтобы одна среда была отличима от другой.

4.5.7 Расширение средства моделирования данных

Средство моделирования данных может быть типовым для систем управления данными. Одновременно может возникнуть требование добавлять типы данных и связанные с ними процессы.

Примером этого требования является полная текстовая обработка в соединении с обработкой структурированных данных типичным средством моделирования данных.

[ГОСТ 34.321].

4.6 Дополнительные эксплуатационные требования для поддержки управления данными в распределенной информационной системе

4.6.1 В распределенной информационной системе объекты, принадлежащие одной информационной системе, распределяются на два или более компьютера. Когда распределяемые объекты являются объектами базы данных, система является распределенной системой баз данных.

Запрашиваемая услуга может быть доступна из множества вычислительных устройств, вмещающих дублированные данные.

Эксплуатационные требования, зависящие от распределяемых данных, следующие:

- управление распределением;
- управление транзакцией базы данных;
- связь;
- экспорт/импорт;
- независимость распределения.

Некоторые из этих требований также применимы к информационной системе, которая включает более чем одну среду базы данных в единственной компьютерной системе.

Необходимо поддерживать следующие возможности:

a) распределенную систему базы данных, в которой составные среды базы данных проектируются таким образом, что возможно взаимодействие между любой парой;

b) систему баз данных, в которой две или более отдельно спроектированные системы баз данных объединяются, в определенном смысле, после периода раздельного использования и создаются для функционирования как одна распределенная система баз данных;

c) ситуацию, в которой каждая среда базы данных согласуется множеством стандартов и, следовательно, может взаимодействовать (возможно, на специальной основе) с другими средами баз данных, каждая из которых была спроектирована отдельно, но согласно тем же самым стандартам.

4.6.2 Управление распределением данных

Управление распределением включает управление фрагментацией, управление дублированием и автономию месторасположения.

Могут использоваться следующие способы распределения данных:

a) назначить все экземпляры определенного типа данных на одну среду базы данных (нефрагментированный способ);

b) назначить множество экземпляров данных (возможно различных типов) на две или более среды баз данных (горизонтальная фрагментация);

c) назначить экземпляры различных частей того же самого типа на две или более среды баз данных (вертикальная фрагментация);

d) комбинация пунктов b) и c) (комбинированная горизонтальная и вертикальная фрагментация).

Горизонтальная фрагментация предназначена для записи на вычислительном устройстве только экземпляры данных, которые относятся к этому вычислительному устройству.

Вертикальная фрагментация предназначена для записи на конкретном вычислительном устройстве только экземпляры данных, которые относятся к нему.

Если фрагментация поддерживается в распределенной среде, то не требуется, чтобы пользователь информационной системы знал, как данные фрагментируются или распределяются между компьютерными системами.

По причинам производительности или защиты от сбоя компьютерной системы необходимо обеспечить копию всей базы данных или ее части. Такие дублированные данные должны храниться в компьютерной системе, отличной от той, в которой данные первоначально создаются и в дальнейшем управляются. Требование для фрагментации должно быть объединено с требованием дублирования так, чтобы копии множества фрагментов назначались на две или более среды баз данных. Информация о том, какие объекты, в какой среде данных являются доступными, должна быть доступна в каждой среде.

Необходимо иметь возможность управлять содержанием точных копий, когда данные обновляются. Алгоритмы, которые обеспечивают контроль точных копий, должны также гарантировать обновления в транзакциях.

Требования для дублирования данных на различных компьютерных системах должны соблюдаться для того, чтобы системы были автономными, настолько, насколько это возможно. Такие требования относятся к производительности, доступности данных в течение сбоя связи и к административным вопросам, таким как учет системных ресурсов и идентифицирование пользователей.

4.6.3 Управление транзакцией базы данных

Необходимо синхронизировать действия локальных систем управления транзакцией, чтобы гарантировать, что изменения в распределенных данных заканчиваются непротиворечивым состоянием для каждой базы данных, а также для всех баз данных.

Обработка в одной компьютерной системе может осуществляться параллельно с обработкой в другой компьютерной системе без влияния на целостность данных в каждой из компьютерных систем.

4.6.4 Связь между информационными системами

Необходимо обеспечить информационным системам возможность связываться друг с другом.

