СОГЛАСОВАНО
Начальник управления
ФСТЭК России

В.Селин
« »_____ 2006 года

УТВЕРЖДАЮ
Генеральный директор
ООО «Майкрософт Рус»

Б.Стеен
« »_____ 2006 года

Система управления базами данных Microsoft® SQL Server™ 2005 Standard Edition

Задание по безопасности

MS.SQL_Srv2005_Std.3Б

Версия 1.0

2006

СОДЕРЖАНИЕ

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

БД	– база данных
ЗБ	– задание по безопасности
ИС	– информационная система
ИТ	– информационная технология
НСД	– несанкционированный доступ
ОДФ	– область действия функции безопасности объекта оценки
ОК	– Общие критерии
ОО	– объект оценки
ОС	– операционная система
ОУД	– оценочный уровень доверия
ПБО	– политика безопасности объекта оценки
ПЗ	– профиль защиты
СУБД	– система управления базами данных
СФБ	– стойкость функции безопасности
УК	– управление конфигурацией
ФБО	– функции безопасности объекта оценки
ФТБ	– функциональные требования безопасности
DBCC	– Database Console Command
DDL	– Data Definition Language
DTS	– Data Transformation Services
GUID	– Globally Unique Identifiers
MMC	– Microsoft Management Console
OLTP	– Online Transaction Processing Systems
PSS	– Process Status Structure
RID	– Relative Identifiers
SID	– Security Identifier
UID	– User Identifier

1 Введение ЗБ

Данный раздел содержит информацию общего характера. Подраздел «Идентификация ЗБ» предоставляет маркировку и описательную информацию, которые необходимы, чтобы контролировать и идентифицировать ЗБ и ОО, к которому оно относится. Подраздел «Аннотация ЗБ» содержит общую характеристику ЗБ, позволяющую определить применимость ОО, к которому относится настоящее ЗБ, в конкретной ситуации. В подразделе «Соглашения» дается описание операций конкретизации компонентов требований безопасности ИТ. В подразделе «Термины и определения» представлены определения основных терминов, специфичных для данного ЗБ. В подразделе «Организация ЗБ» дается пояснение организации документа.

1.1 Идентификация ЗБ

Название ЗБ:	Система управления базами данных Microsoft® SQL Server™ 2005 Standard Edition. Задание по безопасности.
Версия ЗБ:	Версия 1.0.
Обозначение ЗБ:	MS.SQL_Srv2005_Std.ЗБ.
Идентификация ОО:	Система управления базами данных Microsoft® SQL Server™ 2005 Standard Edition.
Уровень доверия:	ОУД1, усиленный компонентом AVA_SOF.1 (Оценка стойкости функции безопасности).
Идентификация ОК:	ГОСТ Р ИСО/МЭК 15408–2002 Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Части 1, 2, 3. Руководящий документ. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий. Часть 1: Введение и общая модель, Гостехкомиссия России, 2002. Руководящий документ. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий. Часть 2: Функциональные требования безопасности, Гостехкомиссия России, 2002.

Руководящий документ. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий. Часть 3: Требования доверия к безопасности, Гостехкомиссия России, 2002.

Ключевые слова: Система управления базами данных, средство защиты информации, дискреционное управление доступом, задание по безопасности, ОУД1, Microsoft®.

1.2 Аннотация ЗБ

Настоящее ЗБ определяет требования безопасности для системы управления базами данных Microsoft® SQL Server™ 2005 Standard Edition (далее – объект оценки).

Объект оценки представляет собой полнофункциональную реляционную систему управления базами данных масштаба предприятия, обеспечивающую надежную инфраструктурную платформу высокой производительности для создания, развертывания и поддержки больших производственных БД. Реляционное ядро ОО обеспечивает достоверность и защиту хранимых в реляционных таблицах данных, отказоустойчивость и динамическую оптимизацию производительности системы.

1.3 Соответствие ОК

Объект оценки и ЗБ согласованы со следующими спецификациями:

- «Безопасность информационных технологий. Системы управления базами данных. Системы управления базами данных масштаба предприятия. Профиль защиты. Версия 1.0, 2005» СУБД.СУБД_МП.ПЗ (**соответствие ПЗ** – ОО соответствует всем частям данного ПЗ);
- Руководящий документ. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий. Часть 2: Функциональные требования безопасности, Гостехкомиссия России, 2002 (**соответствие части 2 ОК** – ОО соответствует функциональным требованиям, основанным только на функциональных компонентах из части 2 ОК);
- Руководящий документ. Безопасность информационных технологий. Критерии оценки безопасности информационных технологий. Часть 3: Требования доверия к безопасности, Гостехкомиссия России, 2002 (**усиление части 3 ОК** –

требования доверия представлены в виде ОУД1 и, кроме того, включают компонент AVA_SOF.1 из части 3 ОК).

1.4 Соглашения

Руководящий документ Гостехкомиссии России «Безопасность информационных технологий. Критерии оценки безопасности информационных технологий» (далее – Общие критерии) допускает выполнение определенных в части 2 ОК операций над функциональными требованиями. Соответственно в настоящем ЗБ используются операции «уточнение», «выбор», «назначение» и «итерация».

Операция **«уточнение»** используется для добавления к требованию некоторых подробностей (деталей) и, таким образом, ограничивает диапазон возможностей его удовлетворения.

Операция **«выбор»** используется для выбора одного или нескольких элементов из перечня в формулировке требования. Результат операции **«выбор»** в настоящем ЗБ обозначается *подчеркнутым курсивным текстом*.

Операция **«назначение»** используется для присвоения конкретного значения ранее неконкретизированному параметру. Операция **«назначение»** обозначается заключением значения параметра в квадратные скобки, [назначаемое значение].

Операция **«итерация»** используется для более чем однократного использования компонента функциональных требований безопасности ИТ при различном выполнении разрешенных операций («уточнение», «выбор», «назначение»). Выполнение операции «итерация» сопровождается помещением номера итерации, заключенного в круглые скобки, после краткого имени соответствующего компонента, (номер итерации).

1.5 Термины и определения

В настоящем ЗБ применяются следующие термины с соответствующими определениями.

Активы – информация или ресурсы ОО, подлежащие защите контрмерами ОО.

Аутентификационные данные – информация, используемая для верификации предъявленного идентификатора.

Аутентификация – процесс установления подлинности информации, предъявленной администратором ОО и пользователем ОО при регистрации.

Достоверность – свойство безопасности активов, обеспечивающее соответствие предусмотренным значениям.

Зависимость – соотношение между требованиями, при котором требование, от которого зависят другие требования, должно быть удовлетворено, чтобы и другие требования могли отвечать своим целям.

Задание по безопасности – совокупность требований безопасности и спецификаций, предназначенная для использования в качестве основы для оценки конкретного ОО (в данном случае – СУБД Microsoft® SQL Server™ 2005 Standard Edition).

Идентификатор – уникальный признак администратора ОО или пользователя ОО, однозначно его идентифицирующий.

Конфиденциальность – свойство безопасности активов предотвращать возможность доступа к информации и/или ее раскрытия неуполномоченным лицам, объектам или процессам.

Объект ОО – сущность в пределах ОДФ, которая содержит или получает информацию, и над которой субъекты выполняют операции (база данных (Database), таблица (Table), столбец таблицы (Column), определяемая пользователем функция (User Defined Function), представление (Views), хранимая процедура (Stored Procedures)).

Объект оценки – подлежащая оценке СУБД Microsoft® SQL Server™ 2005 Standard Edition с руководствами по эксплуатации.

Подконтрольность – свойство безопасности активов, обеспечивающее однозначное отслеживание действий объектов и субъектов информационных отношений.

Политика безопасности ОО – совокупность правил, регулирующих управление, защиту и распределение активов, контролируемых ОО.

Политика функции безопасности – политика безопасности, осуществляемая ФБ.

Пользователь – любая сущность (человек-пользователь или внешний объект ИТ) вне ОО, которая взаимодействует с ОО.

Администратор ОО – уполномоченный пользователь, ответственный за установку, администрирование и эксплуатацию ОО.

Продукт ИТ – совокупность программных, программно-аппаратных и/или аппаратных средств ИТ, предоставляющая определенные функциональные возможности и предназначенная для непосредственного использования или включения в различные системы (в данном случае продукт ИТ совпадает с ОО, идентифицированным в настоящем ЗБ).

Профиль защиты – независимая от реализации совокупность требований безопасности для некоторой категории ОО, отвечающая специфическим запросам потребителя.

Ресурс ОО – все, что может использоваться или потребляться в ОО (вычислительные возможности, физическая память, дисковое пространство).

Система ИТ – специфическое воплощение ИТ с конкретным назначением и условиями эксплуатации.

Субъект ОО – сущность в пределах ОДФ, которая инициирует выполнение операций (процессы, действующие от имени пользователей ОО).

Функции безопасности ОО – совокупность всех функций безопасности ОО, направленных на осуществление ПБО.

Функция безопасности – функциональные возможности части или частей ОО, обеспечивающие выполнение подмножества взаимосвязанных правил ПБО.

Целостность – свойство безопасности активов, обеспечивающее поддержание полноты и неизменности информации.

1.6 Организация ЗБ

Раздел 1 «Введение ЗБ» содержит информацию управления документооборотом и описательную информацию, необходимые для идентификации ЗБ и ОО, к которому оно относится.

Раздел 2 «Описание ОО» содержит описание функциональных возможностей ОО, среды функционирования ОО и границ ОО, служащее цели лучшего понимания требований безопасности и дающее представление о типе продукта.

Раздел 3 «Среда безопасности ОО» содержит описание аспектов среды безопасности ОО. В данном разделе определяется совокупность угроз, имеющих отношение к безопасному функционированию ОО, политика безопасности организации, которой должен следовать ОО, и предположения (обязательные условия) безопасного использования ОО.

В разделе 4 «Цели безопасности» определена совокупность целей безопасности для ОО и среды функционирования ОО.

В разделе 5 «Требования безопасности ИТ» на основе частей 2 и 3 ОК определены, соответственно, функциональные требования безопасности ИТ и требования доверия к безопасности ОО.

В раздел 6 «Краткая спецификация ОО» включено описание реализуемых ОО функций безопасности ИТ, соответствующих специфицированным в ЗБ функциональным требованиям безопасности, а также мер доверия к безопасности, соответствующих специфицированным в ЗБ требованиям доверия к безопасности ОО.

В разделе 7 «Утверждения о соответствии ПЗ» идентифицируется ПЗ, о соответствии которому заявляется в ЗБ, а также дополнения и уточнения аспектов среды безопасности, целей и требований безопасности.

В Разделе 8 «Обоснование» демонстрируется, что ЗБ специфицирует полную и взаимосвязанную совокупность требований безопасности ИТ, что ОО учитывает идентифицированные аспекты среды безопасности ИТ, а также что функции безопасности ИТ и меры доверия к безопасности соответствуют требованиям безопасности ОО.

2 Описание ОО

Объектом оценки является система управления базами данных Microsoft® SQL Server™ 2005 Standard Edition (далее – СУБД Microsoft® SQL Server™ 2005 Standard Edition).

2.1 Тип продукта ИТ

Система управления базами данных Microsoft® SQL Server™ 2005 Standard Edition представляет собой полнофункциональную реляционную систему управления базами данных масштаба предприятия, обеспечивающую надежную инфраструктурную платформу высокой производительности для создания, развертывания и поддержки больших производственных БД. Реляционное ядро СУБД Microsoft® SQL Server™ 2005 Standard Edition обеспечивает достоверность и защиту хранимых в реляционных таблицах данных, отказоустойчивость и динамическую оптимизацию производительности системы.

Ключевыми компонентами СУБД Microsoft® SQL Server™ 2005 Standard Edition являются следующие:

- SQL Server Database Services (Службы баз данных SQL Server);
- Analysis Services (Аналитические службы);
- Integration Services (Службы интеграции);
- Notification Services (Службы уведомлений);
- Reporting Services (Службы отчетов);
- Service Broker (Брокер службы).

Службы баз данных SQL Server включают ядро базы данных (Database Engine), а также средства репликации и полнотекстового поиска. Ядро Database Engine — основная служба для хранения, обработки и защиты данных, обеспечивающая управляемый доступ и быструю обработку транзакций. Database Engine используется для создания реляционных баз данных для оперативной обработки транзакций или интерактивной аналитической обработки. Средства репликация позволяют увеличить доступность данных посредством их тиражирования между множеством БД, что позволяет разделять нагрузку по чтению данным между несколькими выделенными серверами БД, а функции полнотекстового поиска предоставляют возможность выполнения запросов к данным, хранящимся в таблицах БД, на естественном языка.

Службы Analysis Services являются основными службами по обеспечению быстрого анализа бизнес-данных, интерактивной аналитической обработки (OLAP) и функций интеллектуального анализа данных для использования в приложениях бизнес-аналитики. Аналитические службы позволяют объединять данные из множества источников, например, реляционных БД, и использовать их для решения различных практических задач.

Аналитические службы сочетают в себе различные аспекты традиционного анализа на основе OLAP и реляционной отчетности, позволяя разработчикам определять одну модель данных, именуемую унифицированной многомерной моделью (UDM), для одного или нескольких физических источников данных. Все запросы конечного пользователя из OLAP, из отчетов и из пользовательских приложений бизнес-анализа получают доступ к данным в базовых источниках данных посредством унифицированной многомерной модели, обеспечивающей единое бизнес-представление таких реляционных данных.

Службы Analysis Services предоставляют большой набор алгоритмов интеллектуального анализа данных, которые позволяют пользователям выполнять интеллектуальный анализ данных с целью выявления определенных закономерностей и тенденций. Такие алгоритмы интеллектуального анализа данных могут использоваться для анализа данных посредством унифицированной многомерной модели или непосредственно из физического хранилища данных.

Службы Integration Services — это платформа для построения решений по интеграции и преобразованию данных уровня предприятия. Службы Integration Services используются для решения сложных бизнес-задач при помощи копирования и загрузки файлов, отправки электронных сообщений в ответ на события, обновления хранилищ данных, очистки и интеллектуального анализа данных, а также управления объектами и данными SQL Server. Службы интеграции Integration Services реализуют функции преобразования и интеграции данных, позволяющие извлекать их из множества источников, преобразовывать, а затем предоставлять получателям данных. Данный функционал предоставляет возможность объединения данных из множества неоднородных источников, их преобразования и загрузки в хранилища. Инструменты служб Integration Services обеспечивают проектирование, создание и управление пакетами, ориентированными на решение повседневных бизнес-задач.

Службы уведомлений Notification Services предназначены для автоматического создания и своевременной отправки пользователям персонализированных сообщений при

возникновении какого-либо события. Службы Notification Services представляют собой платформу для разработки и развертывания приложений, создающих уведомления и отправляющих их подписчикам, а также платформу для размещения этих приложений. Создаваемые уведомления представляют собой индивидуальные сообщения, которые могут своевременно отправляться на множество устройств и которые отражают предпочтения подписчика.

Службы отчетов Reporting Services представляют собой платформу отчетов на основе сервера, которая обеспечивает комплексное ведение отчетов для данных из реляционных и многомерных источников данных. При помощи служб Reporting Services можно создавать интерактивные, табличные и другие отчеты, получение данных в которых происходит через запланированные интервалы времени или по требованию при открытии отчета. Службы Reporting Services также позволяют пользователям создавать нерегламентированные отчеты, основанные на предопределенных моделях, а также исследовать данные модели отчета в интерактивном режиме. Все отчеты могут подготавливаться как в формате обычного документа, так и в виде веб-страницы.

Брокер службы Service Broker обеспечивает надежную, тесно интегрированную с базой данных инфраструктуру для организации очередей сообщений и асинхронного обмена сообщениями. В дальнейшем очереди сообщений могут быть использованы для накопления заданий, таких как запросы и другие обращения к данным, и их выполнение по мере освобождения ресурсов. В свою очередь асинхронный обмен сообщениями позволяет приложениям БД связываться между собой. Service Broker позволяет снизить время, необходимое для разработки приложений, предоставляя большую часть инфраструктуры, требующейся для создания распределенных приложений.

Поддержка СУБД Microsoft® SQL Server™ 2005 Standard Edition службы каталогов Microsoft® Active Directory™ позволяет публиковать с ее помощью информацию о расположении СУБД Microsoft® SQL Server™ 2005 Standard Edition в вычислительной сети, именах, размерах и расположении баз данных, а также датах их последнего резервного копирования. Кроме того, СУБД Microsoft® SQL Server™ 2005 Standard Edition, установленная на компьютере с серверной ОС Microsoft® Windows Server™ 2003, функционирующем в домене на базе Microsoft® Active Directory™, поддерживает механизм делегирования учетной записи (возможность получать доступ к ресурсам на различных серверах БД, сохраняя при переключении между ними пароль и имя прошедшего аутентификацию пользователя) и может использовать режим проверки

подлинности средствами Windows (Windows Authentication Mode), т.е. позволять ОС управлять доступом к СУБД Microsoft® SQL Server™ 2005 Standard Edition. Благодаря этому, пользователь, имеющий действительную учетную запись и успешно зарегистрировавшийся в ОС, может подключиться к СУБД Microsoft® SQL Server™ 2005 Standard Edition, не проходя дополнительных процедур проверки и регистрации в самой СУБД Microsoft® SQL Server™ 2005 Standard Edition.

Благодаря встроенной поддержке сетевых библиотек (Net-Libraries), поддерживающих основные сетевые протоколы, СУБД Microsoft® SQL Server™ 2005 Standard Edition позволяет обеспечить обмен данными между клиентскими приложениями и самой СУБД Microsoft® SQL Server™ 2005 Standard Edition.

Глубокая интеграция СУБД Microsoft® SQL Server™ 2005 Standard Edition с ОС, под управлением которой она функционирует, обеспечивает для СУБД Microsoft® SQL Server™ 2005 Standard Edition такие функциональные возможности, как управление службами СУБД Microsoft® SQL Server™ 2005 Standard Edition с использованием консоли управления Microsoft (MMC – Microsoft Management Console), просмотр относящихся к функционированию СУБД событий с использованием утилиты «Event Viewer» и др.

2.2 Основные функциональные возможности системы управления базами данных Microsoft® SQL Server™ 2005 Standard Edition

В СУБД Microsoft® SQL Server™ 2005 Standard Edition реализован ряд функциональных возможностей и средств, позволяющих обеспечить безопасность ИТ, надежность СУБД, а также упрощающих администрирование ОО и управление вычислительной средой ОО. В данном подразделе представлено краткое описание этих функциональных возможностей и средств.

2.2.1 Основные функциональные возможности обеспечения безопасности

Система управления базами данных Microsoft® SQL Server™ 2005 Standard Edition характеризуется как управляемая, надежная и безопасная система, что достигается за счет таких возможностей обеспечения безопасности, как использование единых регистрационных данных пользователя при доступе к ОС и к СУБД Microsoft® SQL Server™ 2005 Standard Edition, аудит событий безопасности, управление ролями, дискреционное управление доступом.

2.2.1.1 Аудит событий безопасности

Система управления базами данных Microsoft® SQL Server™ 2005 Standard Edition обеспечивает широкие возможности, связанные с мониторингом и обнаружением нежелательных условий, которые могут возникнуть, а также событий, которые могут произойти в вычислительной среде. Мониторинг относящихся к безопасности событий позволяет обнаруживать нарушителей безопасности, а также выявлять попытки несанкционированного доступа к СУБД Microsoft® SQL Server™ 2005 Standard Edition или использования разрешений на выполнение инструкций языка DDL (Transact-SQL) или доступа к защищаемым активам. В частности, определяя политику аудита, уполномоченный администратор ОО может осуществлять аудит только необходимых классов событий безопасности, таких как создание и удаление пользователей БД или неудачные попытки подключения пользователей к СУБД Microsoft® SQL Server™ 2005 Standard Edition. Запись результатов аудита событий безопасности осуществляется в журналы регистрации событий аудита, доступ к которому разрешен только уполномоченному администратору ОО. Просмотр журналов регистрации событий аудита выполняется с использованием специализированного инструментального средства SQL Profiler. Кроме того, в СУБД Microsoft® SQL Server™ 2005 Standard Edition предусмотрены средства, обеспечивающие возможность мониторинга и регистрации только тех событий аудита, которые удовлетворяют заданным критериям, что позволяет ограничить объем данных, собираемых о событиях безопасности. Для задания критериев аудита событий безопасности в СУБД Microsoft® SQL Server™ 2005 Standard Edition используются числовые и строковые фильтры.