Для обмена объектов данных необходимо, чтобы средство моделирования данных, в соответствии с которым объекты данных структурируются, было использовано в каждой из компьютерных систем.

Необходимо иметь средства, которые предотвращают потерю целостности баз данных из-за таких видов сбоя связи:

- сообщение может быть потеряно во время передачи;

- сообщение не может поступить в надлежащем виде из-за ошибок трансляции и ретрансляции;

- при некоторых обстоятельствах сбой связи трудно отличить от сбоя на удаленном вычислительном устройстве.

Следует определить необходимую степень дублирования данных.

4.6.5 Экспорт-импорт данных

Данные экспортируются из одной среды и импортируются в другую. Для этого необходимо иметь копию части или всей базы данных, с определением данных или без него. Экспортируемые данные могут быть импортированы во многие другие среды, если это требуется, а также сохраняться.

4.6.6 Независимость распределения данных

Прикладной процесс должен иметь доступ к данным в распределенной базе данных таким образом, чтобы он не зависел от того, как могут быть распределены данные.

4.7 Форматы обмена информацией

Под форматами обмена информацией между информационными системами в настоящем документе понимают форматы, предназначенные для обеспечения обмена информацией между информационными системами органов государственного управления и государственной власти на местах.

Форматы обмена информацией являются средством согласования структуры и характера записей в массивах и базах данных, являющихся объектами передачи и приема в процессах информационного взаимодействия систем.

В частности, под форматами в настоящем документе понимают:

a) совокупность правил записи и представления данных в памяти, в базе данных, на экране монитора или на внешнем носителе. Основной структурной единицей формата является элемент данных, который записывается в поле данных формата. Формат определяет перечень полей данных, их характеристики, содержание вносимых данных и их размещение;

b) элемент языка, в символическом виде описывающий представление информационных объектов в записи (в т. ч. в файле, базе данных и т. п.).

c) способ кодирования записи информации, например, текстовый формат – представление текстовой информации в Unicode*.

Основой построения информационной системы является определение минимального набора общих форматов данных. Эти форматы используются как для хранения, так и для обмена информацией между программами. При выборе рекомендованных форматов данных предпочтение отдается стандартам World Wide Web Consortium (W3C). Стандарты W3C существуют для большинства используемых видов данных, отличаются проработанностью и широко поддерживаются во всем мире. Ниже перечислены основные форматы данных.

* Стандарт кодирования символов, позволяющий представить знаки практически всех письменных языков

Текст. Для представления текстовых данных применяются форматы, основанные на SGML. Такие форматы ориентированы прежде всего на структуру, а не на внешнее оформление.

Основным видом текстовых данных должен быть гипертекст. Форматы представления описываются стандартами W3C: HTML, XHTML, XML. Для внутреннего хранения информации допускается использовать другие форматы, основанные на SGML.

В случае если необходимо предоставить жестко отформатированный документ для вывода на принтер, используется формат W3C SVG.

Растровая графика.

W3C PNG используется для сохранения рисунков и иных изображений, содержащих большие области одного цвета.

Векторная графика.

В качестве основного формата используется формат SVG, описываемый стандартом W3C.

Трехмерная графика.

Для представления трехмерных векторных изображений используется формат W3C VRML.

Звук и видео.

Допускается использование для этих типов данных стандарт OGG.

5 Требования к протоколам обмена информацией между информационными системами

Программная реализация обмена информацией между приложениями взаимодействующих информационных систем должна поддерживать протоколы прикладного уровня эталонной модели взаимосвязи открытых систем OSI, отражающие:

- роли взаимодействующих приложений;
- прямые транзакции, прикладные подтверждения, запросы и ответы;
- наличие коммутирующих агентов.

Приложения взаимодействующих информационных систем, поддерживающие форматы обмена информацией, должны опираться на стандартные протоколы уровней модели OSI.

6 Основные требования к программному обеспечению баз данных

6.1 Общая характеристика построения системы.

ПО системы должно строиться по принципам клиент-серверной архитектуры. Общая схема архитектуры ПО системы приведена на рисунке 1. Основными компонентами ПО системы должны быть система пользовательского интерфейса, системное приложение и система хранения данных.

ПО системы пользовательского интерфейса и системы хранения данных должно выполняться на серверах организации, обслуживаемых техническим персоналом организации. За исключением специальных случаев ПО

прикладных приложений также должно выполняться на серверах организации. Для упрощения сопровождения прикладного ПО разработчикам и владельцам прикладного ПО должен быть предоставлен эффективный доступ к вычислительным мощностям для выполнения прикладного ПО.

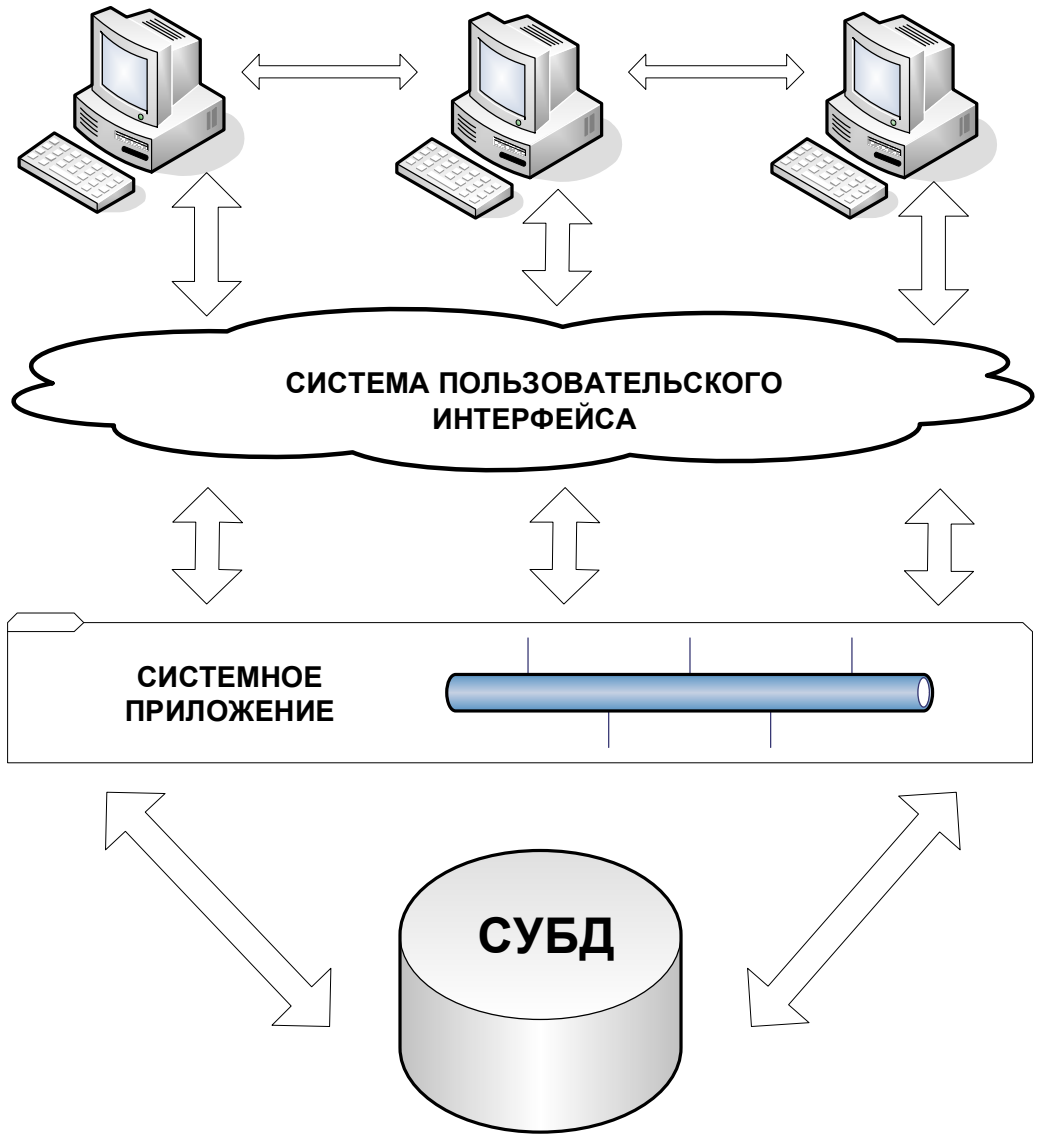

Рисунок 1 - Общая схема архитектуры ПО системы.

Основными требованиями к ПО баз данных являются: доступность, многопользовательский режим, среда и масштабируемость, информационная безопасность и надежность.