2.2.1.2 Дискреционное управление доступом

В СУБД Microsoft® SQL Server™ 2005 Standard Edition доступ к защищаемым активам разрешен только уполномоченным на это пользователям ОО. Модель защиты СУБД Microsoft® SQL Server™ 2005 Standard Edition включает компоненты, которые реализуют контроль субъектов доступа и действий, предпринимаемых конкретной сущностью по отношению к объекту доступа.

Каждый пользователь, осуществляющий взаимодействие с СУБД Microsoft® SQL Server™ 2005 Standard Edition, представлен в ней регистрационной записью, определяющей сущностей, имеющих право доступа к СУБД Microsoft® SQL Server™ 2005 Standard Edition, и учетной записью пользователя БД, сопоставленной с регистрационной

записью и используемой СУБД Microsoft® SQL Server™ 2005 Standard Edition при управлении доступом как к самой БД (базам данных), так и ее объектам, таким как таблицы, представления, хранимые процедуры и др. Для каждой БД система управления базами данных Microsoft® SQL Server™ 2005 Standard Edition поддерживает собственную таблицу (список дискреционного управления доступом), в которой определены права доступа к объектам данной БД. Список дискреционного управления доступом включает перечень пользователей и ролей, которым разрешен доступ к объекту, а также набор допустимых над объектом действий.

СУБД Microsoft® SQL Server™ 2005 Standard Edition обеспечивает возможность контекстного переключения, повышая гибкость и безопасность управления разрешениями на цепочки владения между пользовательскими модулями и объектами, на которые они ссылаются. Используя механизм контекстного переключения, СУБД Microsoft® SQL Server™ 2005 Standard Edition позволят указывать, учетные данные каких пользователей следует использовать при проверке разрешений на объекты, на которые ссылается вызываемый модуль.

2.2.1.3 Управление учетными данными пользователей ОО, имеющих доступ к БД

Функция управления учетными данными обеспечивает безопасное хранение учетных данных пользователя БД. СУБД Microsoft® SQL Server™ 2005 Standard Edition поддерживает таблицу, в которой полностью определены учетные записи пользователей, имеющих доступ к БД (содержимое данной таблицы представляет БД учетных записей пользователей БД). При этом таблица учетных записей пользователей поддерживается отдельно для каждой существующей БД, для которой определены права доступа. Если пользователю необходимо получить доступ к какой-либо БД, то при осуществлении попыток доступа к ней потребуется пройти процедуру проверки подлинности, в ходе которой пользователь предъявляет свой идентификатор безопасности, на основании которого определяется возможность доступа пользователя к данной БД.

2.2.1.4 Управление ролями

Использование ролей позволяет упростить управление доступом к защищаемым активам, позволяя назначать разрешения и права группе пользователей, а не отдельной учетной записи. Таким образом, исходя из потребностей в доступе к новым активам,

пользователь ОО может быть включен в состав участников определенной роли или исключен из участия в указанной роли.

Система управления базами данных Microsoft® SQL Server™ 2005 Standard Edition поддерживает ряд предопределенных ролей сервера БД (server role), создаваемых в момент установки СУБД Microsoft® SQL Server™ 2005 Standard Edition. Членство в данных ролях предоставляет право выполнять ряд административных и системных задач, такие как управление файлами и устройствами резервного копирования, установка и изменение параметров конфигурации удаленных и связанных серверов БД и т.д. Помимо предопределенных ролей сервера в СУБД Microsoft® SQL Server™ 2005 Standard Edition создаются фиксированные роли БД (fixed database role), у которых имеются предопределенные полномочия для работы с конкретными БД. Каждая БД в СУБД Microsoft® SQL Server™ 2005 Standard Edition содержит девять фиксированных ролей БД с разрешениями, определяемыми на уровне БД. Имеется возможность создания и дальнейшего использования роли БД, определяемой пользователем (user-defined database role), которая позволяет определять специфичные для конкретной группы пользователей ОО права доступа при работе с БД.

2.2.1.5 Принудительное применение учетной записи гостя

Система управления базами данных Microsoft® SQL Server™ 2005 Standard Edition обеспечивает поддержку модели общего доступа с использованием учетной записи «Гость» (Guest). Использование данной модели позволяет в любой создаваемой БД определять особое имя пользователя – «Гость», предоставляющее любому подключившемуся к СУБД Microsoft® SQL Server™ 2005 Standard Edition пользователю доступ к данной БД с минимальным набором полномочий. Если прошедший проверку подлинности пользователь (независимо от режима проверки подлинности) имеет доступ к СУБД Microsoft® SQL Server™ 2005 Standard Edition, но не имеет доступа к какой-либо базе данных, СУБД Microsoft® SQL Server™ 2005 Standard Edition автоматически предоставит доступ к этой БД с полномочиями пользователя «Гость».

2.2.2 Основные функциональные возможности повышения надежности

Система управления базами данных Microsoft® SQL Server™ 2005 Standard Edition обеспечивает надежную защиту данных от непредвиденных сбоев или отказов системы, обеспечивая следующие возможности по повышению надежности.

2.2.2.1 Резервное копирование данных

В СУБД Microsoft® SQL Server™ 2005 Standard Edition входят стандартные средства предотвращения потери данных и их восстановления в случае возможных сбоев. Имеющиеся средства резервного копирования предоставляют пользователям возможность выбора различных стратегий резервного копирования, обеспечивающих необходимый уровень защиты данных в случае возникновения сбоев в работе системы, при этом пользователям предоставляется возможность выполнения резервного копирования файлов данных и журналов транзакций на несъемные и съемные устройства хранения.

СУБД Microsoft® SQL Server™ 2005 Standard Edition поддерживает резервные копии моментальных снимков и технологии восстановления (резервные копии моментальных снимков SQL Server) вместе с независимыми поставщиками программного и аппаратного обеспечения. Резервные копии моментальных снимков снижают или исключают использование ресурсов СУБД при резервном копировании, что особенно важно для БД большого объема, для которых критична доступность.

Моментальные снимки базы данных предоставляют эффективный способ возврата базы данных к точке с известной логической согласованностью. Моментальный снимок базы данных записывает текущее состояние данных в базе данных, как если бы произошел откат всех активных транзакций. Затем моментальный снимок записывает все изменения данных, произошедшие после этой точки. Если сделана ошибка, например удалена большая таблица, база данных может быть возвращена в состояние, в котором она находилась в момент выполнения моментального снимка.

2.2.2.2 Восстановление системы

Функциональная возможность восстановления системы позволяет возвращать СУБД Microsoft® SQL Server™ 2005 Standard Edition в состояние, предшествующее сбою. При этом в БД не происходит потери (либо потери будут минимальны) и искажения данных. Данная возможность обеспечивается поддержкой СУБД Microsoft® SQL Server™ 2005 Standard Edition журналов транзакций. Журналы транзакций содержат всю информацию, необходимую для отмены или повторения любого из изменений БД. Благодаря данной возможности любое изменение, записанное на диск, например создание нового объекта БД или добавление данных в таблицу, может быть отменено, если транзакция, вызвавшая изменение, была прервана или ее невозможно завершить, либо может быть подтверждено, что транзакция была завершена, но результат ее выполнения

не был записан на диск. При использовании данной возможности осуществляется активный мониторинг всех изменений БД, а также автоматическое создание контрольных точек. В СУБД Microsoft® SQL Server™ 2005 Standard Edition создание контрольных точек производится в следующих случаях:

- при использовании оператора CHECKPOINT;
- при использовании оператора ALTER DATABASE;
- при корректном завершении работы ОО.

Использование механизма контрольных точек позволяет уменьшить простой в случае возможного сбоя в работе СУБД Microsoft® SQL Server™ 2005 Standard Edition. Благодаря этому механизму количество страниц в буферном кэше, которые не были записаны на диск, минимально.

СУБД Microsoft® SQL Server™ 2005 Standard Edition предоставляет улучшенную систему обнаружения ошибок и позволяет восстановить БД по журналу, несмотря на обнаружение ошибок. Механизм обнаружения ошибок состоит в возможном создании контрольной суммы резервной копии, которую можно создать операцией резервного копирования и проверить операцией восстановления. СУБД обеспечивает возможность управления операциями по проверки наличия ошибок и реакцией системы в случае их обнаружении.

2.2.2.3 Возможности масштабирования

Система управления базами данных Microsoft® SQL Server™ 2005 Standard Edition обеспечивает функции масштабирования для развертывания и поддержки больших производственных баз и хранилищ данных, а также для создания отказоустойчивых кластеров.

Система управления базами данных Microsoft® SQL Server™ 2005 Standard Edition обеспечивает поддержку распределенных транзакций и способна работать, одинаково эффективно используя одно- и многопроцессорные системы. При этом обеспечивается, что код, выполняемый на одном процессоре, не получит доступ и не модифицирует данные, обрабатываемые другим процессором. СУБД Microsoft® SQL Server™ 2005 Standard Edition поддерживает вытесняющую многозадачность, ввод-вывод «вразброс» и асинхронный ввод-вывод, что повышает пропускную способность и обеспечивает поддержку максимального числа одновременно работающих пользователей.

Система управления базами данных Microsoft® SQL Server™ 2005 Standard Edition обеспечивает симметричную многопроцессорную обработку, поддерживая до 32 симметричных процессоров и до 64 гигабайт оперативной памяти при функционировании под управлением ОС Microsoft® Windows Server™ 2003 Enterprise и Datacenter Edition.

2.2.2.4 Обеспечение высокого уровня доступности

СУБД Microsoft® SQL Server™ 2005 Standard Edition обеспечивает поддержку несколько режимов обеспечения высокого уровня доступности сервера БД или базы данных:

- **отказоустойчивый кластер:** обеспечивает поддержку высокого уровня доступности для всего экземпляра SQL Server. Отказоустойчивый кластер представляет собой сочетание одного или более узлов (северов БД), у которых имеются два или более общих дисков. Компоненты СУБД, такие как SQL Server или службы Notification Services, устанавливаются в кластерную группу службы кластеров Microsoft, называемую группой ресурсов. В каждый момент времени только один узел кластера владеет каждой группой ресурсов. У кластера имеется «виртуальное имя», независимое от имени узла, и поэтому на него можно ссылаться, как на виртуальный сервер. Приложение может подключиться к виртуальному серверу, ссылаясь на имя кластера, не зная, на каком узле в действительности находится виртуальный сервер. В сети виртуальный сервер SQL Server выглядит, как один компьютер, но при этом обеспечивает переход на другой узел в случае, если текущий узел становится недоступен;
- **зеркальное отображение базы данных:** это программное решение, предназначенное главным образом для увеличения доступности базы данных, обеспечивающее почти мгновенный переход на другой ресурс. Зеркальное отображение базы данных может использоваться для поддержки одиночной базы данных «горячего резерва», или зеркальной базы данных, которая соответствует базе данных, доступной для чтения и записи, называемой основной базой данных. Зеркальная база данных создается при помощи восстановления полной резервной копии основной базы данных. Зеркальная база данных недоступна для клиентов. Однако возможно ее использование для отчетов путем создания моментального снимка зеркальной базы данных.

Моментальный снимок базы данных предоставляет клиентам доступ только для чтения к данным, находившимся в базе данных в момент создания моментального снимка;

- **доставка журналов:** аналогично зеркальному отображению базы данных, доставка журналов функционирует на уровне базы данных. Доставка журналов может использоваться для поддержки одной или более баз данных «горячего резерва», называемых БД-получателями, которые соответствуют базе данных, доступной для чтения и записи, называемой БД-источник. Каждая БД-получатель создается при помощи восстановления полной резервной копии БД-источника. Конфигурация доставки журналов включает один сервер-источник (содержащий БД-источник), один или несколько серверов-получателей (каждый из которых содержит БД-получатель) и сервер мониторинга. Каждый сервер-получатель регулярно обновляет свою БД-получателя из резервной копии журналов транзакций БД-источника. Доставка журналов обеспечивает гибкость поддержки нескольких резервных баз данных;
- **репликация:** при репликации используются модель публикации-подписки, которая позволяет серверу-источнику (издателю) распространять данные на один или более серверов-получателей (подписчиков). Репликация обеспечивает доступность и масштабируемость этих серверов в режиме реального времени. Она поддерживает фильтрацию, чтобы обеспечить передачу подмножества данных на сервер-подписчик, а также разрешает секционированные обновления. SQL Server предлагает три типа репликации: репликации моментальных снимков, репликации транзакций и репликации слиянием.

2.2.3 Основные средства администрирования, управления и поддержки

Средства администрирования, управления и поддержки обеспечивают полномасштабное и гибкое управление СУБД Microsoft® SQL Server™ 2005 Standard Edition. Краткое описание основных из них представлено ниже.

2.2.3.1 Средства администрирования

В составе СУБД Microsoft® SQL Server™ 2005 Standard Edition интегрированы следующие графические средства администрирования и утилиты командной строки:

1. Графические инструментальные средства
   - *SQL Server Management Studio* – основное средство администрирования СУБД Microsoft® SQL Server™ 2005 Standard Edition и БД;
   - *SQL Query Analyzer* – графическая утилита, используемая для создания и управления объектами БД и интерактивного тестирования операторов, пакетов и сценариев, написанных на языке Transact-SQL;
   - *SQL Server Profiler* – утилита, используемая для мониторинга и перехвата определенных событий аудита с целью их последующего анализа и воспроизведения;
   - *Диспетчер конфигурации SQL Server (SQL Server Configuration Manager)* – утилита, используемая для запуска, приостановления выполнения, завершения работы и изменения конфигурации служб из состава СУБД Microsoft® SQL Server™ 2005 Standard Edition, а также для настройки клиентских сетевых библиотек и создания псевдонимов, включающих настраиваемые параметры подключения к серверам;
   - *Database Engine Tuning Advisor* – средство по настройке параметров производительности ядра SQL Database Engine с целью повышения скорости обработки запросов. Помощник по настройке ядра СУБД выявляет, каким образом запросы обрабатываются в указанных пользователем базах данных, а затем выдает рекомендации по повышению скорости обработки запросов путем изменения структур физического проектирования, таких как индексы, индексированные представления и секции.
2. Утилиты командной строки
   - *Osql* – утилита, позволяющая создавать и передавать СУБД Microsoft® SQL Server™ 2005 Standard Edition интерактивные запросы, составленные из операторов языка Transact-SQL, системных процедур и файлов сценариев;
   - *Bcp* – утилита, позволяющая в пользовательском формате копировать данные из БД в текстовый файл и обратно. С помощью программы bcp можно выполнять импорт большого количества новых строк в таблицы SQL Server или экспорт данных из таблиц в файлы данных;
   - *Dtsexec* – утилита, позволяющая выполнять пакеты DTS (Data Transformation Services), предоставляющие возможность подключения к

источнику данных, копирования и управления данными и объектами БД. Программа dtexec обеспечивает доступ ко всем функциям настройки и выполнения пакетов, таким, как соединения, свойства, переменные, ведение журналов, а также индикаторы выполнения;

– *SQLmain* – утилита, позволяющая администратору выполнять определенный набор задач по обслуживанию одной или нескольких БД, включая проверку целостности средствами консольных команд DBCC (Database Console Command), резервное копирование файлов данных и журнала транзакций, обновление статистики распределения и обновление индексов;
– *sqlcmd* – утилита, позволяющая вводить инструкции Transact-SQL, системные процедуры и файлы сценариев в командной строке.

2.2.3.2 Консоль управления MMC

Консоль управления Microsoft Management Console (MMC) – средство для создания, сохранения и запуска средств администрирования (называемых оснастками MMC), с помощью которых осуществляется управление работой СУБД Microsoft® SQL Server™ 2005 Standard Edition.

Консоль MMC не выполняет административных функций, но в ней размещаются инструменты, выполняющие эти функции. Основным типом инструментов, которые можно добавить в консоль, является оснастка. Оснастка SQL Server Management Studio является оснасткой консоли управления MMC, через которые доступны основные функции управления СУБД Microsoft® SQL Server™ 2005 Standard Edition.

2.2.4 Основные функциональные возможности обеспечения сетевой безопасности

Система управления базами данных Microsoft® SQL Server™ 2005 Standard Edition обеспечивает возможность поддержки безопасных сетей, построенных на основе стандарта безопасности Kerberos v.5.

Поддержка протокола Kerberos

Система управления базами данных Microsoft® SQL Server™ 2005 Standard Edition обеспечивает поддержку протокола Kerberos v.5. Поддержка протокола Kerberos v.5 обеспечивает передачу функций проверки подлинности осуществляющих доступ к СУБД Microsoft® SQL Server™ 2005 Standard Edition пользователей ОС, под управлением которой функционирует СУБД Microsoft® SQL Server™ 2005 Standard Edition. Таким

образом, благодаря поддержке СУБД Microsoft® SQL Server™ 2005 Standard Edition протокола Kerberos v.5 пользователям предоставляется возможность однократного ввода аутентификационных данных при регистрации в операционной системе и доступе к БД, поддерживаемых СУБД Microsoft® SQL Server™ 2005 Standard Edition. Кроме того, это позволяет обеспечить делегирование учетной записи пользователя, т.е. возможности подключения к разным серверам БД, сохраняя при переключении между ними реквизиты проверки подлинности пользователя. Благодаря этому доступ к ресурсам предоставляется по имени и паролю прошедшего проверку подлинности пользователя, а не учетной записи, используемой службой SQL Server.

2.3 Среда функционирования и границы ОО

2.3.1 Среда функционирования

Среда функционирования ОО определяется вариантами установки клиентских приложений и ОО и предусматривает установку приложений и ОО либо на одном компьютере (см. рисунок 2.1), либо на разных компьютерах, объединенных в сеть (см. рисунок 2.2). Функционирование ОО предполагается под управлением серверной ОС Microsoft® Windows® Server 2003.