6.2 Доступность

6.2.1 В качестве пользовательского интерфейса БД должен использоваться интерфейс ПО, разработанный для доступа к БД. Допускается использование Web-браузера пользователя.

6.2.2 Должен использоваться пользовательский интерфейс БД, ориентированный на использование графического ПО. Однако должна существовать возможность осуществлять доступ к БД и при помощи текстового ПО.

6.2.3 ПО БД не должно зависеть от национального языка текстовых данных. Текстовые данные должны храниться и обрабатываться в кодировке Unicode. В случае отличия свойств текстовых данных от принятых соответствующим стандартом по умолчанию (например, английский язык, кодировка символов ASCII), эти свойства должны быть явно заданы и передаваться ПО клиента средствами используемого протокола передачи данных (например, HTTP) или формата данных (например, MIME).

6.3 Многопользовательский режим

6.3.1 ПО БД должно поддерживать одновременную работу произвольного числа пользователей (в зависимости от числа одновременных подключений). Для каждого пользователя должно поддерживаться несколько одновременных сессий работы (как с одного компьютера, так и с нескольких). В случае отсутствия активности пользователя какой-либо сессии в течение определенного промежутка времени, эта сессия должна автоматически завершаться.

6.3.2 Необходимо исключить возможность взаимных блокировок различных сессий. То есть действия одного пользователя не должны ни вызывать задержку выполнения команд другого, ни требовать от ПО БД ожидания каких-либо действий пользователя.

6.4 Среда и масштабируемость

6.4.1 Программная система БД должна быть рассчитана на функционирование в корпоративной сети (КС) со стабильной пропускной способностью.

6.4.2 При наличии для конкретного приложения традиционных протоколов передачи данных (например, для электронной почты это SMTP и IMAP), именно они должны использоваться для работы с соответствующими данными.

6.4.3 Для распределения вычислительной нагрузки и обеспечения надежного функционирования системы должно поддерживаться выполнение программных процессов, составляющих ПО, на различных компьютерах, подключенных к КС. Также должно поддерживаться выполнение нескольких экземпляров программных приложений, работающих с одним источником данных. При этом не должно возникать взаимных блокировок приложений.

6.5 Информационная безопасность

6.5.1 При разработке протоколов взаимодействия компонентов ПО необходимо учитывать то, что КС по умолчанию является незащищенной средой передачи данных. Поэтому для передачи критически важных данных по сети необходимо использовать криптографический метод защиты информации. Возможно расположение серверных компьютеров для ПО в DMZ (demi-

litarized zone) – сервере или подсети с основными сервисами, такими как HTTP-сервер, FTP-сервер, SMTP-сервер, расположенные в сегменте между непосредственно КС и недоверительной сетью (Интернет).

6.5.2 Любой пользователь, осуществляющий доступ к БД должен быть аутентифицирован системой. Аналогично сервер, предоставляющий критически важную информацию, должен быть аутентифицирован ПО либо клиента, либо другой системы (в зависимости от того, кому передаются данные). Аутентификационная информация (логическое имя и пароль) должны передаваться по сети в виде, делающим их перехват невозможным или нецелесообразным. Пароль должен быть зашифрован алгоритмом шифрования (например, MD5 или DES) и состоять из большого числа символов (рекомендуется не менее 8 символов, желательно разного регистра) с целью усложнения его дешифрования в случае перехвата. Аутентификация в среде клиент-сервер должна происходить только от доверенного источника.

6.5.3 ПО должно быть устойчиво к некорректным действиям пользователей и других программных процессов.

6.5.4 ИС органов государственного управления и государственной власти на местах должны учитывать общие требования к информационной безопасности, определенные государственными стандартами: O'z DSt 1105, O'z DSt 1092, RH 45-170.

Указанные требования направлены на обеспечение доступности, целостности, конфиденциальности информации в ИС. Выделены 10 ключевых элементов управления информационной безопасностью:

- политика информационной безопасности;
- распределение ответственности за информационную безопасность;
- образование и тренинг персонала по информационной безопасности;
- отчетность по инцидентам с безопасностью;
- защита от вирусов;
- обеспечение непрерывности работы ИС;
- контроль копирования лицензируемого программного обеспечения;
- защита архивной документации организации/учреждения;
- защита персональных данных;
- выполнение политики информационной безопасности.

На основе этих общих критериев должны быть разработаны профили средств защиты информации.

6.5.5 ИС органов государственного управления и государственной власти на местах должны иметь средства защиты от несанкционированного доступа.

6.5.6 В ИС органов государственного управления и государственной власти на местах должны быть предусмотрены средства защиты от вирусов для всех узлов КС – серверов и рабочих станций. Регламенты администрирования в ИС должны предусматривать централизованную установку и запуск антивирусного ПО во всех узлах сети. Режимы проверки должны обеспечивать контроль распространения вирусов по сети.

Антивирусное ПО должно обеспечивать постоянную защиту программ и данных ИС в фоновом режиме независимо от функционирования приложений. Применяемое в ИС антивирусное ПО должно обладать функциональной полнотой и обеспечивать:

- сканирование;
- мониторинг в режиме реального времени;
- проверку целостности программ и файлов данных;
- обнаружение неизвестных вирусов;
- контроль поведения узлов сети.

В ИС должно применяться только сертифицированное антивирусное ПО. Оно должно быть обеспечено постоянной поддержкой и обновлением со стороны поставщика.

Применяемое антивирусное ПО должно быть многоплатформным, т.е. обеспечивать поддержку рабочих станций пользователей и серверов, функционирующих под управлением разных операционных систем.

В составе средств антивирусной защиты должны быть предусмотрены три категории антивирусного ПО:

- для пользователей сети;
- для технических специалистов;
- для системных и сетевых администраторов.

6.6 Надежность

6.6.1 В случае сбоя в работе сетевого соединения между двумя процессами должно осуществляться его автоматическое восстановление. В случае обрыва в сетевом соединении клиент-сервер пользователь в обязательном порядке должен пройти повторную авторизацию. При аварийном завершении процесса должен происходить его автоматический перезапуск.

6.6.2 Если алгоритм работы подсистемы ПО предполагает наличие каких-либо логических состояний, в которых находится подсистема, то должен существовать механизм сохранения этого состояния в энергонезависимой памяти (в частности при остановке подсистемы). Сохраненные данные в любой момент времени должны соответствовать корректному логическому состоянию подсистемы таким образом, чтобы аварийный перезапуск подсистемы не приводил к нарушению ее работы и не создавал неудобств в работе пользователей.

6.6.3 Должна быть регламентирована система резервирования данных БД. Резервирование данных должно происходить автоматически строго по установленным временным интервалам. Требуется определить степень важности и условия резервирования БД по следующим критериям: разделение БД на сегменты, степень важности каждых сегментов, приоритетность восстанавливаемых данных в случае сбоя ПО или отказа оборудования.

6.6.4 База данных должна иметь возможность возвратиться к предшествующему непротиворечивому состоянию. Это требование может возникнуть из-за ошибочных транзакций, системного сбоя или потери хранимых данных. Чтобы удовлетворить эти требования, могут использоваться различ-

ные механизмы, такие как запись всех изменений, сделанных в базе данных, и сохранение резервных копий всей базы данных или ее части.

Модифицированные данные, которые распределяются в более чем одной базе данных, должны быть восстановлены таким образом, чтобы конечный результат имел непротиворечивое состояние, и состояние базы данных было бы непротиворечивым.

6.6.5 Необходимо обеспечить возможность сохранять записи об успешных изменениях в данных в базе данных и в случае необходимости — записи о транзакциях, которые запрашивают данные и генерируют отчеты. Эти записи должны включать соответствующие значения данных, подробности транзакции и идентификацию пользователя. Эти контрольные журналы должны быть определены, как требуемые для всех данных в базе данных, избранных типов данных или экземпляров определяемых данных.

7 Требования к реализации БД

7.1 Программные интерфейсы

7.1.1 Для организации взаимодействия между программными системами, составляющими ПО ИР, должны использоваться программные библиотеки, протоколы и форматы данных, описываемые открытыми (общедоступными) стандартами. Такие стандарты должны быть выпущены международной организацией и иметь широкую поддержку.

7.1.2 Рекомендованные сетевые протоколы межпрограммного взаимодействия приведены в разделе «Архитектура модулей». Для хранения и передачи мультимедийной информации должны использоваться форматы данных, перечисленные в разделе «Форматы данных».