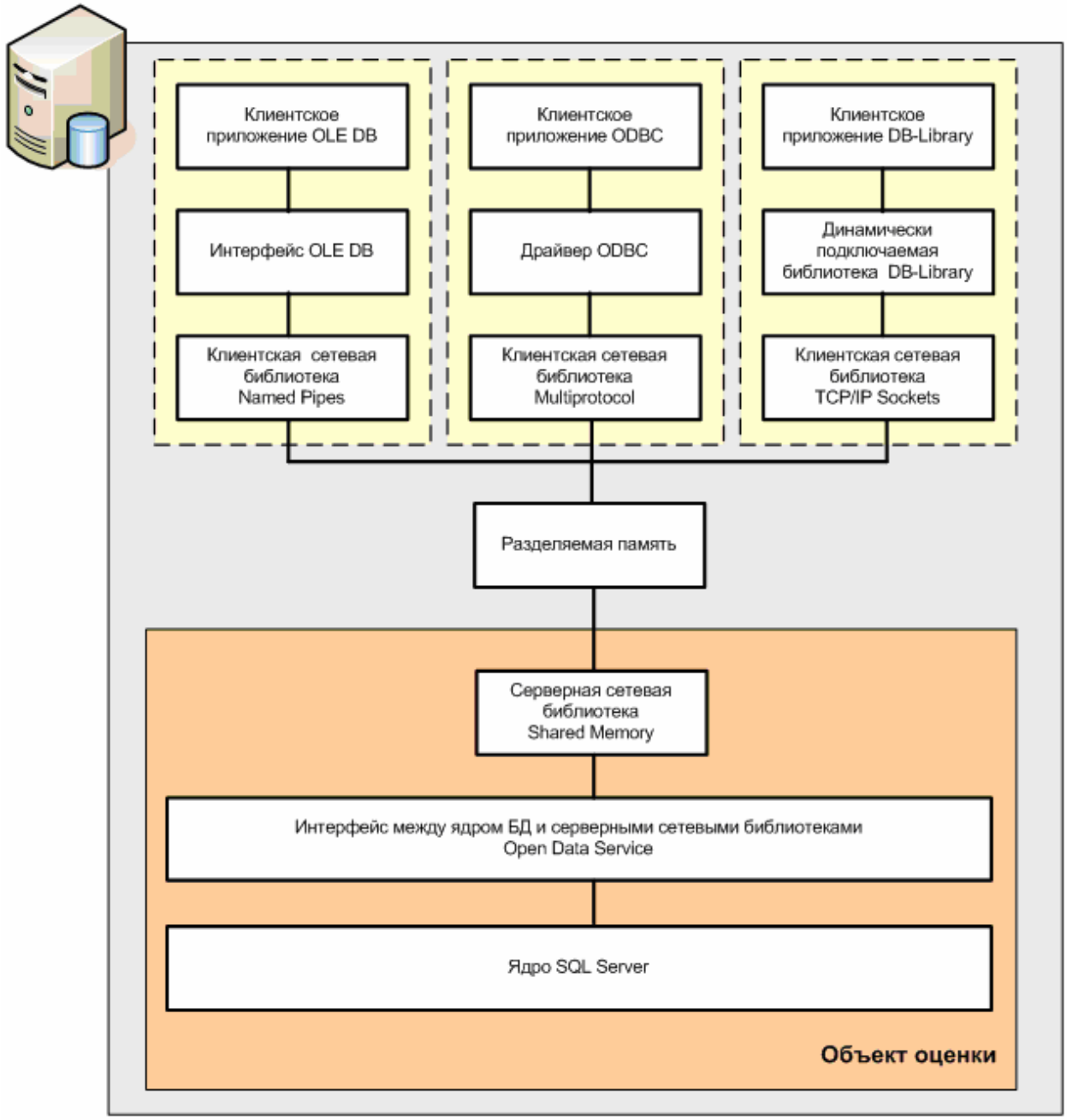

Рисунок 2.1 – Вариант функционирования ОО и клиентских приложений на одном компьютере

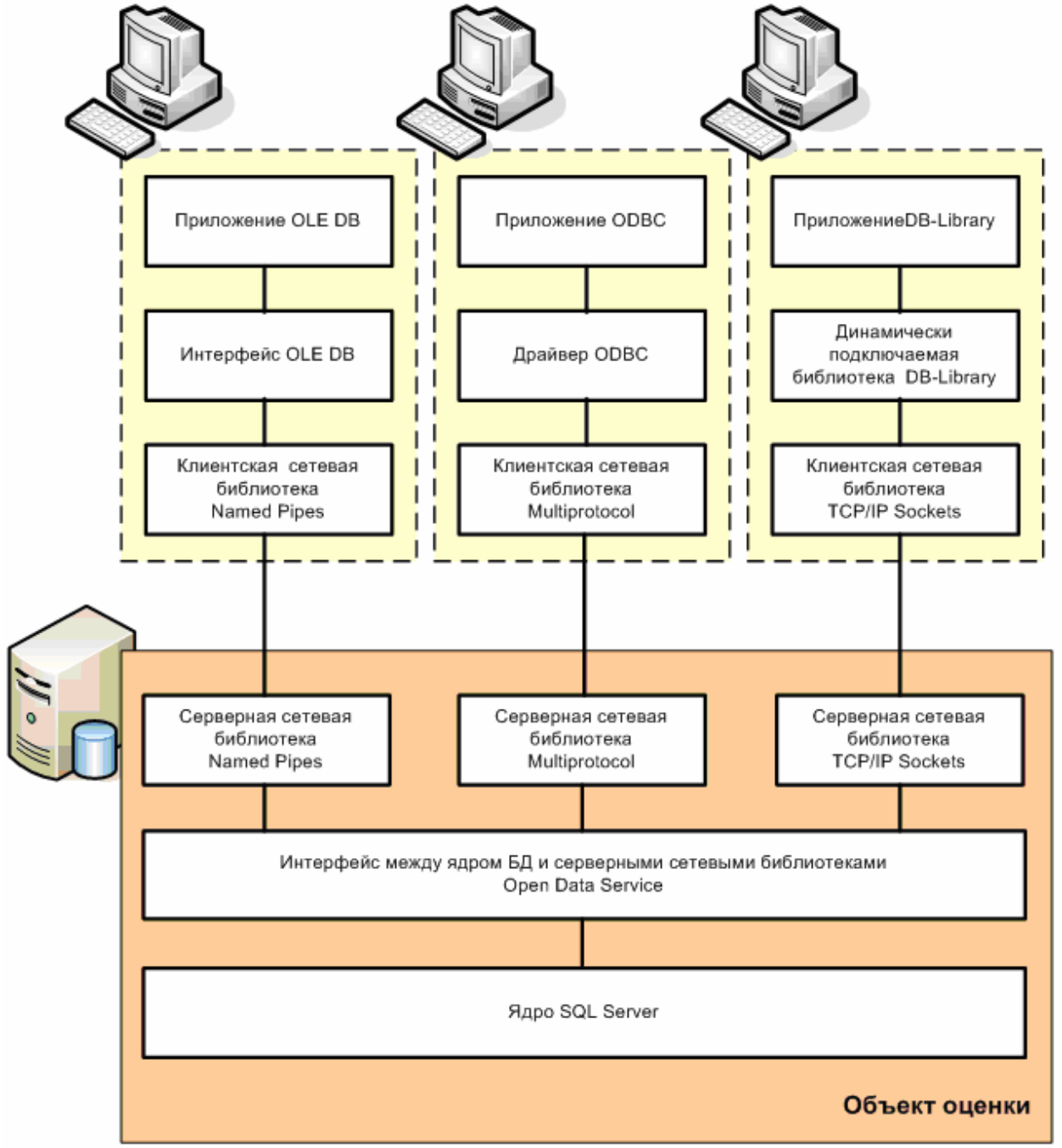

Рисунок 2.2 – Вариант функционирования ОО и клиентских приложений на разных компьютерах, объединенных в сеть

Кроме того, ОО может функционировать как на автономном компьютере (сервере БД), так и на компьютере (сервере БД) в составе локальной вычислительной сети. В свою очередь в локальной вычислительной сети может быть развернута инфраструктура службы каталогов Microsoft® Active Directory™ на базе серверной ОС Microsoft® Windows

Server 2003™. В этом случае компьютер (сервер БД), функционирующий под управлением ОС Microsoft® Windows Server 2003™, может быть включен в состав домена Active Directory™, либо не входить в него, но иметь возможность взаимодействия с другими компьютерами. Взаимодействие компьютера в данной конфигурации с остальными будет эквивалентно взаимодействию компьютеров в составе рабочей группы (Workgroup).

Таким образом, исходя из вариантов размещения ОО и клиентских приложений (на одном, либо на разных компьютерах), а также вариантов функционирования ОО (на автономном компьютере, либо на компьютере в составе локальной вычислительной сети, включенном в домен Active Directory™), установлены следующие конфигурации ОО, определяющие среду функционирования ОО (см. таблицу 2.1).

Таблица 2.1 – Конфигурации ОО, определяющие среду функционирования ОО

№ п/п	Конфигурации ОО
При включении компьютера в состав домена Active Directory™	
1.	ОО установлен на компьютере, одновременно являющемся контроллером домена Active Directory™ и сервером БД. Клиентские приложения установлены на входящие в состав домена Active Directory™ клиентские рабочие станции, функционирующие под управлением клиентской ОС Microsoft® Windows® XP Professional.
2.	ОО установлен на компьютере, не являющемся контроллером домена Active Directory™, функционирующем под управлением серверной ОС Microsoft® Windows Server 2003™. Клиентские приложения также установлены на данном компьютере.
3.	ОО установлен на компьютере, не являющемся контроллером домена Active Directory™, функционирующем под управлением серверной ОС Microsoft® Windows Server 2003™. Клиентские приложения установлены на входящие в состав домена Active Directory™ клиентские рабочие станции, функционирующие под управлением клиентской ОС Microsoft® Windows® XP Professional.

№ п/п	Конфигурации ОО
Компьютер не входит в состав домена Active Directory™ (конфигурация Stand-Alone)	
4.	ОО установлен на автономном компьютере, функционирующем под управлением серверной ОС Microsoft® Windows Server 2003™. Клиентские приложения также установлены на данном компьютере.
5.	ОО установлен на функционирующем под управлением серверной ОС Microsoft® Windows Server 2003™ компьютере, включенном в сеть, но не входящем в состав домена Active Directory™. Клиентские приложения установлены на клиентские рабочие станции, функционирующие под управлением клиентской ОС Microsoft® Windows® XP Professional.

2.3.2 Логические границы ОО

Объект оценки представляет собой модульную систему, состоящую из нескольких программных компонентов, работающих в пользовательском режиме и совместно решающих различные задачи. Каждый компонент ОО имеет необходимые интерфейсы для взаимодействия с другими компонентами системы (см. рисунок 2.3).

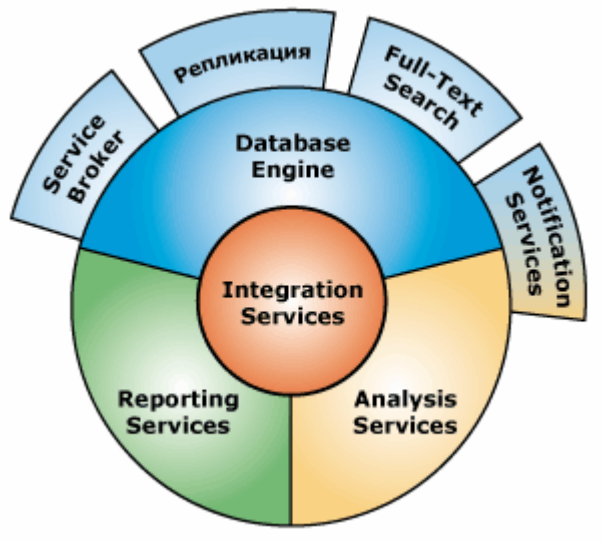

Рисунок 2.3 – Общая схема ОО

2.3.3 Физические границы ОО

Физические границы ОО включают персональный компьютер (сервер) со следующими минимально необходимыми аппаратными характеристиками (см. таблицу 2.2).

Таблица 2.2.

№ п/п	Показатель	Минимальные требования	Рекомендуемые требования
1.	Процессор Intel Pentium III или аналогичный	тактовая частота 600 МГц	тактовая частота 1 ГГц и более
2.	Объем оперативной памяти	512 Мб	1024 Мб и более
3.	Привод CD-ROM	привод CD- или DVD-ROM из списка совместимого оборудования HCL, одобренного компанией Microsoft.	
4.	Монитор	SVGA-совместимый, обеспечивающий поддержку разрешения экрана не менее 1024x768 точек.	
5.	Объем свободного дискового пространства	Ядро Database Engine - 150 Мб; Компоненты службы Analysis Services - 35 Мб; Компоненты службы Reporting Services и Диспетчер отчетов (Report Manager) - 40 Мб; Компоненты службы Notification Services - 5 Мб; Компоненты службы Integration Services - 9 Мб; Клиентские компоненты - 12 Мб; Средства управления - 70 Мб; Средства разработки - 20 Мб; Справочная информация (SQL Server Books Online и SQL Server Mobile Books Online) - 15 Мб; Образцы кода и примеры баз данных - 390 Мб.	

2.4 Службы безопасности ОО

В данном подразделе приводится краткое описание служб безопасности ОО, реализующих оцениваемые (в соответствии с настоящим ЗБ) функции безопасности ОО.

2.4.1 Аудит безопасности

Объект оценки обеспечивает распознавание, запись и хранение информации, связанной с событиями, существенными с точки зрения безопасности, а также предоставляет средства для анализа информации о таких событиях. Категории событий, подлежащих регистрации, определяются администратором ОО и могут детализироваться вплоть до конкретного класса событий. После настройки параметров политики аудита можно отслеживать всю совокупность относящихся к безопасности событий аудита и анализировать недостатки системы безопасности. Записи аудита, содержащие сведения о выбранных событиях, включают информацию о пользователе, который был инициатором события и выполнял какие-либо действия в отношении контролируемого объекта доступа, а также имя компьютера, текст запроса на языке Transact-SQL или хранимой процедуры, время начала и завершения действия и другие данные. ОО обеспечивает возможность доступа к журналу аудита только уполномоченным на это администраторам ОО.

2.4.2 Защита данных пользователя

Объект оценки осуществляет функции и политику дискреционного (избирательного) управления доступом. Дискреционное управление доступом предоставляет возможность ограничивать и контролировать доступ к ОО, базам данных, схемам и их объектам, таким как таблицы, представления и хранимые процедуры. Каждый пользователь, пытающийся получить доступ к ОО, сначала проходит аутентификацию, а затем, при попытках получения доступа к ресурсам – авторизацию, т.е. проверку разрешений пользователя по отношению к какому-либо защищаемому объекту. Вся информация, определяющая контекст безопасности субъекта доступа, хранится в структуре PSS (Process Status Structure), которая содержит идентификатор безопасности пользователя, выполнившего подключение, идентификаторы безопасности ролей, участниками которых он является, и другую относящуюся к безопасности и состоянию сеанса информацию. Структура PSS является постоянной на всем промежутке времени подключения пользователя к ОО. Вся информация, определяющая безопасность защищаемого объекта, хранится в системной таблице `sys.database_permissions`.

2.4.3 Идентификация и аутентификация

Идентификация и аутентификация пользователя должны осуществляться до выполнения им каких-либо действий в ОО. Объект оценки требует, чтобы все пользователи уникально идентифицировались при входе в систему с помощью ввода идентификатора пользователя. При этом аутентификация пользователя может быть обеспечена двумя способами:

- средствами ОО;
- средствами операционной системы.

Первый способ проверки подлинности не позволяет обеспечить передачу аутентификационной информации в защищенном от перехвата виде, а также доверенного маршрута передачи аутентификационной информации. В тоже время при его использовании ОО предоставляет возможность применения к учетным записям SQL Server, используемым для прямого подключения к ОО, требований политики паролей и политики блокировки учетной записи, задаваемых через механизм групповой политики средой ОО, что обеспечивает верификацию критериев качества используемой пользователями SQL Server аутентификационной информации.

Использование второго способа предполагает проверку подлинности аутентификационных данных субъекта доступа средствами операционной системы, под управлением которой функционирует ОО. В дальнейшем при осуществлении доступа к ОО, повторная проверка подлинности не осуществляется, поскольку ОО доверяет результатам проверки, выполненной при регистрации пользователя в операционной системе. Данный способ проверки подлинности позволяет устранить недостатки механизма проверки подлинности средствами ОО.

2.4.4 Управление безопасностью

Объект оценки осуществляет функции, обеспечивающие управление ролями, а также предоставляющие ряд возможностей по управлению различными характеристиками безопасности. Использование ролей обеспечивает простой механизм назначения полномочий пользователю на выполнение определенных действий в БД и над ее объектами. ОО поддерживает ряд предопределенных ролей сервера БД, создаваемых в момент установки, и фиксированные роли БД, для которых определены предопределенные полномочия для работы с БД.

2.4.5 Защита ФБО

Объект оценки и среда функционирования ОО предоставляют ряд возможностей для обеспечения защиты функций безопасности ОО, таких как обеспечение целостности ФБО, поддержание домена безопасности и предоставление ФБО надежных меток времени.

2.4.6 Управление доступом к ОО

Объект оценки обеспечивает возможность ограничения открытия сеанса доступа на основе идентификатора регистрационной записи пользователя. При обращении пользователя к ОО, ФБО осуществляют проверку разрешений на подключение данного субъекта доступа. Проверка осуществляется на основе идентификатора регистрационной записи пользователя (login identifier), для которого администратором определены разрешающие или запрещающие права доступа к ОО. Для идентификации пользователя, осуществляющего доступ к ОО, используется предъявляемый им билет Kerberos (Kerberos ticket), представляющий собой персональное электронное «удостоверение» пользователя. В последующем, ОО извлекает из билета Kerberos идентификаторы безопасности SID, однозначно идентифицирующие пользователя и группы безопасности Windows, участниками которых он является, и проверяет их наличие в системном представлении `sys.server_principals` базы данных `master`. Если в данной таблице существуют записи, содержащие идентификаторы, совпадающие с идентификаторами SID, извлеченными из билета Kerberos, ОО просматривает содержимое полей таблицы, определяющих доступ к ОО. В случае если для регистрационной записи пользователя определены запрещающие права доступа либо пользователь не имеет действительной регистрационной записи в ОО, в доступе к ОО будет отказано.

Объект оценки обеспечивает возможность ограничения количества одновременно открытых сеансов доступа к ОО. По умолчанию количество параллельных пользовательских соединений устанавливается автоматически и изменяется динамически. Если в системе зарегистрировано 10 пользователей, то существует 10 установленных пользовательских соединений. При доступе к ОО еще одного пользователя, автоматически будет создано еще одно пользовательское соединение и так вплоть до разрешенного максимального количества соединений. Максимальное количество пользовательских соединений, поддерживаемых ОО, составляет 32767. В случае

превышения указанного количества соединений система выдаст сообщение об ошибке и в создании нового подключения пользователем будет отказано.

2.4.7 Использование ресурсов ОО

В ОО предусмотрены механизмы управления размером БД, предоставляющие возможность ограничивать объем доступного для БД дискового пространства.

Устанавливаемый по умолчанию для файлов данных и файлов журналов транзакций минимальный размер равен 1 Mb (space allocated – 1Mb), максимальный размер файлов неограничен (maximum file size – unrestricted file growth), величина приращения файлов – 10% от общего объема файла (file growth – by percent 10).

Чтобы контролировать рост файлов БД и объем свободного дискового пространства, ОО предоставляет возможность ограничивать объем доступного для БД дискового пространства (применять квоты), что исключает неограниченное увеличение ее размера. При этом предельный размер выделяемой квоты может быть установлен для файлов данных и файлов журнала транзакций БД. Уполномоченному администратору предоставлена возможность управления минимальным и максимальным размером, величиной приращения и параметром автоматического увеличения размера для каждого (основного и дополнительного) файла данных и файла журнала транзакций БД.

Объект оценки обеспечивает статическое или динамическое управление объемом физической памяти, используемой ОО в качестве буферного пула.

При использовании динамического управления ОО автоматически распределяет и освобождает память для обеспечения повышенной производительности. Если вся доступная физическая память уже передана какому-либо серверному приложению, ОО выполняет перераспределение памяти между приложениями. По умолчанию физическая память распределяется ОО динамически.

Объект оценки позволяет администратору ОО изменять параметры конфигурации памяти таким образом, чтобы ОО мог использовать фиксированный либо динамически изменяемый объем физической памяти. Кроме того, уполномоченному администратору ОО предоставлена возможность управления минимальным и максимальным размером памяти, используемым ОО для буферного пула, а также дополнительным объемом физической памяти, позволяющим резервировать заданный объем памяти от распределения между другими приложениями.

3 Среда безопасности ОО

Данный раздел содержит описание следующих аспектов среды безопасности ОО:

- предположений относительно предопределенного использования ОО и аспектов безопасности среды ОО;
- угроз безопасности, которым нужно противостоять средствами ОО;
- политики безопасности организации, которой должен следовать ОО.

3.1 Предположения безопасности

3.1.1 Предположения относительно предопределенного использования ОО

A.ImpossibleModif

Должно быть обеспечено отсутствие на компьютере с установленным ОО нештатных программных средств, позволяющих осуществить несанкционированную модификацию ОО.

A.Connect

Доступ к ОО должен осуществляться только из санкционированных точек доступа, размещенных в контролируемой зоне, оборудованной средствами и системами физической защиты и охраны (контроля и наблюдения) и исключающей возможность бесконтрольного пребывания посторонних лиц.

A.Peer

Должно быть обеспечено взаимодействие ОО только с доверенными системами ИТ, ПБО которых скоординированы с ПБО рассматриваемого ОО.

A.TOEConfig

Должны быть обеспечены установка, конфигурирование и управление ОО в соответствии с руководствами и согласно оцененным конфигурациям.

A.OSAuth

Аутентификация субъектов, осуществляющих попытку доступа к ОО, должна осуществляться с использованием механизмов ОС, под управлением которой функционирует ОО.

A.Environment

Функционирование ОО должно осуществляться в среде функционирования (ОС), предоставляющей механизм аутентификации, обеспечивающий адекватную защиту от прямого или умышленного нарушения безопасности нарушителями с умеренным потенциалом нападения.

A.RecoverySafeState

Должны быть предусмотрены мероприятия, направленные на восстановление безопасного состояния ОО в случае сбоя (отказа) программного и аппаратного обеспечения ОО.

3.1.2 Предположения относительно среды функционирования ОО

Предположение, связанное с физической защитой ОО

A.Locate

Для предотвращения несанкционированного физического доступа компьютер с установленным ОО должен располагаться в контролируемой зоне, оборудованной средствами и системами физической защиты и охраны (контроля и наблюдения) и исключающей возможность бесконтрольного пребывания посторонних лиц.

Предположения, имеющее отношение к персоналу

A.NoEvilAdm

Персонал, ответственный за администрирование ОО, должен пройти проверку на благонадежность и компетентность, а также в своей деятельности должен руководствоваться соответствующей документацией.

A.NoEvilUser

Уполномоченные на доступ к ОО пользователи должны пройти проверку на благонадежность, а их совместные действия должны быть направлены исключительно на выполнение своих функциональных обязанностей.

3.2 Угрозы

3.2.1 Угрозы, которым противостоит ОО

В настоящем ЗБ определены следующие угрозы, которым противостоит ОО.

T.UnauthAccessData

1. Аннотация угрозы – осуществление доступа к информации, размещаемой на объектах ОО, неуполномоченными на это пользователями ОО.

2. Источники угрозы – пользователи ОО.

3. Способ реализации угрозы – осуществление доступа к информации, размещаемой на объектах ОО, с использованием приложений, поддерживающих возможность взаимодействия с ОО.

4. Используемые уязвимости – недостатки механизмов разграничения доступа к объектам ОО, связанные с возможностью предоставления доступа к информации, размещаемой на объектах ОО, неуполномоченным на это пользователям ОО.

5. Вид активов, потенциально подверженных угрозе – информация, размещаемая на объектах ОО.

6. Нарушаемые свойства безопасности активов – конфиденциальность, целостность, достоверность, доступность.

7. Возможные последствия реализации угрозы – несанкционированное ознакомление с информацией, размещаемой на объектах ОО; несанкционированная модификация информации (в том числе подмена), размещаемой на объектах ОО; несанкционированное удаление информации, размещаемой на объектах ОО.

T.UnauthExecProc&Fanc

1. Аннотация угрозы – выполнение хранимых процедур и определяемых функций неуполномоченными на это пользователями ОО.

2. Источники угрозы – пользователи ОО.

3. Способ реализации угрозы – осуществление доступа к хранимым процедурам и определяемым функциям с использованием приложений, поддерживающих возможность взаимодействия с ОО, и запуск их на выполнение.

4. Используемые уязвимости – недостатки механизмов разграничения доступа к объектам ОО, связанные с возможностью выполнения хранимых процедур и определяемых функций неуполномоченным на это пользователям ОО.

5. Вид активов, потенциально подверженных угрозе – хранимые процедуры и определяемые функции.

6. Нарушаемое свойство безопасности активов – несанкционированное выполнение.

7. Возможные последствия реализации угрозы – несанкционированное ознакомление с информацией, выдаваемой после отработки хранимых процедур и функций; нарушение режимов функционирования ОО и БД.

T.UnauthAccessTOE

1. Аннотация угрозы – осуществление доступа к ОО сторонними субъектами и возможность несанкционированного управления и ознакомления с защищаемой информацией, хранящейся в БД.

2. Источники угрозы – сторонние субъекты (пользователи других экземпляров ОО, пользователи сторонних по отношению к ОО систем (в т.ч. СУБД)).

3. Способ реализации угрозы – осуществление доступа к ОО с использованием приложений, поддерживающих возможность взаимодействия с ОО.

4. Используемые уязвимости – недостатки механизмов разграничения доступа к ОО, связанные с возможностью осуществления доступа к ОО сторонними субъектами.

5. Вид активов, потенциально подверженных угрозе – данные ФБО; защищаемая информация, хранящаяся в БД.

6. Нарушаемые свойства безопасности активов – целостность, подконтрольность, конфиденциальность.

7. Возможные последствия реализации угрозы – нарушение режимов функционирования ОО; несанкционированное ознакомление с защищаемой информацией, хранящейся в БД.

T.MasqAdmin&User

1. Аннотация угрозы – осуществление доступа к ОО пользователем ОО или администратором ОО под видом другого уполномоченного пользователя ОО или администратора ОО.

2. Источники угрозы – пользователи ОО; администраторы ОО.

3. Способ реализации угрозы – осуществление доступа к ОО с использованием приложений, поддерживающих возможность взаимодействия с ОО; осуществление доступа к ОО с использованием инструментальных средств, входящих в состав ОО.

4. Используемые уязвимости – недостатки механизмов разграничения доступа к ОО, связанные с возможностью доступа к ОО под видом других уполномоченных пользователей и администраторов ОО.

5. Вид активов, потенциально подверженных угрозе – данные ФБО; защищаемая информация, хранящаяся в БД.

6. Нарушаемые свойства безопасности активов – целостность, подконтрольность, конфиденциальность.

7. Возможные последствия реализации угрозы – нарушение режимов функционирования ОО; несанкционированное ознакомление с защищаемой информацией, хранящейся в БД; невозможность однозначного сопоставления совершенных в ОО действий с субъектом, совершившим данные действия.

T.UnauthAccessAuditData

1. Аннотация угрозы – осуществление доступа к данным аудита ОО пользователями ОО и неуполномоченными на это администраторами ОО и возможность несанкционированного удаления и модификации данных аудита ОО.

2. Источники угрозы – пользователи ОО; администраторы ОО.

3. Способы реализации угрозы – осуществление доступа к данным аудита ОО с использованием приложений, поддерживающих возможность взаимодействия с ОО; осуществление доступа к данным аудита с использованием инструментальных средств, входящих в состав ОО.

4. Используемые уязвимости – недостатки механизмов разграничения доступа к данным аудита, связанные с возможностью осуществления доступа к данным аудита пользователями ОО и неуполномоченными на это администраторами ОО.

5. Вид активов, потенциально подверженных угрозе – данные аудита ОО.

6. Нарушаемые свойства безопасности активов – подконтрольность, целостность, конфиденциальность.

7. Возможные последствия реализации угрозы – невозможность осуществления контроля действий пользователей ОО и администраторов ОО, а также контроля процесса функционирования ОО в целом; навязывание администраторам ОО, ответственным за контроль данных аудита ОО, ложных (модифицированных) данных аудита; несанкционированное ознакомление о произошедших в ОО событиях.

T.LostAuditDataOverStg

1. Аннотация угрозы – потеря данных аудита ОО вследствие переполнения выделенного для задач аудита хранилища информации.

2. Источники угрозы – события, подвергаемые аудиту.

3. Способ реализации угрозы – переполнение выделенного для задач аудита хранилища информации.

4. Используемые уязвимости – недостатки механизмов защиты данных аудита ОО, связанные с невозможностью предотвращения потери данных аудита из-за переполнения хранилища данных аудита ОО.

5. Вид активов, потенциально подверженных угрозе – данные аудита ОО.

6. Нарушаемые свойства безопасности активов – целостность.

7. Возможные последствия реализации угрозы – невозможность осуществления контроля произошедших в ОО событий.

T.LostAuditDataOverDisk

1. Аннотация угрозы – потеря данных аудита ОО вследствие исчерпания свободного дискового пространства.

2. Источники угрозы – события, подвергаемые аудиту.

3. Способ реализации угрозы – исчерпание свободного дискового пространства.

4. Используемые уязвимости – недостатки механизмов защиты данных аудита ОО, связанные с невозможностью предотвращения потери данных аудита из-за исчерпания свободного дискового пространства.

5. Вид активов, потенциально подверженных угрозе – данные аудита ОО.

6. Нарушаемые свойства безопасности активов – целостность.

7. Возможные последствия реализации угрозы – невозможность осуществления контроля произошедших в ОО событий.

T.UnauthAccessTSF

1. Аннотация угрозы – осуществление доступа к данным ФБО пользователями ОО и неуполномоченными на это администраторами ОО.

2. Источники угрозы – пользователи ОО; администраторы ОО.

3. Способ реализации угрозы – осуществление доступа к данным ФБО с использованием приложений, поддерживающих возможность взаимодействия с ОО; осуществление доступа к данным ФБО с использованием инструментальных средств, входящих в состав ОО.

4. Используемые уязвимости – недостатки механизмов защиты данных ФБО, связанные с возможностью несанкционированного доступа.

5. Вид активов, потенциально подверженных угрозе – данные ФБО.

6. Нарушаемые свойства безопасности активов – конфиденциальность, целостность, доступность, достоверность.

7. Возможные последствия реализации угрозы – несанкционированное ознакомление с данными ФБО (конфигурационные файлы, служебная информация и т.п.); навязывание ОО ложных (модифицированных) данных ФБО; нарушение режимов функционирования ОО.

T.UnauthUsageRes

1. Аннотация угрозы – использование ресурсов ОО неуполномоченными на это субъектами.

2. Источники угрозы – субъекты, действующие от имени пользователей ОО и администраторов ОО.

3. Способ реализации угрозы – неограниченное использование свободных ресурсов ОО субъектами, действующими от имени пользователей ОО и администраторов ОО.

4. Используемые уязвимости – недостатки механизмов защиты ресурсов ОО, связанные с возможностью несанкционированного использования.

5. Вид активов, потенциально подверженных угрозе – ресурсы ОО.

6. Нарушаемое свойство безопасности активов – доступность.

7. Возможные последствия реализации угрозы – нарушение режимов функционирования ОО, связанное с недостаточностью свободных ресурсов ОО.

3.2.2 Угрозы, которым противостоит среда

В настоящем ЗБ определены следующие угрозы, которым противостоит среда функционирования ОО.

TE.UnauthAccessTOE

1. Аннотация угрозы – осуществление доступа к ОО сторонними субъектами и возможность несанкционированного управления и ознакомления с защищаемой информацией, хранящейся в БД.

2. Источники угрозы – сторонние субъекты (пользователи других экземпляров ОО, пользователи сторонних по отношению к ОО систем (в т.ч. СУБД)).

3. Способ реализации угрозы – осуществление доступа к ОО с использованием приложений, поддерживающих возможность взаимодействия с ОО.

4. Используемые уязвимости – недостатки механизмов разграничения доступа к ОО, связанные с возможностью осуществления доступа к ОО сторонними субъектами.

5. Вид активов, потенциально подверженных угрозе – данные ФБО; защищаемая информация, хранящаяся в БД.

6. Нарушаемые свойства безопасности активов – целостность, подконтрольность, конфиденциальность.

7. Возможные последствия реализации угрозы – нарушение режимов функционирования ОО; несанкционированное ознакомление с защищаемой информацией.

TE.MasqAdmin&User

1. Аннотация угрозы – осуществление доступа к ОО пользователем ОО или администратором ОО под видом другого уполномоченного пользователя ОО или администратора ОО.

2. Источники угрозы – пользователи ОО; администраторы ОО.

3. Способ реализации угрозы – осуществление доступа к ОО с использованием приложений, поддерживающих возможность взаимодействия с ОО; осуществление доступа к ОО с использованием инструментальных средств, входящих в состав ОО.

4. Используемые уязвимости – недостатки механизмов разграничения доступа к ОО, связанные с возможностью доступа к ОО под видом других уполномоченных пользователей и администраторов ОО.

5. Вид активов, потенциально подверженных угрозе – данные ФБО; защищаемая информация, хранящаяся в БД.

6. Нарушаемые свойства безопасности активов – целостность, подконтрольность, конфиденциальность

7. Возможные последствия реализации угрозы – нарушение режимов функционирования ОО; несанкционированное ознакомление с защищаемой информацией; невозможность однозначного сопоставления совершенных в ОО действий с субъектом, совершившим данные действия.

TE.UnauthAccessTSF

1. Аннотация угрозы – осуществление доступа к данным ФБО пользователями ОО и неуполномоченными на это администраторами.

2. Источники угрозы – пользователи ОО; администраторы ОО.

3. Способ реализации угрозы – осуществление доступа к данным ФБО с использованием приложений, поддерживающих возможность взаимодействия с ОО; осуществление доступа к данным ФБО с использованием инструментальных средств, входящих в состав ОО.

4. Используемые уязвимости – недостатки механизмов защиты данных ФБО, связанные с возможностью несанкционированного доступа.

5. Вид активов, потенциально подверженных угрозе – данные ФБО.

6. Нарушаемые свойства безопасности активов – конфиденциальность, целостность, доступность, достоверность.

7. Возможные последствия реализации угрозы – несанкционированное ознакомление с данными ФБО (конфигурационные файлы, служебная информация и т.п.); навязывание ОО ложных (модифицированных) данных ФБО; нарушение режимов функционирования ОО.

TE.UnauthUsageRes

1. Аннотация угрозы – использование ресурсов ОО неуполномоченными на использование субъектами в нарушение политики безопасности.

2. Источники угрозы – субъекты, действующие от имени пользователей ОО и администраторов ОО.

3. Способ реализации угрозы – неограниченное использование свободных ресурсов ОО субъектами, действующими от имени пользователей ОО и администраторов ОО.

4. Используемые уязвимости – недостатки механизмов защиты ресурсов ОО, связанные с возможностью несанкционированного использования.

5. Вид активов, потенциально подверженных угрозе – ресурсы ОО.

6. Нарушаемое свойство безопасности активов – доступность.

7. Возможные последствия реализации угрозы – нарушение режимов функционирования ОО, связанное с недостаточностью свободных ресурсов ОО.

TE.UnauthAccessData

1. Аннотация угрозы – осуществление доступа к информации ОО, хранимой на уровне ОС в файлах файловой системы, неуполномоченными на это пользователями ОО.

2. Источники угрозы – пользователи ОО.

3. Способ реализации угрозы – осуществление доступа к информации, хранимой в файлах, с использованием приложений, поддерживающих возможность осуществления доступа к файлам.

4. Используемые уязвимости – недостатки механизмов разграничения доступа к файлам, связанные с возможностью предоставления доступа к информации, размещаемой в файлах, неуполномоченным на это пользователям ОО.

5. Вид активов, потенциально подверженных угрозе – информация, хранимая в файлах.

6. Нарушаемые свойства безопасности активов – конфиденциальность, целостность, достоверность, доступность.

7. Возможные последствия реализации угрозы – несанкционированное ознакомление с информацией, хранимой в файлах; несанкционированная модификация информации (в том числе подмена), хранимой в файлах; несанкционированное удаление информации, хранимой в файлах.

3.3 Политика безопасности организации

Объект оценки должен следовать приведенным ниже правилам политики безопасности организации.

P.Manage

Должны быть в наличии надлежащие корректно функционирующие средства администрирования ОО, доступные только уполномоченным администраторам ОО.

P.Audit

Должны быть обеспечены надлежащая регистрация и предупреждение администратора ОО о любых событиях, относящихся к безопасности ОО. Должна быть обеспечена возможность для администратора ОО выборочного ознакомления с информацией о произошедших по отношению к ОО событиях.

P.Resourse

Для уполномоченного администратора ОО должна быть обеспечена возможность управления надлежащим распределением ресурсов ОО.

P.Access

Должна быть обеспечена возможность для уполномоченных на это пользователей ОО определять доступность объектов ОО для других пользователей ОО.

P.GenerateTime

Должна быть обеспечена привязка по времени событий, подвергаемых аудиту.

P.TOEAuth

Должна обеспечиваться аутентификация субъектов, осуществляющих попытку доступа к ОО с рабочих станций и серверов под управлением ОС, не имеющих совместно с ОС (являющейся средой функционирования ОО) централизованного управления параметрами безопасности, механизмами самого ОО.

P.ManageAuthData

В случае аутентификации субъектов, осуществляющих попытку доступа к ОО, с использованием механизмов самого ОО, операционная система должна предоставлять

механизмы управления качеством аутентификационных данных, обеспечивающие адекватную защиту ОО от прямого или умышленного нарушения безопасности нарушителями с умеренным потенциалом нападения.

4 Цели безопасности

4.1 Цели безопасности для ОО

В данном разделе дается описание целей безопасности для ОО.

O.AccessObject

Разграничение доступа к объектам ОО

ОО должен обеспечивать доступ к объектам ОО только уполномоченным на это пользователям ОО. ОО должен обеспечивать возможность уполномоченным на это пользователям ОО определять доступность объектов ОО для других пользователей ОО.

O.AccessTOE

Разграничение доступа к ОО

ОО должен обеспечивать доступ к ОО только уполномоченным на это пользователям.

O.TOEAuth

Аутентификация с использованием механизмов ОО

ОО должен обеспечивать аутентификацию субъектов, осуществляющих попытку доступа к ОО с рабочих станций и серверов под управлением ОС, не имеющих совместно с ОС (являющейся средой функционирования ОО) централизованного управления параметрами безопасности.

O.AuditEvents

Аудит событий

ОО должен располагать надлежащими механизмами регистрации и предупреждения администратора ОО о любых событиях, относящихся к безопасности ОО. Механизмы регистрации должны предоставлять администраторам ОО возможность выборочного ознакомления с информацией о произошедших в ОО событиях.

O.ProtectAudit

Защита данных аудита

ОО должен обеспечивать доступ к данным аудита только уполномоченным администраторам ОО и предотвращать потерю данных аудита в случае переполнения их хранилища, а также в случае невозможности дальнейшего ведения аудита вследствие исчерпания свободного дискового пространства.

O.AdminManage

Наличие средств администрирования

ОО должен располагать надлежащими корректно функционирующими средствами администрирования, доступными только уполномоченным администраторам ОО.

O.ProtectResTSF

Защита данных ФБО и ресурсов ОО

ОО должен обеспечивать защиту данных ФБО и ресурсов ОО, поддерживая домен для функционирования ФБО.

O.DistrResourse

Распределение ресурсов ОО

ОО должен обеспечивать для уполномоченного администратора ОО возможность надлежащего распределения ресурсов ОО.

4.2 Цели безопасности для среды

В данном разделе дается описание целей безопасности для среды функционирования ОО.

OE.ImpossibleModif

Стерильность среды функционирования

Должно быть обеспечено отсутствие на компьютере с установленным ОО нештатных программных средств, позволяющих осуществить несанкционированную модификацию ОО.

OE.Connect

Контролируемые точки доступа

Доступ к ОО должен осуществляться только из санкционированных точек доступа, размещенных в контролируемой зоне, оборудованной средствами и системами физической защиты и охраны (контроля и наблюдения) и исключающей возможность бесконтрольного пребывания посторонних лиц.

OE.Peer

Взаимодействие с доверенными системами

Должно быть обеспечено взаимодействие ОО только с доверенными системами ИТ, ПБО которых скоординированы с ПБО рассматриваемого ОО.

OE.TOEConfig

Эксплуатация ОО

Должны быть обеспечены установка, конфигурирование и управление ОО в соответствии с руководствами и согласно оцененным конфигурациям.

OE.OSAuth

Аутентификация с использованием механизмов ОС

Аутентификация субъектов, осуществляющих попытку доступа к ОО, должна осуществляться с использованием механизмов ОС, под управлением которой функционирует ОО.

OE.Environment

Стойкость функции безопасности

Функционирование ОО должно осуществляться в среде функционирования (ОС), предоставляющей механизм аутентификации, обеспечивающий адекватную защиту от прямого или умышленного нарушения безопасности нарушителями с умеренным потенциалом нападения.

OE.ManageAuthData

Управление качеством аутентификационных данных

В случае аутентификации субъектов, осуществляющих попытку доступа к ОО, с использованием механизмов самого ОО, операционная система должна предоставлять механизмы управления качеством аутентификационных данных, обеспечивающие адекватную защиту ОО от прямого или умышленного нарушения безопасности нарушителями с умеренным потенциалом нападения.

OE.Locate

Физическая защита ОО

Для предотвращения несанкционированного физического доступа компьютер с установленным ОО должен располагаться в контролируемой зоне, оборудованной средствами и системами физической защиты и охраны (контроля и наблюдения) и исключающей возможность бесконтрольного пребывания посторонних лиц.

OE.NoEvilAdm

Требования к администраторам ОО

Персонал, ответственный за администрирование ОО, должен пройти проверку на благонадежность и компетентность, а также в своей деятельности должен руководствоваться соответствующей документацией.

OE.NoEvilUser

Требования к пользователям ОО

Уполномоченные на доступ к ОО пользователи должны пройти проверку на благонадежность, а их совместные действия должны быть направлены исключительно на выполнение своих функциональных обязанностей.

OE.ProtectResTSF

Защита данных ФБО и ресурсов ОО

Должна быть обеспечена защита данных ФБО и ресурсов ОО, а также поддержка домена для функционирования ФБО.

OE.GenerateTime

Поддержка аудита

Должна быть обеспечена поддержка средств аудита, используемых в ОО, и предоставление для них надлежащего источника меток времени.

OE.ProtectFileSystem

Защита на уровне файловой системы

Должна быть обеспечена защита данных, размещаемых в базах данных ОО, на уровне файлов файловой системы ОС от несанкционированного доступа.

OE.RecoverySafeState

Восстановление ОО

Должны быть предусмотрены мероприятия, направленные на восстановление безопасного состояния ОО в случае сбоя (отказа) программного и аппаратного обеспечения ОО.

5 Требования безопасности ИТ

В данном разделе ЗБ представлены требования безопасности ИТ, которым должен удовлетворять ОО и его среда. Функциональные требования, представленные в настоящем ЗБ, основаны на функциональных компонентах из части 2 ОК. Требования доверия основаны на компонентах требований доверия из части 3 ОК и представлены в настоящем ЗБ в виде оценочного уровня доверия ОУД1, усиленного компонентом доверия AVA_SOF.1 (Оценка стойкости функции безопасности ОО).