7.2 Организация данных

7.2.1 Данные в базах данных должны быть распределены таким образом, чтобы исключить хранение избыточной информации. Соответствующее хранилище должно относиться к наиболее общему приложению БД (например, хранилище персональной информации должно относиться к программе информационного каталога людей и организаций). Допускается использовать кэширование (промежуточный буфер с быстрым доступом) данных приложением, однако у кэшируемых данных должно быть определенное время жизни и должен существовать механизм проверки актуальности кэшируемых данных. Работы по изменению приложений БД должны проводиться с учетом возможности доступа других приложений к данным, хранящимся в БД (напрямую к СУБД или посредством прикладной программы).

7.2.2 Схемы внешних баз данных (потенциально используемых более чем одним приложением) и структуры данных, используемые для обмена

между приложениями, должны быть документированы*. Эта документация должна включать:

– описание схем БД и структур данных;

– регламент модификации схем БД и структур данных с указанием минимального периода времени между модификациями (для сохраняющих совместимость снизу вверх рекомендуется период 6 месяцев, для не сохраняющих - 1 год);

– рекомендации по процедурам доступа к данным и их обработки (для поддержания совместимости при модификации схем и структур);

– регламент резервирования данных;

– регламент архивирования данных.

7.2.3 Должны использоваться форматы данных (такие как XML), позволяющие строить расширяемые структуры. Не допускается использовать методы обработки данных, использующие неточные данные о структуре данных (размере блока данных, наборе полей и др.).

7.2.4 Рекомендации по обработке данных:

– необходимо вести протокол операций с БД. Объем этого протокола должен быть достаточен для того, чтобы восстановить состояние БД на определенный момент в прошлом. Для любой операции должен быть указан инициировавший ее пользователь;

– целесообразно не использовать операцию фактического удаления или изменения данных, необходимо реализовать логическое обновление или удаление, заключающееся в соответствующей отметке удаляемой или обновляемой записи данных и исключении ее из дальнейшей обработки;

– должны использоваться средства (утилиты) очистки БД от неиспользуемых (логически удаленных определенное время назад) данных.

7.2.5 Независимость данных - это независимость процессов от объектов данных, которая состоит в том, что объекты данных могут быть изменены без нарушения процессов.

Независимость данных, достигается тремя способами.

Первый способ состоит в связывании процесса со схемой таким образом, что процесс знает только ту часть схемы, а именно прикладную схему, которая необходима процессу управления данными.

Второй способ - это обеспечение независимости прикладных процессов от физического представления данных.

Третий способ - это включение ограничений целостности в схему, а не в прикладные процессы.

7.3 Программный код

7.3.1 Программные системы, составляющие ПО, должны представлять собой набор взаимосвязанных модулей с документированными программны-

---

* Виды документов на программные средства, используемые при создании автоматизированных систем (ее частей) приведены в ГОСТ 19.101. Наименования конкретных документов, разрабатываемых при проектировании автоматизированной системы, приведены в O‘z DSt 1985.

(Измененная редакция, Изм. № 1)

ми интерфейсами (API). Каждый модуль должен выполнять минимальный независимый набор функций. Функции модуля должны быть документированы, использование недокументированных функций запрещается.

7.3.2 При разработке ПО должен использоваться доступный инструментарий с правом получения исходных кодов и их дальнейшей модификации. Предпочтение должно отдаваться средствам разработки, которые доступны на различных программных и аппаратных платформах. Исходный код программ должен быть доступен для разработчиков, и определяться лицензией на программное обеспечение с открытым исходным кодом (например, GNU, GPL). Программный исходный код должен быть документирован в мере, достаточной для понимания логики его работы.

7.4 Управление доступом к БД

7.4.1 Субъектом доступа к БД является пользователь, который должен проходить аутентификацию и авторизацию.

7.4.2 Условием организации доступа к ПО БД является корректная аутентификация и последующая авторизация пользователя в системе. При этом идентификационные данные пользователя (логическое имя, пароль) должны быть уникальными. Недопустимо существование двух одинаковых имен пользователя в системе.

7.4.3 Права доступа должны указываться как для пользователей, так и для логических групп пользователей. Объектом доступа является любой элемент пользовательского интерфейса (экранная форма или ее отдельный элемент). Для указания объекта доступа должны использоваться иерархические идентификаторы (построенные по принципу Приложение:Форма:Элемент). Набор прав доступа: поиск, чтение, запись, модификация, удаление, изменение.