5.1 Требования безопасности для ОО

5.1.1 Функциональные требования безопасности ОО

Функция безопасности «Аутентификация» реализуется механизмом паролей. Этот механизм можно отнести к типу вероятностных и перестановочных механизмов, для которых возможен анализ их стойкости. В качестве минимального уровня стойкости функции безопасности «Аутентификация» в настоящем ЗБ заявлена **«Средняя СФБ»**

Другие механизмы (некриптографические), реализуемые ФБО, нельзя отнести к вероятностным и перестановочным механизмам, поэтому заявлений об их стойкости в настоящем ЗБ не делается.

Функциональные компоненты из части 2 ОК, на которых основаны функциональные требования безопасности ОО, приведены в таблице 5.1.

Таблица 5.1 – Функциональные компоненты, на которых основаны ФТБ ОО

Идентификатор компонента требований	Название компонента требований
FAU_GEN.1	Генерация данных аудита
FAU_GEN.2	Ассоциация идентификатора пользователя
FAU_SAR.1	Просмотр аудита
FAU_SAR.2	Ограниченный просмотр аудита
FAU_SAR.3	Выборочный просмотр аудита
FAU_SEL.1	Избирательный аудит
FAU_STG.1	Защищенное хранение журнала аудита
FAU_STG.3	Действия в случае возможной потери данных аудита

Идентификатор компонента требований	Название компонента требований
FAU_STG.4	Предотвращение потери данных аудита
FDP_ACC.1	Ограниченное управление доступом
FDP_ACF.1	Управление доступом, основанное на атрибутах безопасности
FIA_AFL.1	Обработка отказов аутентификации
FIA_ATD.1	Определение атрибутов пользователя
FIA_UAU.2	Аутентификация до любых действий пользователя
FIA_UID.2	Идентификация до любых действий пользователя
FIA_USB.1	Связывание пользователь-субъект
FMT_MOF.1	Управление режимом выполнения функций безопасности
FMT_MSA.1	Управление атрибутами безопасности
FMT_MSA.3	Инициализация статических атрибутов
FMT_MTD.1	Управление данными ФБО
FMT_REV.1	Отмена
FMT_SMR.1	Роли безопасности
FPT_RVM.1	Невозможность обхода ПБО
FPT_SEP.1	Отделение домена ФБО
FRU_RSA.2	Минимальные и максимальные квоты
FTA_TSE.1	Открытие сеанса с ОО

5.1.1.1 Аудит безопасности (FAU)

FAU_GEN.1 Генерация данных аудита

FAU_GEN.1.1 ФБО должны быть способны генерировать запись аудита для следующих событий, потенциально подвергаемых аудиту:

а) запуск и завершение выполнения функций аудита;

б) все события, потенциально подвергаемые аудиту, на *неопределенном* уровне аудита;

в) **(события, приведенные во втором столбце таблицы 5.2)**.

FAU_GEN.1.2 ФБО должны регистрировать в каждой записи аудита, по меньшей мере, следующую информацию:

а) дата и время события, тип события, идентификатор субъекта и результат события (успешный или неуспешный);

б) для каждого типа событий, потенциально подвергаемых аудиту, из числа определенных в функциональных компонентах, которые включены в ЗБ, [информацию, определенную в третьем столбце таблицы 5.2].

Зависимости: FPT_STM.1 «Надежные метки времени».

Таблица 5.2 – События, подлежащие аудиту

Компонент	Событие	Детализация
FAU_GEN.1	Запуск и завершение выполнения функций аудита	
FAU_SEL.1	Все модификации конфигурации аудита, происходящие во время сбора данных аудита	
FAU_STG.3	Предпринимаемые действия после превышения порога заполнения журнала аудита	
FAU_STG.4	Факт останова ОО при отсутствии свободного дискового пространства для создания журнала аудита	
FDP_ACF.1	Все запросы на выполнение операций на именованном объекте, на который распространяется политика дискреционного управления доступом	Идентификатор объекта
FIA_AFL.1 (1)	Достижение ограничения неуспешных попыток аутентификации и предпринятые действия	
FIA_UAU.2 (1)	Все случаи использования механизма аутентификации субъектов доступа	
FIA_UID.2	Все случаи использования механизма идентификации субъектов доступа	
FIA_USB.1	Факт создания регистрационной и	

Компонент	Событие	Детализация
	учетной записи пользователя	
FMT_MOF.1	Все модификации режима выполнения аудита и режима аутентификации	
FMT_MSA.1	Все модификации значений атрибутов безопасности, используемых в политике дискреционного управления доступом	
FMT_MSA.3	Модификации настройки по умолчанию ограничительных правил, все модификации начальных значений атрибутов безопасности, которые используются для политики дискреционного управления доступом	
FMT_MTD.1	Все модификации значений данных ФБО	
FMT_REV.1 (1)	Все попытки отмены полномочий у пользователей ОО на доступ к объектам, отмены прав доступа к объекту (модификация списка дискреционного доступа)	
FMT_REV.1 (2)	Все попытки отмены прав доступа к объекту (модификация списка дискреционного доступа)	
FMT_SMR.1	Модификация множества администраторов ОО и пользователей ОО	
FTA_TSE.1	Все попытки открытия сеанса доступа к ОО со стороны субъектов	
FRU_RSA.2 (1)	Установление и модификация объема физической памяти, доступного для ОО	
FRU_RSA.2 (2)	Установление и модификация объема дискового пространства для баз данных	

FAU_GEN.2 Ассоциация идентификатора пользователя

FAU_GEN.2.1 ФБО должны быть способны ассоциировать каждое событие, потенциально подвергаемое аудиту, с идентификатором **учетной записи** пользователя **или идентификатором регистрационной записи пользователя**, который был инициатором этого события.

Зависимости: FAU_GEN.1 «Генерация данных аудита»,
FIA_UID.2 «Идентификация до любых действий пользователя».

FAU_SAR.1 Просмотр аудита

FAU_SAR.1.1 ФБО должны предоставлять [уполномоченному администратору ОО] возможность читать [всю информацию аудита] из записей аудита.

FAU_SAR.1.2 ФБО должны предоставлять записи аудита в виде, позволяющем **уполномоченному администратору ОО** воспринимать содержащуюся в них информацию.

Зависимости: FAU_GEN.1 «Генерация данных аудита».

FAU_SAR.2 Ограниченный просмотр аудита

FAU_SAR.2.1 ФБО должны запретить всем пользователям доступ к чтению записей аудита, за исключением **уполномоченных администраторов ОО**, которым явно предоставлен доступ для чтения.

Зависимости: FAU_SAR.1 «Просмотр аудита».

FAU_SAR.3 Выборочный просмотр аудита

FAU_SAR.3.1 ФБО должны **предоставить** возможность выполнить *поиск* данных аудита, основанный на

[

следующих критериях в логическом отношении «И»:

а) наименование поля данных;

б) значение поля данных

].

Зависимости: FAU_SAR.1 «Просмотр аудита».

FAU_SEL.1 Избирательный аудит

FAU_SEL.1.1 ФБО должны быть способны к включению событий, потенциально подвергаемых аудиту, в совокупность событий, подвергающихся аудиту, или к их исключению из этой совокупности по следующим атрибутам:

а) ***категория*** *события*;

[

б) класс события;

в) поле данных

].

Зависимости: FAU_GEN.1 «Генерация данных аудита»,
FMT_MTD.1 «Управление данными ФБО».

FAU_STG.1 Защищенное хранение журнала аудита

FAU_STG.1.1 ФБО должны защищать хранимые записи аудита от несанкционированного удаления.

FAU_STG.1.2 ФБО должны быть способны к *предотвращению* модификации записей аудита.

Зависимости: FAU_GEN.1 «Генерация данных аудита».

FAU_STG.3 Действия в случае возможной потери данных аудита

FAU_STG.3.1 ФБО должны выполнить [создание нового журнала аудита], если журнал аудита **превысит** [установленный уполномоченным администратором ОО размер].

Зависимости: FAU_STG.1 «Защищенное хранение журнала аудита».

FAU_STG.4 Предотвращение потери данных аудита

FAU_STG.4.1 ФБО должны выполнить *игнорирование событий, подвергающихся аудиту* и [останов ОО] при **отсутствии свободного дискового пространства для создания журнала аудита**.

Зависимости: FAU_STG.1 «Защищенное хранение журнала аудита».

5.1.1.2 Защита данных пользователя (FDP)

FDP_ACC.1 Ограниченное управление доступом

FDP_ACC.1.1 ФБО должны осуществлять [политику дискреционного управления доступом] для

[

а) субъектов – процессов, действующих от имени пользователей;

б) именованных объектов:

1) на уровне сервера БД – конечная точка (Endpoint), регистрационная запись (Login), база данных (Database);

2) на уровне БД – схема (Schema), пользователь (Database User), контракт (Contract), роль (Role), роль приложения (Application Role), сборка (assemblies), типы сообщений (Message Types), привязки удаленных служб (Remote Service Binding), маршрут (Route), служба (Service), полнотекстовый каталог (Full Text Catalog);

3) на уровне схемы – таблица (Table), столбец таблицы (Column), функция (Function), представление (Views), хранимая процедура (Stored Procedures), синоним (Synonym), очередь (Query), типы (Types), коллекция XML-схем (XML Schema Collection);

в) всех операций между субъектами и объектами

].

Зависимости: FDP_ACF.1 «Управление доступом, основанное на атрибутах безопасности».

FDP_ACF.1 Управление доступом, основанное на атрибутах безопасности

FDP_ACF.1.1 ФБО должны осуществлять [политику дискреционного управления доступом] к объектам, основываясь на

[

следующем:

а) ассоциированные с субъектом идентификатор учетной записи пользователя, принадлежность к роли (ролям), определяемой пользователем (user-defined database role);

б) следующие, ассоциированные с объектами, атрибуты управления доступом:

[

– владелец объекта;
– список дискреционного управления доступом, который сопоставлен с объектом доступа и содержит записи:
  – идентификатор учетной записи пользователя или роли, определяемой пользователем;
  – тип (разрешение или запрет);
  – право доступа к объекту;

]

].

FDP_ACF.1.2 ФБО должны реализовать следующие правила определения того, разрешена ли операция управляемого субъекта на управляемом объекте:

[

доступ к объекту разрешен, если, по крайней мере, выполняется одно из следующих условий:

а) субъект является владельцем объекта;
б) запись, содержащаяся в списке дискреционного управления доступом, явно разрешает доступ субъекту, и доступ не был явно запрещен записью, содержащейся в списке дискреционного управления доступом;
в) запись, содержащаяся в списке дискреционного управления доступом, явно разрешает доступ роли, участником которой является субъект, и доступ не был явно запрещен записью, содержащейся в списке дискреционного управления доступом;

в случае если доступ к объекту не разрешен правилами, изложенными в FDP_ACF.1.3, то доступ субъекта к объекту запрещен

].

FDP_ACF.1.3 ФБО должны явно разрешать доступ субъектов к объектам, основываясь на следующих дополнительных правилах:

[

а) уполномоченному администратору ОО предоставлен доступ к объектам ОО вне зависимости от списков дискреционного управления доступом

б) полномочия администратора ОО на доступ к объекту определяются участием в предопределенных ролях сервера БД (server role) и (или) фиксированных ролях БД (fixed database role), предполагающих возможность доступа к объектам вне зависимости от списков дискреционного управления доступом

].

FDP_ACF.1.4 ФБО должны явно отказывать в доступе субъектов к объектам, основываясь на следующих дополнительных правилах:

[

в доступе к объекту явно отказано, если выполняется, по крайней мере, одно из следующих условий:

а) запись в списке дискреционного управления доступом явно запрещает доступ для субъекта;

б) запись в списке дискреционного управления доступом явно запрещает доступ роли, участником которой является субъект

].

Зависимости: FDP_ACC.1 «Ограниченное управление доступом»,
FMT_MSA.3 «Инициализация статических атрибутов».

5.1.1.3 Идентификация и аутентификация (FIA)

FIA_AFL.1 (1) Обработка отказов аутентификации

FIA_AFL.1.1 ФБО должны обнаруживать, когда произойдет [установленное администратором ОО число (не более 10)] неуспешных попыток аутентификации [с момента последней успешной попытки аутентификации пользователя].

FIA_AFL.1.2 При **достижении** определенного **в элементе FIA_AFL.1.1** числа неуспешных попыток аутентификации ФБО должны**:**

[

а) сделать невозможным доступ субъекта доступа к ОО, осуществив блокировку регистрационной записи;

б) осуществить сброс счетчика неуспешных попыток аутентификации по команде уполномоченного администратора ОО

].

Зависимости: FIA_UAU.2 (1) «Аутентификация до любых действий пользователя».

FIA_ATD.1 Определение атрибутов пользователя

FIA_ATD.1.1 ФБО должны поддерживать для каждого пользователя следующий список атрибутов безопасности:

[

а) идентификатор регистрационной записи пользователя;

б) идентификатор роли, участником которой является пользователь;

в) идентификатор учетной записи пользователя

].

Зависимости: отсутствуют.

FIA_UAU.2 (1) Аутентификация до любых действий пользователя

FIA_UAU.2.1 ФБО должны требовать, чтобы каждый **субъект доступа к ОО и объектам ОО** был успешно аутентифицирован до разрешения любого действия, выполняемого при посредничестве ФБО от имени этого **субъекта доступа**.

Зависимости: FIA_UID.2 «Идентификация до любых действий пользователя».

FIA_UID.2 Идентификация до любых действий пользователя

FIA_UID.2.1 ФБО должны требовать, чтобы каждый **субъект доступа к ОО и объектам ОО** был успешно идентифицирован до разрешения любого действия, выполняемого при посредничестве ФБО от имени этого **субъекта доступа**.

Зависимости: отсутствуют.

FIA_USB.1 Связывание пользователь-субъект

FIA_USB.1.1 ФБО должны ассоциировать соответствующие атрибуты безопасности **субъекта доступа** с субъектами, действующими от имени этого **субъекта доступа**.

Зависимости: FIA_ATD.1 «Определение атрибутов пользователя».

5.1.1.4 Управление безопасностью (FMT)

FMT_MOF.1 Управление режимом выполнения функций безопасности

FMT_MOF.1.1 ФБО должны **предоставлять** возможность *определять режим выполнения, модифицировать режим выполнения* функций**, связанных с:**

[

а) аудитом;

б) аутентификацией субъектов доступа

]

только [уполномоченному администратору ОО].

Зависимости: FMT_SMR.1 «Роли безопасности».

FMT_MSA.1 Управление атрибутами безопасности

FMT_MSA.1.1 ФБО должны осуществлять [политику дискреционного управления доступом], **предоставляющую** возможность *модифицировать* атрибуты безопасности, [перечисленные в элементе FDP_ACF.1.1 компонента FDP_ACF.1], только [уполномоченному администратору ОО и пользователю ОО, являющемуся владельцем объекта].

Зависимости: FDP_ACC.1 «Ограниченное управление доступом»,
FMT_SMR.1 «Роли безопасности».

FMT_MSA.3 Инициализация статических атрибутов

FMT_MSA.3.1 ФБО должны осуществлять [политику дискреционного управления доступом], **предусматривающую** *ограничительные* значения по умолчанию для атрибутов безопасности, которые используются для осуществления **политики дискреционного управления доступом**.

FMT_MSA.3.2 ФБО должны позволять [уполномоченному администратору ОО и пользователю ОО, являющемуся владельцем объекта] определять альтернативные начальные значения для отмены значений по умолчанию при создании объекта.

Зависимости: FMT_MSA.1 «Управление атрибутами безопасности»,
FMT_SMR.1 «Роли безопасности».

FMT_MTD.1 Управление данными ФБО

FMT_MTD.1.1 ФБО должны **предоставлять** возможность [*выполнения операций, указанных во втором столбце таблицы 5.3*] над данными, [указанными в третьем столбце таблицы 5.3] только [уполномоченному администратору ОО].

Зависимости: FMT_SMR.1 «Роли безопасности».

Таблица 5.3 – Управляемые данные ФБО

Компонент	Операция	Данные ФБО
FAU_SAR.1	удаление, модификация, добавление	состав администраторов ОО, являющихся участниками ролей, предусматривающих чтение записей аудита
FAU_STG.3	установление, модификация	размер журнала аудита
FIA_UID.2	создание, модификация, удаление	идентификационная информация регистрационной записи пользователя, идентификационная информация учетной записи пользователя
FMT_MOF.1	удаление, модификация, добавление	состав администраторов ОО, являющихся участниками ролей, предусматривающих доступ к управлению режимами аудита и аутентификации
FMT_MSA.1	удаление, модификация, добавление	состав администраторов ОО, являющихся участниками ролей, предусматривающих модификацию атрибутов безопасности
FMT_MSA.3	удаление, модификация, добавление	состав администраторов ОО, являющихся участниками ролей, предусматривающих модификацию начальных значений атрибутов

Компонент	Операция	Данные ФБО
		безопасности
FMT_MTD.1	удаление, модификация, добавление	состав администраторов ОО, являющихся участниками ролей, предусматривающих модификацию данных ФБО, определенных в настоящей таблице
FMT_REV.1 (1)	удаление, модификация, добавление	состав администраторов ОО, являющихся участниками ролей, предусматривающих возможность отмены атрибутов безопасности, ассоциированных с пользователями и объектами
FMT_SMR.1	удаление, модификация, добавление	состав пользователей ОО, являющихся участниками ролей администратор ОО и пользователь ОО
FTA_TSE.1	установление, модификация	значение параметров, запрещающих установление сеанса с ОО (идентификатор регистрационной записи пользователя, предельное количество одновременно открытых сеансов доступа к ОО)
FRU_RSA.2 (1)	установление, модификация	объем физической памяти, который ОО может использовать в процессе функционирования
FRU_RSA.2 (2)	установление, модификация	объем дискового пространства, который базы данных могут использовать одновременно

FMT_REV.1 (1) Отмена

FMT_REV.1.1 ФБО должны предоставлять возможность отмены атрибутов безопасности, ассоциированных с ***пользователями ОО и объектами***, в пределах ОДФ только [уполномоченному администратору ОО].

FMT_REV.1.2 ФБО должны осуществлять **следующие** правила:

[

а) отмена полномочий у пользователей ОО на доступ к объектам должна вступать в силу при следующем сеансе работы пользователя ОО;

б) отмена прав доступа к объекту (модификация списка дискреционного доступа) должна происходить немедленно и вступать в силу до любых попыток доступа к объекту, следующих за отменой прав доступа;

].

Зависимости: FMT_SMR.1 «Роли безопасности».

FMT_REV.1 (2) Отмена

FMT_REV.1.1 ФБО должны предоставлять возможность отмены атрибутов безопасности, ассоциированных с ***объектами***, в пределах ОДФ только [пользователю ОО, являющемуся владельцем объекта].

FMT_REV.1.2 ФБО должны осуществлять **следующие** правила:

[

а) отмена прав доступа к объекту (модификация списка дискреционного доступа) должна происходить немедленно и вступать в силу до любых попыток доступа к объекту, следующих за отменой прав доступа;

].

Зависимости: FMT_SMR.1 «Роли безопасности».

FMT_SMR.1 Роли безопасности

FMT_SMR.1.1 ФБО должны поддерживать следующие роли**:**

[

а) администратор ОО;

б) пользователь ОО

].

FMT_SMR.1.2 ФБО должны быть способны ассоциировать **субъектов доступа** с ролями.

Зависимости: FIA_UID.2 «Выбор момента идентификации».

5.1.1.5 Защита ФБО (FPT)

FPT_RVM.1 (1) Невозможность обхода ПБО

FPT_RVM.1.1 ФБО должны обеспечить, чтобы функции, осуществляющие ПБО, вызывались и успешно выполнялись прежде, чем разрешается выполнение любой другой функции в пределах ОДФ.

Зависимости: отсутствуют.

FPT_SEP.1 (1) Отделение домена ФБО

FPT_SEP.1.1 ФБО должны поддерживать домен безопасности для собственного выполнения, защищающий их от вмешательства и искажения недоверенными субъектами.

FPT_SEP.1.2 ФБО должны реализовать разделение между доменами безопасности субъектов в ОДФ.

Зависимости: отсутствуют.

5.1.1.6 Использование ресурсов (FRU)

FRU_RSA.2 (1) Минимальные и максимальные квоты

FRU_RSA.2.1 ФБО должны реализовать максимальные квоты [объема физической памяти], который ***ОО*** может использовать ***в процессе функционирования***.

FRU_RSA.2.2 ФБО должны обеспечить выделение минимального [объема физической памяти], который является доступными для ***ОО***, чтобы использовать ***в процессе функционирования.***

Зависимости: отсутствуют.

FRU_RSA.2 (2) Минимальные и максимальные квоты

FRU_RSA.2.1 ФБО должны реализовать максимальные квоты [объема дискового пространства], который ***базы данных*** могут использовать *одновременно*.

FRU_RSA.2.2 ФБО должны обеспечить выделение минимального [объема дискового пространства], который является доступными для ***баз данных***, чтобы использовать *одновременно.*

Зависимости: отсутствуют.

5.1.1.7 Доступ к ОО (FTA)

FTA_TSE.1 Открытие сеанса с ОО

FTA_TSE.1.1 ФБО должны быть способны отказать в открытии сеанса **доступа к ОО**, основываясь на

[

следующих атрибутах:

а) идентификатор регистрационной записи пользователя;

б) предельное количество одновременно открытых сеансов доступа к ОО

].

Зависимости: отсутствуют.

5.1.2 Требования доверия к безопасности ОО

Требования доверия к безопасности ОО взяты из части 3 ОК и образуют ОУД1, усиленный компонентом AVA_SOF.1 (Оценка стойкости функции безопасности ОО) (см. таблицу 5.4).

Таблица 5.4 – Требования доверия к безопасности ОО

Класс доверия	Идентификатор компонентов доверия	Название компонентов доверия
Управление конфигурацией	ACM_CAP.1	Номера версий
Поставка и эксплуатация	ADO_IGS.1	Процедуры установки, генерации и запуска
Разработка	ADV_FSP.1	Неформальная функциональная спецификация
	ADV_RCR.1	Неформальная демонстрация соответствия

Класс доверия	Идентификатор компонентов доверия	Название компонентов доверия
Руководства	AGD_ADM.1	Руководство администратора
	AGD_USR.1	Руководство пользователя
Тестирование	ATE_IND.1	Независимое тестирование на соответствие
Оценка уязвимостей	AVA_SOF.1	Оценка стойкости функции безопасности ОО

5.1.2.1 Управление конфигурацией (ACM)

ACM_CAP.1 Номера версий

ACM_CAP.1.1D Разработчик должен предоставить маркировку для ОО.

Элементы содержания и представления свидетельств

ACM_CAP.1.1C Маркировка ОО должна быть уникальна для каждой версии ОО.

ACM_CAP.1.2C ОО должен быть помечен маркировкой.

Элементы действий оценщика

ACM_CAP.1.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

5.1.2.2 Поставка и эксплуатация (ADO)

ADO_IGS.1 Процедуры установки, генерации и запуска

Элементы действий разработчика

ADO_IGS.1.1D Разработчик должен задокументировать процедуры, необходимые для безопасной установки, генерации и запуска ОО.

Элементы содержания и представления свидетельств

ADO_IGS.1.1C Документация должна содержать описание последовательности действий, необходимых для безопасной установки, генерации и запуска ОО.

Элементы действий оценщика

ADO_IGS.1.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

ADO_IGS.1.2E Оценщик должен сделать независимое заключение, что процедуры установки, генерации и запуска приводят к безопасной конфигурации.

5.1.2.3 Разработка (ADV)

ADV_FSP.1 Неформальная функциональная спецификация

Элементы действий разработчика

ADV_FSP.1.1D Разработчик должен представить функциональную спецификацию.

Элементы содержания и представления свидетельств

ADV_FSP.1.1C Функциональная спецификация должна содержать неформальное описание ФБО и их внешних интерфейсов.

ADV_FSP.1.2C Функциональная спецификация должна быть внутренне непротиворечивой.

ADV_FSP.1.3C Функциональная спецификация должна содержать описание назначения и методов использования всех внешних интерфейсов ФБО, обеспечивая, где это необходимо, детализацию результатов, нештатных ситуаций и сообщений об ошибках.

ADV_FSP.1.4C Функциональная спецификация должна полностью представить ФБО.

Элементы действий оценщика

ADV_FSP.1.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

ADV_FSP.1.2E Оценщик должен сделать независимое заключение, что функциональная спецификация – точное и полное отображение функциональных требований безопасности ОО.

ADV_RCR.1 Неформальная демонстрация соответствия

Элементы действий разработчика

ADV_RCR.1.1D Разработчик должен представить анализ соответствия между всеми смежными парами имеющихся представлений ФБО.

Элементы содержания и представления свидетельств

ADV_RCR.1.1C Для каждой смежной пары имеющихся представлений ФБО анализ должен демонстрировать, что все функциональные возможности более абстрактного представления ФБО, относящиеся к безопасности,

правильно и полностью уточнены в менее абстрактном представлении ФБО.

Элементы действий оценщика

ADV_RCR.1.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

5.1.2.4 Руководства (AGD)

AGD_ADM.1 Руководство администратора

Элементы действий разработчика

AGD_ADM.1.1D Разработчик должен представить руководство администратора, предназначенное для персонала системного администрирования.

Элементы содержания и представления свидетельств

AGD_ADM.1.1C Руководство администратора должно содержать описание функций администрирования и интерфейсов, доступных администратору ОО.

AGD_ADM.1.2C Руководство администратора должно содержать описание того, как управлять ОО безопасным способом.

AGD_ADM.1.3C Руководство администратора должно содержать предупреждения относительно функций и привилегий, которые следует контролировать в безопасной среде обработки информации.

AGD_ADM.1.4C Руководство администратора должно содержать описание всех предположений о поведении пользователя, которые связаны с безопасной эксплуатацией ОО.

AGD_ADM.1.5C Руководство администратора должно содержать описание всех параметров безопасности, контролируемых администратором, указывая, при необходимости, безопасные значения.

AGD_ADM.1.6C Руководство администратора должно содержать описание каждого типа относящихся к безопасности событий, связанных с выполнением обязательных функций администрирования, включая изменение характеристик безопасности сущностей, контролируемых ФБО.

AGD_ADM.1.7C Руководство администратора должно быть согласовано со всей другой документацией, представленной для оценки.

AGD_ADM.1.8C Руководство администратора должно содержать описание всех требований безопасности к среде ИТ, которые относятся к администратору.

Элементы действий оценщика

AGD_ADM.1.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

AGD_USR.1 Руководство пользователя

Элементы действий разработчика

AGD_USR.1.1D Разработчик должен представить руководство пользователя.

Элементы содержания и представления свидетельств

AGD_USR.1.1C Руководство пользователя должно содержать описание функций и интерфейсов, которые доступны пользователям ОО, не связанным с администрированием.

AGD_USR.1.2C Руководство пользователя должно содержать описание применения доступных пользователям функций безопасности, предоставляемых ОО.

AGD_USR.1.3C Руководство пользователя должно содержать предупреждения относительно доступных для пользователей функций и привилегий, которые следует контролировать в безопасной среде обработки информации.

AGD_USR.1.4C Руководство пользователя должно четко представить все обязанности пользователя, необходимые для безопасной эксплуатации ОО, включая обязанности, связанные с предположениями относительно действий пользователя, содержащимися в изложении среды безопасности ОО.

AGD_USR.1.5C Руководство пользователя должно быть согласовано со всей другой документацией, представленной для оценки.

AGD_USR.1.6C Руководство пользователя должно содержать описание всех требований безопасности к среде ИТ, которые имеют отношение к пользователю.

Элементы действий оценщика

AGD_USR.1.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

5.1.2.5 Тестирование (ATE)

ATE_IND.1 Независимое тестирование на соответствие

Элементы действий разработчика

ATE_IND.1.1D Разработчик должен представить ОО для тестирования.

Элементы содержания и представления свидетельств

ATE_IND.1.1C ОО должен быть пригоден для тестирования.

Элементы действий оценщика

ATE_IND.1.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

ATE_IND.1.2E Оценщик должен протестировать необходимое подмножество ФБО, чтобы подтвердить, что ОО функционирует в соответствии со спецификациями.

5.1.2.6 Оценка уязвимостей (AVA)

AVA_SOF.1 Оценка стойкости функции безопасности ОО

Элементы действий разработчика

AVA_SOF.1.1D Разработчик должен выполнить анализ стойкости функции безопасности ОО для каждого механизма, идентифицированного в ЗБ как имеющего утверждение относительно стойкости функции безопасности ОО.

Элементы содержания и представления свидетельств

AVA_SOF.1.1C Для каждого механизма, имеющего утверждение относительно стойкости функции безопасности ОО, анализ должен показать, что ее стойкость достигает или превышает минимальный уровень стойкости, определенный в ПЗ/ЗБ.

AVA_SOF.1.2C Для каждого механизма, имеющего утверждение относительно конкретной стойкости функции безопасности ОО, анализ должен показать, что ее стойкость достигает или превышает конкретный показатель, определенный в ПЗ/ЗБ.

Элементы действий оценщика

AVA_SOF.1.1E Оценщик должен подтвердить, что представленная информация удовлетворяет всем требованиям к содержанию и представлению свидетельств.

AVA_SOF.1.2E Оценщик должен подтвердить, что утверждения относительно стойкости корректны.

5.2 Требования безопасности для среды ИТ

Функцией безопасности, реализуемой средой ИТ (операционной системой) в интересах обеспечения безопасности ОО, является функция безопасности «Аутентификация». Данная функция реализуется механизмом паролей среды ИТ (операционной системы). Этот механизм можно отнести к типу вероятностных и перестановочных механизмов, для которых возможен анализ их стойкости. В качестве минимального уровня стойкости функции безопасности «Аутентификация» в настоящем ЗБ заявлена **«Средняя СФБ»**

Другие механизмы (некриптографические), реализуемые средой ИТ в интересах обеспечения безопасности ОО, нельзя отнести к вероятностным и перестановочным механизмам, поэтому заявлений об их стойкости в настоящем ЗБ не делается.

Функциональные компоненты из части 2 ОК, на которых основаны функциональные требования безопасности среды ИТ, приведены в таблице 5.5.

Таблица 5.5 – Функциональные компоненты, на которых основаны ФТБ среды ИТ

Идентификатор компонента требований	Название компонента требований
FIA_AFL.1	Обработка отказов аутентификации
FIA_SOS.1	Верификация секретов
FIA_UAU.2	Аутентификация до любых действий пользователя
FPT_RVM.1	Невозможность обхода ПБО
FPT_SEP.1	Отделение домена ФБО
FPT_STM.1	Надежные метки времени

5.2.1 Идентификация и аутентификация (FIA)

FIA_AFL.1 (2) Обработка отказов аутентификации

FIA_AFL.1.1 **Функции безопасности среды ИТ** должны обнаруживать, когда произойдет [установленное администратором ОС число (не более 10)] неуспешных попыток аутентификации [с момента последней успешной попытки аутентификации пользователя].

FIA_AFL.1.2 При **достижении** определенного **в элементе FIA_AFL.1.1** числа неуспешных попыток аутентификации **функции безопасности среды ИТ** должны**:**

[

а) сделать невозможным доступ субъекта доступа к ОО, осуществив блокировку регистрационной записи на 30 минут;

б) по истечении 30 минут осуществить сброс счетчика неуспешных попыток аутентификации

].

Зависимости: FIA_UAU.2 (2) «Аутентификация до любых действий пользователя».

FIA_SOS.1 Верификация секретов

FIA_SOS.1.1 **Функции безопасности среды ИТ** должны предоставить механизм для верификации того, что **пароли на доступ к ОО** отвечают **следующей метрики качества**

[

а) минимальная длина – 6 символов;

б) пароль не может содержать имя учетной записи пользователя или какую-либо его часть;

в) в пароле должны присутствовать символы как минимум трех категорий из числа следующих:

– прописные буквы английского алфавита от A до Z;

– строчные буквы английского алфавита от a до z;

– десятичные цифры от 0 до 9;

– символы, не принадлежащие алфавитно-цифровому набору;

].

Зависимости: отсутствуют.

FIA_UAU.2 (2) Аутентификация до любых действий пользователя

FIA_UAU.2.1 **Функции безопасности среды ИТ** должны требовать, чтобы каждый **субъект доступа к ОО и объектам ОО** был успешно аутентифицирован до разрешения любого действия, выполняемого при посредничестве ФБО от имени этого **субъекта доступа**.

Зависимости: FIA_UID.2 «Идентификация до любых действий пользователя».

5.2.2 Защита ФБО (FPT)

FPT_RVM.1 (2) Невозможность обхода ПБО

FPT_RVM.1.1 **Функции безопасности среды ИТ** должны обеспечить, чтобы функции, осуществляющие ПБО, вызывались и успешно выполнялись прежде, чем разрешается выполнение любой другой функции в пределах ОДФ.

Зависимости: отсутствуют.

FPT_SEP.1 (2) Отделение домена ФБО

FPT_SEP.1.1 **Функции безопасности среды ИТ** должны поддерживать домен безопасности для выполнения **ФБО**, защищающий их от вмешательства и искажения недоверенными субъектами.

FPT_SEP.1.2 **Функции безопасности среды ИТ** должны реализовать разделение между доменами безопасности субъектов в ОДФ.

Зависимости: отсутствуют.

FPT_STM.1 Надежные метки времени

FPT_STM.1.1 **Функции безопасности среды ИТ** должны быть способны предоставить надежные метки времени для **использования ФБО**.

Зависимости: отсутствуют.

6 Краткая спецификация ОО

В данном подразделе представлено описание функций безопасности ОО и мер доверия к безопасности ОО, а также – их сопоставление с требованиями безопасности для ОО.

6.1 Функции безопасности ОО

ОО реализует следующие функции безопасности:

- аудит безопасности;
- защиту данных пользователя;
- идентификацию и аутентификацию;
- управление безопасностью;
- защиту ФБО;
- управление доступом к ОО;
- использование ресурсов ОО.

6.1.1 Функции безопасности «Аудит безопасности»

Функции безопасности ОО «Аудит безопасности» обеспечивают:

- сбор данных аудита;
- просмотр журнала регистрации событий аудита (журнала аудита);
- защиту журнала аудита от переполнения;
- ограничение доступа к журналу аудита.

6.1.1.1 Сбор данных аудита

Объект оценки обеспечивает поддержку двух способов аудита, позволяющих отслеживать и регистрировать относящиеся к безопасности события аудита.

Первый способ предполагает использование механизмов аудита, реализуемых средствами операционной системы Microsoft® Windows Server 2003™, под управлением которой функционирует ОО. При использовании данного способа аудита в журнал регистрации событий аудита, в качестве которого выступает журнал «Приложение» (Application Log) ОС Microsoft® Windows Server 2003™, заносятся все события аудита, относящиеся к процессу регистрации пользователя при доступе к ОО, старта/останова различных служб ОО и выполнения системных хранимых процедур, управляющих

различными параметрами настройки ОО. В то же время, в журнал регистрации событий аудита (журнал «Приложение») не заносятся события, связанные с вызовом относящихся к безопасности системных хранимых процедур, созданием и удалением объектов БД, с назначением и проверкой прав доступа к ним, события, идентифицирующие выполняемые субъектом доступа действия непосредственно в самой БД, и другие критичные с точки зрения безопасности события аудита.

За создание журнала «Приложение» отвечает локальная служба «Регистратор событий» (Event Logger) операционной системы Microsoft® Windows Server 2003™, под управлением которой функционирует ОО.

При использовании второго способа для обеспечения регистрации различных категорий событий в ОО задействуются собственные функции аудита, в том числе позволяющих отслеживать и регистрировать все события аудита, относящиеся к безопасности. При использовании данного механизма аудита ФБО осуществляют регистрацию всего спектра событий аудита для всех субъектов доступа, осуществляющих взаимодействие с ОО. При этом уполномоченный администратор получает всю полноту сведений относительно успешных и неуспешных попыток входа в систему, использования разрешений доступа к объектам и разрешений на выполнения инструкций языка DDL (Transact-SQL), добавления/удаления участника из состава фиксированной роли БД или предопределенной роли сервера БД и т.д. Данный уровень аудита интерпретируется системой как «режим аудита C2» (C2 audit mode).

События аудита, регистрируемые ОО, объединены в категории (наборы), в каждой из которых имеются собственные классы событий для сбора сведений о конкретных событиях ОО (любые операции, генерируемые ядром ОО). Для мониторинга и регистрации доступны следующие категории событий аудита (см. таблицу 6.1).

Таблица 6.1 – Категории событий, доступные для мониторинга

№ п/п	Категория событий	Описание	Назначение
1	Broker	В состав данной категории входят классы событий, созданные с помощью компонента Service Broker.	Мониторинг событий, формируемых при использовании компонента Service Broker.

№ п/п	Категория событий	Описание	Назначение
2	Cursors	К данной категории относятся классы событий, создаваемые с использованием операций курсора.	Мониторинг операций использования курсоров.
3	Среда CRL	К данной категории относятся классы событий, созданные путем выполнения объектов среды .NET CLR.	Мониторинг событий, возникающих при выполнении объектов среды CLR .NET в ОО.
4	База данных (Database)	К данной категории относятся события, создаваемые при автоматическом увеличении и уменьшении размеров файлов данных и файлов журналов транзакций.	Мониторинг автоматического увеличения размеров файлов данных и файлов журналов транзакций, позволяющий определить их подходящий размер и достичь максимальной производительности.
5	Ошибки и предупреждения (Errors and Warnings)	Ошибки и предупреждения.	Мониторинг очередей ожидания доступа к ресурсу. Данный класс событий позволяет оценить эффективность планов выполнения, сгенерированных оптимизатором запросов.
6	Полнотекстный поиск (Full Text)	К данной категории событий относятся классы событий, созданные при запуске, прерывании или остановке полнотекстного поиска.	Мониторинг событий, формируемых при выполнении операций полнотекстного поиска.
7	Блокировки (Locks)	К данной категории событий относятся классы событий, созданные при наложении, отмене, повышение уровня и	Мониторинг конфликтов на основании типов и длительности блокировок. Класс также применяется для мониторинга взаимо-

№ п/п	Категория событий	Описание	Назначение
		снятие блокировки, а также при других действиях с блокировкой.	блокировок и событий, связанных с истечением срока удержания блокировки.
8	Objects	К данной категории относятся классы событий, созданные при создании, открытии, закрытии, очистке и удалении объектов баз данных.	Мониторинг произвольного создания объектов баз данных пользователями и приложениями.
9	OLE DB	К данной категории относятся классы событий, созданные с помощью вызовов OLE DB.	Мониторинг общих событий при обращении к поставщику OLE DB.
10	Performance	К данной категории относятся классы событий, созданные при выполнении операторов языка обработки данных DML SQL.	Мониторинг эффективности выполнения запросов и работы оптимизаторов запросов на основе перехвата дерева запросов, определения цены плана выполнения запроса, сбор статистики о выполнении запроса, мониторинг дерева плана запросов.
11	Progress Report	К данной категории событий относится класс событий Progress Report: Online Index Operation.	Мониторинг процесса выполнения оперативного построения индекса.
12	Scans	К данной категории событий относится класс событий, создаваемых при сканирование таблиц и индексов.	Мониторинг типов операций сканирования конкретного объекта.

№ п/п	Категория событий	Описание	Назначение
13	События аудита безопасности (Security Audit)	Аудит событий безопасности.	Мониторинг событий входа и выхода из системы, изменение параметров, разрешений безопасности и паролей, а также событий резервного копирования и восстановления, и т.д.
14	Server	Аудит основных событий сервера.	Мониторинг изменений объема используемой SQL Server памяти, событий закрытия файла трассировки во время отката, получения запроса на монтирование ленты.
15	Sessions	К данной категории относятся классы событий, создаваемые при подключении (отключении) клиента к (от) экземпляру SQL Server.	Мониторинг подключенных пользователей, активности БД, длительности каждого пользовательского подключения и нагрузки на процессор, генерируемая передаваемыми по подключению запросами.
16	Хранимые процедуры (Stored Procedures)	К данной категории относятся классы событий, создаваемые при выполнении хранимых процедур, включая число «промахов» и «попаданий» в кэш, порядок выполнения, время удаления из кэша и время повторной компиляции.	Мониторинг памяти, позволяющий определить достаточность ее объема. Класс также используется для наблюдения за случаями использования хранимых процедур приложениями.
17	Transactions	К данной категории относятся классы событий, создаваемые при выполнении	Мониторинг типов записей, заносимых в журналы приложениями. Класс также используется для на-

№ п/п	Категория событий	Описание	Назначение
		транзакций координатора распределенных транзакций Microsoft или при записи в журнал транзакций.	блюдения за подтверждениями, откатами и распределенными транзакциями.
18	TSQL	К данной категории событий относятся классы событий, создаваемые при выполнении инструкций языка Transact-SQL, передаваемых экземпляру SQL Server от клиента.	Сравнение точности результатов, полученных в ходе обычной работы и при тестировании приложения. Класс также используется для мониторинга длительно выполняющихся событий, включая сведения о пользователях, предавших соответствующие запросы.
19	User-Configurable	К данной категории событий относятся определяемые классы событий.	Отслеживание пользовательских событий, мониторинг которых с помощью системных событий других категорий невозможен.