7.4.4 Управление доступом - это предотвращение несанкционированного использования ресурса, включая предотвращение использования ресурса несанкционированным образом.

7.4.5 Для управления данными задание управления доступом состоит в разрешении санкционированного доступа к данным и предотвращении несанкционированного доступа. Такое управление доступом определяет процессы, которые может выполнять пользователь.

7.4.6 В любой организационной ситуации существуют требования к управлению доступом, которые могут быть выражены в терминах стратегии безопасности. Стратегия безопасности устанавливает, какую форму доступа требует каждый пользователь информационной системы. Информационная система должна иметь соответствующие механизмы управления доступом для проведения в жизнь стратегии безопасности.

7.4.7 Управление доступом должно основываться на принципе идентичности человека и процесса.

7.4.8 Требования управления доступом в контексте управления данными должны быть следующими:

- определять и впоследствии модифицировать привилегии управления доступом;
- проводить в жизнь в любое время ограничения управления доступом, которые применимы в том же месте в то же время.

7.4.9 Для определения привилегий требуются определенные средства. Процесс выделения привилегий пользователям называется санкционированием. Глобальные полномочия даются тому, кто должен создать или модифицировать другие привилегии управления доступом в среде управления данными.

7.4.10 Привилегии должны определяться в терминах идентификатора пользователя, ограничениями на использование информационной системы, баз данных, схем, типов данных, времени и размещения, а также используя их комбинации.

7.4.11 При необходимости может потребоваться дополнительная информация, такая, например, как идентификатор пользователя, который санкционирует привилегию.

7.4.12 Данные, описывающие привилегии, называют данными по управлению доступом. Эти данные должны храниться и управляться точно так же, как и любые другие данные в области управления данными.

7.4.13 Решение о предоставлении конкретного доступа к данным основывается на привилегиях пользователя.

7.4.14 Проведение в жизнь управления доступом требует, чтобы пользователи и процессы, выполняющие роль пользователей, были идентифицированы и чтобы законность запроса на использование этого процесса доступа к требуемым данным могла быть проконтролирована в момент выполнения.

8 Архитектура модулей

8.1 Приложение

8.1.1 В рамках предложенной архитектуры ПО приложение - это программа обработки данных, ориентированная на обработку не связанных между собой транзакций. В рамках приложения должна реализовываться специфичная логика обработки данных, тогда как взаимосвязь между операциями с данными реализуется средствами системы пользовательского интерфейса. Приложения могут быть прикладными (обслуживающими запросы пользователей) и служебными (обслуживающими запросы других программ).

8.1.2 Приложение может взаимодействовать с системой хранения данных, с системой пользовательского интерфейса и с другими приложениями. Для обращения к системе хранения данных должны использоваться соответствующие протоколы и API (раздел «Система хранения данных»). Для взаимодействия с другими приложениями и с системой пользовательского интерфейса целесообразно использовать представление данных в формате XML, а в качестве сетевого протокола - HTTP. Если необходима криптографическая защита информации - HTTPS. При взаимодействии с другими приложениями приложение может являться либо клиентом (запрашивающим),

либо сервером (отвечающим). При взаимодействии с системой пользовательского интерфейса приложение является сервером.

8.1.3 Приложение должно содержать подсистему проверки корректности запроса на обработку данных и подсистему исполнения запроса. Программный интерфейс между этими подсистемами должен быть документирован. Это необходимо для добавления функции репликации на уровне приложения и построения программной системы, распределенной по корпоративной сети.

8.2 Система пользовательского интерфейса

8.2.1 Система пользовательского интерфейса ПО предназначена для организации доступа пользователей к средствам приложений. Ее задачи:

- предоставление средств взаимодействия с пользователем;
- аутентификация и контроль доступа пользователей;
- протоколирование действий пользователя;
- управление сеансами работы пользователя (сессиями);
- организация логической связи операций по обработке данных, предоставляемых приложениями.

8.2.2 Процесс управления данными может быть вызван пользователем, процессами управления данными или другими процессами. Процессы выполняются процессорами, каждый из которых имеет интерфейс. Интерфейс процессора должен быть точно определен. Такие интерфейсы могут быть независимыми от стандартного языка программирования, используемого для определения процесса с использованием интерфейса.