При использовании «режима аудита C2» файлы журналов регистрации событий аудита (имя которых представлено в формате `audittrace_ГГГГММДДЧЧММСС.trc`, где ГГГГ – год, ММ – месяц, ДД – день, ЧЧ – часы, ММ – минуты, СС - секунды), автоматически располагаются в том же каталоге файловой системы, что и файлы данных БД. По умолчанию максимальный размер файлов журналов регистрации событий аудита ограничен 200 Мб. При превышении указанного размера ОО автоматически создаст новый файл журнала регистрации событий аудита, в который будет осуществляться дальнейшая запись событий аудита. В случае если регистрации событий аудита невозможна - по причине отсутствия доступного дискового пространства, достаточного для создания нового файла журнала регистрации событий аудита – ОО прекратит свою работу.

При инициализации «режима аудита C2» ОО задействует профиль, используемый по умолчанию (default profile). Данный профиль содержит параметры, определяющие

необходимость отслеживания и регистрации в журнале аудита всей совокупности событий аудита, включая выполнение хранимых процедур и операторов Transact-SQL, создание и удаление таблиц БД, попытки регистрации пользователей, изменения объема используемой памяти, выполнения транзакций, т.е. всех операций, генерируемых ядром ОО (SQL Server Database Engine). При использовании данного режима аудита отсутствует возможность регистрации только относящихся к безопасности событий аудита, что приводит к перенасыщению журналов регистрации событий аудита иной, не относящейся к обеспечению безопасности, информацией.

Для обеспечения выборочного аудита требуемых категорий событий аудита (в частности событий безопасности категории «Security Audit») в ОО реализован механизм трассировок (traces). В отличие от указанных выше режимов аудита при использовании трассировок исключается необходимость перезапуска служб ОО и мониторинга всех операций, генерируемых ядром ОО. Таким образом, использование механизма трассировок позволяет осуществлять регистрацию только относящихся к безопасности событий аудита, не приводя к перенасыщению журналов регистрации событий аудита иной информацией.

Определение параметров задания на трассировку требуемой категории событий аудита осуществляется как с использованием стандартных хранимых процедур ОО `sp_trace_create`, `sp_trace_setevent` и `sp_trace_setstatus`, так и с использованием утилиты SQL Server Profiler. При этом запись результатов трассировки может осуществляться либо в файл с расширением `*.trc`, расположенный на локальном жестком диске компьютера, либо в заданную таблицу указанной уполномоченным администратором ОО базы данных.

Категория событий аудита «Security Audit» (Аудит безопасности) включает предопределенный набор классов событий, позволяющих отслеживать весь спектр относящихся к безопасности событий, в том числе события создания и удаления пользователей БД, использования разрешений доступа к контролируемым объектам БД и разрешений на выполнение инструкций языка DDL (Transact-SQL), старта и останова служб ОО, события успешной и неуспешной регистрации пользователей при подключении к ОО и т.д.

В таблице 6.2 представлено описание всего множества классов событий безопасности для категории событий аудита «Security Audit» (Аудит безопасности).

Таблица 6.2 – Классы событий для категории событий «Security Audit»

№ п/п	Класс события	Назначение
1.	Audit Add DB User	Регистрация событий добавления или удаления из базы данных имени входа пользователя.
2.	Audit Add Login to Server Role	Регистрация событий добавления или удаления участника в/из состава предопределенной роли сервера посредством системных хранимых процедур `sp_addsrvrolemember` и `sp_dropsrvrolemember`.
3.	Audit Add Member to DB Role	Регистрация событий добавления и удаления участника в/из состава фиксированной роли БД или определяемой пользователем роли БД (user-define role) посредством системных хранимых процедур `sp_addrolemember`, `sp_droprolemember` и `sp_changegroup`.
4.	Audit Add Role	Регистрация событий создания и удаления определяемой пользователем роли БД посредством системных хранимых процедур `sp_addrole` и `sp_droprole`.
5.	Audit Addlogin	Регистрация событий создания и удаления регистрационной записи (имени входа) пользователя посредством системных хранимых процедур `sp_addlogin` и `sp_droplogin`.
6.	Audit App Role Change Password	Регистрация событий смены пароля роли приложения (application role).
7.	Audit Backup/Restore	Регистрации событий резервного копирования и восстановления данных (при использовании инструкций BACKUP и RESTORE).
8.	Audit Broker Conversation	Регистрация событий аудита, относящихся к безопасности диалога компонента Service Broker.
9.	Audit Broker Login	Регистрация событий, относящихся к транспортной безопасности компонента Service Broker.

№ п/п	Класс события	Назначение
10.	Audit Change Audit	Регистрация изменений, вносимых в трассировку событий аудита.
11.	Audit Change Database Owner	Регистрация событий проверки разрешений на изменение владельца БД.
12.	Audit Database Management	Регистрация событий создания, изменения или удаления БД.
13.	Audit Database Mirroring Login	Регистрация событий аудита, относящихся к транспортной безопасности зеркального отображения базы данных.
14.	Audit Database Object Access	Регистрация событий аудита доступа к объекту базы данных.
15.	Audit Database Object GDR	Регистрация событий предоставления полномочий доступа к объекту БД с использованием инструкций GRANT, REVOKE или DENY.
16.	Audit Database Object Management	Регистрация событий выполнения инструкций CREATE, ALTER или DROP в отношении объекта БД.
17.	Audit Database Object Take Ownership	Регистрация события изменения владельца объекта, расположенного в БД.
18.	Audit Database Operation	Событие, указывающее, что выполнена одна из операций, таких как уведомление запроса контрольной точки или подписки.
19.	Audit Database Principal Impersonation	Регистрация событий, возникающих в случае использования механизма олицетворения в отношении субъекта доступа на уровне базы данных, например, с помощью инструкции EXECUTE AS <*пользователь*> или SETUSER.
20.	Audit Database Principal Management	Регистрация событий, возникающих в случае создания, удаления или изменения участников безопасности (principal) в БД.

№ п/п	Класс события	Назначение
21.	Audit Database Scope GDR	Регистрация событий выполнения пользователем БД инструкций GRANT, REVOKE или DENY.
22.	Audit DBCC	Регистрация исполнения консольных команд БД (DBCC).
23.	Audit Login	Регистрация событий подключения пользователей к ОО, начиная с момента старта трассировки (trace).
24.	Audit Login Change Password	Регистрация события изменения пользователем пароля, используемого для входа в SQL Server. В случае если пользователь является участником предопределенных ролей сервера БД «System Administrators» и «Security Administrators» и выполнил смену собственного пароля с использованием системной хранимой процедуры sp_password (с явным указанием параметров 'old_password', 'new_password', 'login') запись аудита будет отображать факт смены чужого, а не собственного пароля пользователя.
25.	Audit Login Change Property	Регистрация событий изменения параметров входа в систему, таких как подключаемая БД (с использованием системной хранимой процедуры `sp_defaultdb`) и используемый язык (с использованием системной хранимой процедуры `sp_defaultlanguage`), установленных по умолчанию для данной регистрационной записи пользователя.
26.	Audit Login Failed	Регистрация неуспешных попыток доступа к ОО.
27.	Audit Login GDR	Регистрация событий предоставления или отзыва для регистрационной записи пользователя разрешений на доступ к ОО (при использовании системных хранимых процедур `sp_grantlogin`, `sp_revokelogin` и `sp_denylogin`).

№ п/п	Класс события	Назначение
28.	Audit Logout	Регистрация событий отключения пользователей от ОО, начиная с момента старта трассировки.
29.	Audit Object Derived Permission	Регистрация событий выполнения инструкций CREATE, ALTER или DROP для конкретных объектов.
30.	Audit Schema Object Access	Регистрация событий использования разрешений на объект (например, SELECT).
31.	Audit Schema Object GDR	Регистрация событий выполнения пользователем инструкций GRANT, REVOKE или DENY по предоставлению разрешений для объекта схемы.
32.	Audit Schema Object Management	Регистрация событий создания, удаления или изменения объекта схемы.
33.	Audit Schema Object Take Ownership	Регистрация события выполнения проверки разрешений на изменение владельца объект схемы.
34.	Audit Server Alter Trace	Регистрация события проверки разрешения ALTER TRACE.
35.	Audit Server Object GDR	Регистрация события выполнения пользователем инструкций GRANT, REVOKE или DENY по предоставлению разрешений на объект сервера.
36.	Audit Server Object Management	Регистрация событий CREATE, ALTER или DROP в отношении объекта сервера.
37.	Audit Server Object Take Ownership	Регистрация событий изменения владельца объекта сервера.
38.	Audit Server Operation	Регистрация событий, указывающих, что на сервере выполнены операции аудита безопасности (такие как, настройка параметров, доступ к ресурсам, авторизации и т.д.).
39.	Audit Server Principal Impersonation	Регистрация событий, возникающих в случае использования механизма олицетворения в отношении субъекта доступа уровня сервера БД, например, с помо-

№ п/п	Класс события	Назначение
		щью инструкции EXECUTE AS <*Login*>.
40.	Audit Server Principal Management	Регистрация событий создания, изменение или удаления участника безопасности (principal) уровня сервера.
41.	Audit Server Scope GDR	Регистрация событий при использовании инструкций GRANT, REVOKE или DENY для задания разрешений на уровне сервера, например, при создании имени входа.
42.	Audit Server Starts and Stops	Регистрация событий старта и останова (паузы) службы SQL Server .
43.	Audit Statement Permission	Регистрация событий аудита (успешных и неуспешных), связанных с использованием разрешений на выполнение инструкций языка DDL (Transact-SQL).

Для каждого класса событий безопасности категории событий аудита «Security Audit» (Аудит безопасности) ФБО обеспечивают сбор определенных сведений, описывающих данное событие, включая имя компьютера, объект доступа, имя пользователя, текст запроса на языке Transact-SQL или хранимой процедуры, время начала и завершения события, а также ряд иных дополнительных сведений. При этом каждый класс событий безопасности категории «Security Audit» описывается собственным набором атрибутов (полями данных), содержащим сведения, однозначно характеризующими данное событие.

Таким образом, использование механизма трассировок позволяет отслеживать только критичные с точки зрения безопасности события аудита, связанные с выполнением определенных действий или доступом к определенным объектам непосредственно в БД. Единственным исключением из данного правила является невозможность трассировки исполнения системных хранимых процедур для администрирования учетных записей `sp_addapprole`, `sp_password`, `sp_addlogin` и `sp_addlinkedsrvlogin`.

6.1.1.2 Просмотр журналов аудита

Инструментальное средство ОС Microsoft® Windows Server 2003™ «Просмотр событий» (Event Viewer) предоставляет пользовательский интерфейс для просмотра содержимого журнала «Приложение», а также возможность поиска и фильтрации конкретных событий аудита. Для журнала «Приложение» в качестве параметров фильтрации и поиска событий могут быть заданы: источник события, категория события, код события, временной интервал, за который необходимо просмотреть события, и имя компьютера. В качестве критерия поиска может также выступать имя пользователя, осуществившего попытку успешной или неудачной регистрации при доступе к ОО. При этом поиск должен осуществляться по полю «Описание».

Интерфейс для управления записями аудита при использовании «режима аудита C2» или механизма трассировок обеспечивается утилитой SQL Server Profiler, входящей в состав ОО. Полученная при использовании указанных режимов аудита информация может быть проанализирована с целью обеспечения безопасности данных.

С использованием утилиты SQL Server Profiler уполномоченному администратору предоставляется возможность мониторинга и регистрации только тех событий аудита, которые удовлетворяют определенным критериям. С целью ограничения объема собираемых данных о событиях безопасности в ОО предусмотрено использование фильтров типа `LIKE`, `NOT LIKE`, `EQUALS`, `NOT EQUALS`, `GREATER THAN OR EQUAL` и `LESS THAN OR EQUAL`, применяемых к объектам контроля, таким как базы данных, пользователи, приложения и т.д. Каждый из указанных фильтров относится либо к строковым фильтрам (string filter), либо к числовым фильтрам (numeric filter). Таким образом, каждый элемент данных может быть отфильтрован только с использованием фильтра того или иного вида, т.е. если поле данных содержит строковые значения (например, поля данных `ApplicationName` или `DatabaseName`), к ним применимы исключительно строковые фильтры типа `LIKE` и `NOT LIKE` и наоборот, если поле данных содержит числовые значения (например, поля данных `DatabaseID` или `Duration`), к ним применимы только числовые фильтры типа `EQUALS`, `NOT EQUALS`, `GREATER THAN OR EQUAL` и `LESS THAN OR EQUAL`.

При анализе относящихся к безопасности событий аудита предусмотрена возможность использования механизма поиска событий. При этом поиск в журнале регистрации событий аудита (журналах трассировки) может осуществляться по полям

данных. В качестве критериев поиска могут выступать сведения, содержащиеся в полях данных, специфичных для каждого конкретного класса событий аудита.

6.1.1.3 Защита журнала аудита от переполнения

Объект оценки предотвращает потерю данных аудита посредством управления регистрацией и очередью событий аудита. ОО обеспечивает добавление данных аудита в журнал регистрации событий аудита до тех пор, пока он не станет полным. В случае если размер журнала регистраций событий аудита достигнет установленного для него порогового значения, ОО автоматически создаст новый файл журнала регистрации событий аудита, в который будет осуществляться дальнейшая запись событий аудита. По умолчанию максимальный размер файлов журналов регистрации событий аудита при использовании «режима аудита C2» ограничен 200 Мб.

Объект оценки обеспечивает защиту данных аудита от потери, используя возможность аварийного завершения работы при условии невозможности создания нового файла журнала регистрации событий аудита по причине отсутствия доступного дискового пространства, необходимого для его создания. Возобновление функционирования ОО возможно только после восстановления возможности ведения аудита. Завершение работы ОО в случае превышения файлом журнала регистрации событий аудита установленного размера обеспечивается только при использовании «режима аудита C2» и механизма трассировок. В случае аварийного завершения функционирования ОО в результате невозможности ведения аудита уполномоченный администратор может выполнить старт ОО в минимальной конфигурации в однопользовательском режиме.

При использовании режима минимальной конфигурации конфигурирование ОО может осуществляться только уполномоченным администратором с использованием системной хранимой процедуры `sp_configure`. В тоже время однопользовательский режим функционирования объекта оценки позволит предотвратить доступ к нему пользователей, за исключением уполномоченного администратора.

При использовании механизма трассировок уполномоченный администратор может самостоятельно определять параметры трассировки, в качестве которых могут выступать максимальный размер файла журнала регистрации событий аудита, поведение ФБО в случае достижения файлом журнала регистрации событий аудита своего максимального размера и поведение ОО в случае невозможности ведения аудита. Уполномоченный администратор может определить такое поведение ФБО, которое

предусматривает автоматическое создание нового файла журнала регистрации событий в случае превышения старым своего максимального размера. В тоже время потеря данных аудита может произойти в случае невозможности создания, по каким либо причинам, файла журнала регистрации событий аудита. ОО может быть настроен таким образом, чтобы обеспечить аварийное завершение работы при возникновения указанной ситуации.

6.1.1.4 Ограничение доступа к журналу аудита

Объект оценки обеспечивает защиту журналов регистрации событий аудита (результатов трассировки событий безопасности). Чтобы просмотреть содержимое журналов регистрации событий аудита, создаваемых при использовании «режима аудита C2» или механизма трассировок, пользователь должен быть определен в роли уполномоченного администратора, т.е. являться участником предопределенной фиксированной роли сервера «System administrators», либо для него должны быть явно определены разрешения файловой системы NTFS на доступ к файлу журнала регистрации событий аудита. В случае если запись результатов трассировки событий безопасности осуществляется в указанную уполномоченным администратором таблицу, их просмотр будет возможен только при наличии у пользователя соответствующих разрешений доступа к объекту (object permissions).

Для просмотра содержимого журнала «Приложение» пользователю не нужно обладать какими-либо дополнительными административными полномочиями.

Удаление содержимого журнала «Приложение» возможно только членами локальной группы безопасности операционной системы «Администраторы». Удаление содержимого таблицы, содержащей результаты регистрации событий аудита, либо самой таблицы возможно при условии наличия соответствующих разрешений на выполнение указанных операций в рамках содержащей данную таблицу БД.

Поскольку файл журнала регистрации событий аудита (результатов трассировки событий безопасности) расположен на дисковом разделе с файловой системой NTFS, доступ к нему разграничивается посредством использования разрешений NTFS. Таким образом, его удаление возможно только членами локальной группы безопасности операционной системы «Администраторы» либо пользователем при наличии у него разрешений, позволяющих выполнить указанные действия.

Инструментальное средство «Просмотр событий» (Event Viewer) предоставляет пользовательский интерфейс для просмотра содержимого журнала «Приложение».

Утилита «SQL Server Profiler» предоставляет пользовательский интерфейс для просмотра содержимого журналов регистрации событий аудита (результатов трассировки событий безопасности).

Сопоставление с ФТБ

Функции безопасности «Аудит безопасности» удовлетворяют следующим функциональным требованиям безопасности:

- FAU_GEN.1 – ОО обеспечивает генерацию данных аудита для всех категорий событий, представленных в таблице 6.1. Для каждого события аудита ФБО регистрируют дату, время, идентификатор учетной или регистрационной записи пользователя, идентификатор события, источник, тип и категорию события;
- FAU_GEN.2 – ФБО обеспечивают ассоциирование каждого события, потенциально подвергаемое аудиту, с идентификатором учетной записи пользователя или идентификатором регистрационной записи пользователя, который был инициатором этого события;
- FAU_SAR.1 – инструментальные средства просмотра событий предоставляют администратору ОО возможность просмотра данных аудита в удобочитаемом формате;
- FAU_SAR.2 – ФБО предоставляют доступ к чтению записей аудита только уполномоченным администраторам ОО;
- FAU_SAR.3 – инструментальные средство просмотра событий аудита предоставляют возможность выполнения поиска данных аудита по наименованию поля данных и значению поля данных;
- FAU_SEL.1 – ФБО предоставляют возможность включать события, потенциально подвергаемые аудиту, в совокупность событий, подвергающихся аудиту;
- FAU_STG.1 – ФБО защищают хранимые записи аудита от несанкционированного изменения и предотвращают их модификацию;
- FAU_STG.3 – ОО может быть настроен на создание нового журнала аудита в случае превышения данными аудита установленного для журнала аудита размера;

– FAU_STG.4 – ФБО выполняют останов ОО при отсутствии свободного дискового пространства для создания журнала аудита.

6.1.2 Функции безопасности «Защита данных пользователя»

К предоставляемым ОО механизмам обеспечения защиты данных пользователя относится дискреционное (избирательное) управление доступом.

Объект оценки обеспечивает опосредованный доступ между субъектами (участниками безопасности – security principals) и объектами доступа (БД, схемами и ее объектами). Субъекты доступа представлены набором процессов с одним или несколькими потоками, выполняющимися от имени пользователей. В таблице 6.3 представлен перечень стандартных защищаемых объектов (securable objects) ОО, на которые распространяется политика дискреционного управления доступом. При этом выделяются три объекта верхнего уровня, к которым относятся сервер БД, база данных и схема. Указанные объекты доступа образуют иерархии, вложенные одна в другую, каждая из которых содержит определенное множество других объектов. Данные иерархии объектов образуют области действия (scopes). Таким образом, основными областями действия в ОО являются сервер БД, база данных и схема.

Таблица 6.3 – Перечень объектов, на которые распространяется политика дискреционного управления доступом

Область действия	Тип объекта	Описание
Сервер БД	Конечная точка (Endpoint)	Точка коммуникации между ОО и клиентом. ОО автоматически создает конечную точку для каждого из четырех протоколов сетевой библиотеки, поддерживаемых им.
	Регистрационная запись (Login)	Учетная запись, создаваемая на уровне сервера БД и используемая для подключения пользователя к требуемому экземпляру SQL Server.
	База данных (Database)	Единое хранилище информации, представленной в структурированной форме.