В любом интерфейсе существуют факторы, о которых пользователь должен знать, чтобы иметь возможность использовать основной процессор. Эти факторы должны быть сведены к минимуму, чтобы обеспечить как можно большую независимость в интерфейсе.

8.2.3 ПО пользователя использует протокол HTTP/HTTPS для доступа к системе пользовательского интерфейса. Для передачи данных, необходимых для аутентификации пользователя, требуется использовать штатные средства протокола HTTP.

8.2.4 Подсистема управления сессиями должна отслеживать сеансы работы пользователей. Она должна содержать абстрактное XML - описание форм пользовательского интерфейса, их связи и идентификаторы, необходимые для управления доступом.

8.2.5 Для визуального оформления форм пользовательского интерфейса нужно использовать подсистему Web-интерфейса. Эта подсистема содержит необходимые текстовые и графические файлы, а также преобразует абстрактное XML - описание интерфейсной формы в отображаемое HTML представление.

8.2.6 При необходимости следует иметь возможность отображать данные в формате, предпочитаемом системой управления данными, и формате, предпочитаемом пользователем. Это требование связано с тем, что пользова-

тель может предпочесть манипулировать данными в соответствии со средством моделирования данных, отличным от средства, обеспеченного системой управления данными.

8.3 Система хранения данных

8.3.1 Для хранения данных должна использоваться СУБД, использующая язык запросов SQL. ПО СУБД должно поддерживать многопоточную обработку запросов и сетевой доступ, а также включать средства управления и архивирования данных.

8.3.2 Для доступа к СУБД приложения должны использовать сетевой протокол соответствующей СУБД. В качестве программного интерфейса (API) должны использоваться программные библиотеки для соответствующих языков программирования.

8.3.3 Недопустим непосредственный доступ ПО пользователей к СУБД. СУБД должна обслуживать только запросы приложений. Для получения доступа к данным приложения должны быть аутентифицированы средствами СУБД.

9 Лицензирование

Права на использование программного кода, исходного программного кода и данных, необходимых для генерации и работы кодов должны принадлежать разработчикам программного кода. Организации, использующие ПО БД и систем обмена информацией должны иметь право на выполнение ПО, исследования работы ПО, модификацию ПО и создание на его основе дополнительных программных систем. Права на все результаты работы ПО должны принадлежать владельцам полностью. Обязательным условием является патентная чистота ПО и используемых технологий в Республике Узбекистан.

10 Ответственность лиц, участвующих в разработке, эксплуатации и техническом сопровождении программного обеспечения

10.1 В разработке ПО БД участвуют разработчики программного обеспечения БД, разработчики инфраструктурного ПО и технические администраторы, область ответственности которых различна.

10.2 Разработчики программного обеспечения БД:

- схемы БД, специфичных для данного приложения;
- описание пользовательского интерфейса; визуальное оформление интерфейса на основе готовых стандартных элементов;
- программные модули обработки данных.

10.3 Разработчики инфраструктуры:

- ПО системы пользовательского интерфейса;
- система протоколирования действий пользователей;
- служебные приложения: справочник пользователей, система аутентификации.

10.4 Технические администраторы:

- СУБД, библиотеки API;
- системный каталог пользователей;
- программная платформа для выполнения программ;
- общие схемы БД и форматы структур данных, используемых для взаимодействия между программами; распределение сетевых ресурсов.

10.5 При отсутствии в органах государственного управления и государственной власти на местах отделов по разработке программного обеспечения следует использовать программное обеспечение сторонних разработчиков, отвечающее техническому заданию предъявленному заказчиком.

10.6 При отсутствии технических администраторов, или лиц, исполняющих их обязанности, рекомендуется создать отдел по обеспечению и системному сопровождению информационной системы с наличием квалифицированных специалистов.

Библиография

[1] **(Исключен, Изм. № 1)**

[2] RH 45-170:2004 Основные технические требования по созданию локальных и корпоративных ведомственных компьютерных сетей

[3] **(Исключен, Изм. № 1)**

УДК 65.015 ОКС 35.040

Ключевые слова: алгоритм; база данных; данные; интерфейс; корпоративная сеть; программное обеспечение; пользователь, целостность данных