Область действия	Тип объекта	Описание
База данных	Схема (Schema)	Коллекция сущностей БД, формирующая единое пространство имен.
	Пользователь (Database User)	Учетная запись, создаваемая на уровне БД и используемая для доступа пользователя к требуемой БД.
	Контракт (Contract)	Определяет тип сообщений, которые приложение использует для выполнения конкретной задачи. Контракт представляет собой соглашение между двумя службами о том, какое сообщение отправляет каждая служба, чтобы выполнить определенную задачу.
	Роль (Role)	Логическая группировка пользователей в соответствии с предоставленными им разрешениями на доступ.
	Роль приложения (Application Role)	Структура, используемая для ограничения доступа пользователей к данным при работе с конкретным приложением
	Сборка (assemblies)	Файлы динамической библиотеки, которые используются в экземпляре SQL Server для развертывания функций, хранимых процедур, триггеров, пользовательских статистических вычислений и определяемых пользователем типов, записанных на одном из языков управляемого кода.
	Типы сообщений (Message Types)	Определяют имя сообщения, с использованием которого осуществляется взаимодействие между приложениями, и тип данных, которые содержаться в этом сообщении.
	Привязки удаленных служб	Компонент Service Broker, устанавливающий связь между пользователем локальной базы

Область действия	Тип объекта	Описание
	(Remote Service Binding)	данных, сертификатом этого пользователя и именем удаленной службы. Компонент Service Broker использует привязку удаленной службы для обеспечения безопасности двустороннего взаимодействия при диалоге с удаленным сервером.
	Маршрут (Route)	Определяет маршрут доставки сообщения.
	Служба (Service)	Имя для конкретной бизнес-задачи или набора бизнес-задач. Каждая служба указывает очередь для хранения входящих сообщений.
	Полнотекстовый каталог (Full Text Catalog)	Используется в качестве хранилища полнотекстовых индексов. Каждый каталог может обеспечивать индексирование одной или нескольких таблиц базы данных.
Схема	Таблица (Table)	Место хранения данных. Таблица состоит из строк и столбцов. Каждая строка таблицы представляет уникальную запись, каждый столбец – отдельное поле данной записи. Помимо самой таблицы ОО предусматривает возможность разграничения доступа субъектов к ее столбцам и строкам.
	Функция (Function)	Программа, состоящая из одной или нескольких функций, включающих в себя операторы Transact-SQL. Функции применяются для инкапсуляции кода с целью его повторного использования.
	Представление (Views)	Виртуальная таблица, ограничивающая объем данных, которые пользователь может просматривать и модифицировать. Представление содержит только некоторые из

Область действия	Тип объекта	Описание
		записей или столбцов, имеющихся в таблице, либо объединяют данные из разных таблиц, представляя их пользователю как одну таблицу.
	Хранимая процедура (Stored Procedures)	Набор операторов на языке Transact-SQL, скомпилированных в одну программу.
	Синоним (Synonym)	Объект базы данных, выполняющий следующие функции: – предоставляет альтернативное имя для другого объекта базы данных, существующего на локальном или удаленном сервере, на которое затем ссылаются как на базовый объект; – обеспечивает уровень абстракции, защищающий клиентские приложения от изменений, производимых в имени или местоположении базовых объектов.
	Очередь (Query)	Область хранения, используемая для передачи сообщений.
	Типы (Types)	Атрибут, определяющий, какого рода данные могут храниться в объекте: целые числа, символы, данные денежного типа, метки времени и даты, двоичные строки и т.д. ОО предоставляет набор системных типов данных, определяющих все типы данных, которые могут использоваться в нем. Можно также определять собственные типы данных.
	Коллекция XML-схем (XML Schema Collection)	Сущность класса метаданных, подобная таблице в базе данных. Коллекции XML-схем используются для типизации переменных,

Область действия	Тип объекта	Описание
		параметров и xml-столбцов.

В качестве субъектов доступа (участников безопасности) в ОО рассматриваются сущности, которые могут запрашивать ресурсы ОО. Как и другие компоненты модели авторизации, все субъекты доступа могут быть иерархически упорядочены. При этом область их влияния зависит от области определения субъекта: среда функционирования ОО (операционная система Microsoft® Windows Server 2003™), сервер БД или база данных.

К субъектам доступа, определяемым на уровне среды функционирования ОО (участники уровня Windows), относится регистрационная запись (имя входа) пользователя, которая может быть ассоциирована с определенной группой безопасности или учетной записью пользователя (локальной или доменной) операционной системы Microsoft® Windows Server 2003™, под управлением которой функционирует ОО, используемая для подключения к ОО.

К субъектам доступа, определяемым на уровне ОО (SQL Server), относится регистрационная запись (имя входа), ассоциированная с учетной записью пользователя ОО (учетной записью SQL Server).

К субъектам доступа уровня БД относятся:

- пользователь БД;
- роль БД;
- роль приложения.

Для осуществления каких-либо действий в ОО пользователь должен пройти процедуру обязательной идентификации и аутентификации. После проверки подлинности уполномоченный пользователь может выполнять только те задачи и обращаться только к тем БД, для которых ему были предоставлены соответствующие разрешения. Разграничение доступа субъектов к объектам доступа обеспечивается ФБО посредством реализации политики дискреционного управления доступом. ФБО реализуют политику дискреционного управления доступом к объектам, основываясь на идентификаторе участника (principal ID), идентификаторе безопасности SID (SID – Security Identifier) запрашивающего субъекта доступа, идентификаторах безопасности групп безопасности Windows, участниками которых он является, и назначаемых разрешениях.

При создании регистрационной записи пользователя ей назначается идентификатор участника и идентификатор безопасности SID (Security Identifier). Идентификатор участника (principal ID) определяет регистрационную запись как защищаемый объект в рамках сервера БД. ОО присваивает его во время создания. После удаления регистрационной записи пользователя ее идентификационный номер используется повторно.

Идентификатор безопасности SID определяет контекст безопасности пользователя и является уникальным в пределах экземпляра SQL Server. Источник идентификатора безопасности зависит от способа создания регистрационной записи пользователя. Если она сопоставляется с учетной записью пользователя или группой безопасности Windows, ей присваивается идентификатор безопасности, принадлежащий исходному участнику безопасности, т.е. SID учетной записи пользователя или группы безопасности Windows. Если регистрационная запись создается для пользователя SQL Server, то идентификатор безопасности создается сервером самостоятельно.

При создании учетной записи пользователя БД ей также присваивается идентификатор участника и идентификатор безопасности. Идентификатор учатника определяет учетную запись пользователя БД как защищаемый объект в рамках базы данных. После удаления пользователя из БД его идентификационный номер используется повторно.

Идентификатор безопасности, присвоенный ученой записи пользователя БД, является уникальным в рамках этой базы данных. Источник идентификатора безопасности зависит от способа создания учетной записи пользователя БД. Если данная учетная запись сопоставлена с регистрационной записью пользователя, определяемой на уровне сервера БД, то ей присваивается идентификатор безопасности (SID) указанной записи. Если пользователь БД не сопоставлен с каким-либо именем входа, идентификатор безопасности данной учетной записи принимает значение NULL.

За исключением системных хранимых процедур область действия разрешений, назначаемых пользователю, ограничена рамками одной базы данных, поскольку учетная запись пользователя существует в каждой БД, к которой он имеет доступ.

Объект оценки поддерживает следующие типы разрешений:

- разрешения доступа к объектам (object permissions);
- разрешения на выполнение операторов (statement permissions);
- предопределенные разрешения (predefined permissions);

– неявно назначаемые (implicit) или наследуемые (derived) разрешения.

В свою очередь данные разрешения разделяются на разрешения, определяемые на уровне сервера БД, и разрешения, определяемые на уровне БД.

К разрешениям, определяемым на уровне сервера БД, относятся предопределенные разрешения, получаемые пользователем в результате включения его в состав участников предопределенных фиксированных ролей сервера БД. В ОО предусмотрено несколько предопределенных фиксированных ролей сервера БД, обладающих полномочиями на выполнение тех или иных административных задач в рамках всего сервера БД. Предопределенные разрешения наследуются всеми участниками роли и не могут быть изменены.

В число разрешений, определяемых на уровне БД, входят неявно назначаемые разрешения, предопределенные разрешения, получаемые пользователем в результате становления участником фиксированных ролей БД (database role), разрешения на выполнение операторов (statement permissions) и разрешения доступа к объектам (object permissions).

Неявно назначаемые или наследуемые разрешения приобретаются пользователем в случае, если он является владельцем объекта доступа. Например, владелец таблицы может изменять таблицу, создавать триггеры (trigger) или назначать разрешения для данной таблицы.

Разрешения на выполнения операторов представляют собой разрешения на выполнение определенных административных действий в ОО, например создание БД или ее резервной копии. Данный вид разрешений может быть назначен субъекту только участником предопределенной фиксированной роли сервера «System administrator» или владельцем БД.

Ниже представлено описание основных типов разрешений, которые предоставляются участнику безопасности (security principal) права на выполнение каких-либо действий с защищаемой сущностью (объектом доступа) в ОО:

– CONTROL;

Данное разрешение предоставляет возможности, схожие с владением. Обладающий данным разрешением субъект получает все установленные разрешения на защищаемый объект доступа в ОО. Субъект, получивший разрешение CONTROL, может также предоставлять разрешения на защищаемый объект доступа другим участникам безопасности. Так как в ОО используется иерархическая модель безопасности,

разрешение CONTROL на определенную область неявно включает разрешение CONTROL на все защищаемые сущности в пределах данной области. Например, разрешение CONTROL на базу данных неявно предполагает все разрешения на базу данных, все разрешения на все сборки в базе данных, все разрешения на все схемы в базе данных, а также все разрешения на объекты в пределах всех схем базы данных.

– ALTER;

Предоставляет возможность изменения свойств объекта доступа, кроме его владельца. При предоставлении разрешения ALTER на ту или иную область также предоставляется возможность изменения, создания или удаления любого защищаемого объекта доступа, содержащейся в пределах данной области. Например, разрешение ALTER на схему включает возможность создания, изменения и удаления объектов этой схемы.

– ALTER ANY <*защищаемый объект сервера*>, где <*защищаемый объект сервера*> может быть любым защищаемым объектом доступа на уровне сервера БД;

Данное разрешение предоставляет субъекту возможность создавать, изменять и удалять отдельные экземпляры объектов, определяемых на уровне сервера. Например, разрешение ALTER ANY LOGIN предоставляет пользователю возможность создания, изменения и удаления любой регистрационной записи пользователя (имени входа).

– ALTER ANY <*защищаемый объект БД*>, где <*защищаемый объект БД*> может быть любым защищаемым объектом доступа, определяемым на уровне базы данных;

Данное разрешение предоставляет субъекту возможность создавать (CREATE), изменять (ALTER) и удалять (DROP) отдельные экземпляры объектов, определяемых на уровне базы данных. Например, разрешение ALTER ANY SCHEMA предоставляет пользователю возможность создания, изменения и удаления любой схемы в базе данных.

– TAKE OWNERSHIP;

Данное разрешение позволяет субъекту переопределять владение защищаемого объекта, на который данное разрешение предоставлено.

– IMPERSONATE <*имя входа*>;

Позволяет олицетворять (имперсонировать) регистрационную запись пользователя.

– IMPERSONATE <*пользователь*>;

Позволяет олицетворять (имперсонировать) пользователя БД.

– CREATE <*защищаемый объект сервера*>;

Данное разрешение позволяет субъекту, которому оно предоставлено, создавать защищаемые объекты на уровне сервера БД. Например, наличие данного разрешения потребуется при создании пользователем базы данных, имени входа или конечной точки.

– CREATE < *защищаемый объект БД*>;

Данное разрешение позволяет субъекту, которому оно предоставлено, создавать защищаемые объекты на уровне БД. Например, наличие данного разрешения требуется при создании пользователем схемы, контракта, учетной записи пользователя БД и т.д.

– CREATE < *защищаемый объект схемы*>;

Данное разрешение предоставляет субъекту возможность создания защищаемых объектов, содержащихся в схеме. Однако для создания защищаемого объекта в той или иной схеме на эту схему требуется разрешение ALTER.

– VIEW DEFENITION;

Данное разрешение предоставляет пользователю доступ к метаданным объектов без предоставления непосредственного доступа к этим объектам.

– BACKUP DATABASE, BACKUP LOG;

Данное разрешение предоставляет пользователю возможность создания резервной копии всей БД, журнала транзакций, а также одного или несколько файлов или файловых групп.

– RESTORE DATABASE, RESTORE LOG;

Данное разрешение предоставляет пользователю выполнить следующие операции:

- восстановление всей базы данных из полной резервной копии (полное восстановление);
- восстановление части базы данных (частичное восстановление);
- восстановление в базе данных определенные файлы, файловые группы или страницы (восстановление файлов или страниц);
- восстановление в базе данных журнала транзакций (восстановление журнала транзакций);
- возвращение базы данных к моменту времени, на который был выполнен моментальный снимок базы данных.

Разрешения доступа к объектам представляют собой разрешения на выполнение уполномоченным пользователем определенных операций с защищаемыми объектами, такими как таблицы, представления, определяемые пользователем функции, хранимые

процедуры и т.д. В таблице 6.4 представлен перечень поддерживаемых ОО разрешений доступа к объектам и описание соответствующих им действий.

Таблица 6.4 – Разрешения доступа к защищаемым объектам и область их применения

№ п/п	Разрешение	Область применения	Допустимые действия
1.	SELECT	Синонимы; Таблицы; Возвращающие табличное значение функции Transact-SQL; Представления.	Просмотр данных в таблице, представлении или поле таблицы. Разрешение SELECT может быть также предоставлено на определяемые пользователем функции. Данное разрешение наследуется участниками предопределенной фиксированной роли сервера «System Administrators» и фиксированных ролей БД db_owner и db_reader. В указанном разрешении отказано всем участникам фиксированной роли БД db_denydatareader.
2.	INSERT	Синонимы; Таблицы; Представления.	Добавление новых данных в таблицу или представление. Данное разрешение наследуется участниками предопределенной фиксированной роли сервера «System Administrators» и фиксированных ролей БД db_owner и db_datawriter. В указанном разрешении отказано всем участникам фиксированной роли БД db_denydatawriter.
3.	UPDATE	Синонимы; Таблицы; Представления.	Обновление данных в таблице, поле таблицы или представлении. Данное разрешение наследуется участниками предопределенной фиксированной роли сервера «System Administrators» и фиксированных ролей БД db_owner и db_datawriter. В ука-

№ п/п	Разрешение	Область применения	Допустимые действия
			занном разрешении отказано всем участникам фиксированной роли БД db_denydatawriter.
4.	DELETE	Синонимы; Таблицы; Представления.	Удаление данных из таблицы или представления. Данное разрешение наследуется участниками предопределенной фиксированной роли сервера «System Administrators» и фиксированных ролей БД db_owner и db_datawriter. В указанном разрешении отказано всем участникам фиксированной роли БД db_denydatawriter.
5.	EXECUTE	Процедуры; Скалярные и статистические функции; Синонимы.	Выполнение хранимых процедур и пользовательских функций. Данное разрешение наследуется участниками предопределенной роли сервера «System Administrators» и фиксированной роли БД db_owner.
6.	REFERENCES	Скалярные и статистические функции; Очереди Service Broker; Таблицы; Возвращающие табличное значение функции; Представления.	Обращение к таблице с ограничением FOREIGN KEY при отсутствии разрешений SELECT на таблицу. Данное разрешение наследуется участниками предопределенной роли сервера «System Administrators» и фиксированных ролей БД db_owner и db_datareader. В указанном разрешении отказано всем участникам фиксированной роли БД db_denydatareader.
7.	RECEIVE	Очереди Service Broker	Извлечение из очереди одного или нескольких сообщений и возвращение ре-

№ п/п	Разрешение	Область применения	Допустимые действия
			зультирующего набора. Возвращаемый результирующий набор может быть пустым или содержать несколько строк, каждая из которых содержит одно сообщение. В зависимости от настройки хранения для очереди сообщение из очереди может удаляться или осуществляться обновление состояния сообщения в очереди.
8.	VIEW DEFINITION	Процедуры; Очереди Service Broker; Скалярные и статистические функции; Синонимы; Таблицы; Возвращающие табличное значение функции; Представления.	Просмотр метаданных защищаемого объекта, на который предоставлено разрешение. Однако данное разрешение не предоставляет доступ непосредственно к самому объекту. Разрешение VIEW DEFINITION может быть предоставлено на следующих уровнях: – область сервера; – область базы данных; – область схемы; – отдельные объекты.
9.	ALTER	Процедуры; Скалярные и статистические функции; Очереди Service Broker; Таблицы; Возвращающие табличное значение функции; Представления	Изменение защищаемого объекта, не затрагивающее владельца объекта.

№ п/п	Разрешение	Область применения	Допустимые действия
10.	TAKE OWNER-SHIP	Процедуры; Скалярные и статистические функции; Синонимы; Таблицы; Возвращающие табличное значение функции; Представления	Передача прав на обладание объектом от одного субъекта к другому.
11.	CONTROL	Процедуры; Скалярные и статистические функции; Очереди Service Broker; Синонимы; Таблицы; Возвращающие табличное значение функции; Представления	Получение разрешений в объеме, схожем с владением данным объектом. Обладающий данным разрешением субъект получает все установленные разрешения на защищаемый объект.

Объект оценки обеспечивает возможность предоставления, блокирования и отзыва разрешений пользователя только уполномоченным администратором. Управление разрешениями на выполнение операторов и разрешениями доступа к объектам обеспечивается в ОО посредством одноименных операторов Transact-SQL: `GRANT` (предоставить), `DENY` (блокировать) и `REVOKE` (отозвать).

Объект оценки обеспечивает следующие способы получения пользователями разрешений для работы с данными, создания объектов данных и выполнения административных задач:

- в результате членства в соответствующей предопределенной фиксированной роли сервера БД;
- в результате членства в соответствующей фиксированной роли БД;

- в результате предоставления права владельца БД (при этом пользователь наследует все связанные с объектом разрешения доступа, включая право предоставлять разрешения на работу с данным объектом);
- в результате предоставления права владельца объекта БД, полученного в результате членства в соответствующей фиксированной роли БД;
- посредством назначения отдельных разрешений на доступ к объектам и разрешений на выполнения операторов (при этом исходя из иерархической модели безопасности ОО, предоставленное разрешение на определенную область неявно включает аналогичные разрешения на все защищаемые объекты в пределах данной области);
- наследование разрешений роли `public` пользователем, который обладает доступом к БД;
- наследование разрешений пользователя `guest` пользователем, который не обладает доступом к БД.

Алгоритм реализации политики дискреционного управления доступом

Представленный ниже алгоритм дает краткое описание механизма принятия решения о разрешении доступа к объекту данных пользователю. Для того, чтобы предоставить доступ к объекту, ОО выполняет проверку запрашиваемых прав доступа, осуществляемую в несколько этапов и предусматривающую проверку разрешений на подключение к ОО и проверку разрешений на выполнение действий с самой базой данных, со схемой и объектами в данной схеме БД (таблицами, представлениями, хранимыми процедурами и т.д.). При этом, как отмечалось выше, для идентификации субъектов доступа, выполняющих в системе различные действия, ОО использует не символьные имена (которые могут быть не уникальными), а идентификаторы участника (principal ID) и идентификаторы безопасности SID, которые используются для внутреннего представления данных субъектов доступа.

Идентификаторы безопасности имеются у пользователей, локальных и доменных групп безопасности Windows, компьютеров и представляют собой числовое значение переменной длины, формируемое из номера версии структуры SID, 48-битного кода агента идентификатора и переменного количества 32-битных кодов субагентов и/или относительных идентификаторов (RID – relative identifiers).

Использование идентификаторов безопасности возможно только при условии доверенного соединения (trusted connection) пользователя с ОО, при котором проверка подлинности пользователя осуществляется средствами операционной системы Microsoft® Windows Server 2003™, под управлением которой функционирует ОО, и не требует его отдельной регистрации как пользователя ОО. Все регистрационные записи, сопоставленные с учетными записями пользователей или групп безопасности Windows, хранятся в системном представлении `sys.server_principals`. Данное представление содержит также идентификаторы безопасности для указанных учетных записей пользователей или групп безопасности.

В случае недоверенного соединения (non-trusted connection), для успешно аутентифицированного субъекта доступа ОО генерирует собственный 16-битный глобально уникальный идентификатор GUID (globally unique identifiers), который в дальнейшем используется системой безопасности ОО таким же образом, что и идентификаторы безопасности SID. Все учетные записи для подключения к ОО также хранятся в системном представлении `sys.server_principals`. Идентификатор GUID, который используется в качестве идентификатора безопасности, также хранится в данном представлении.

Для однозначной идентификации субъектов доступа внутри БД используются идентификаторы пользователя базы данных UID (User identifier), представляющие собой целые 2-байтные числа. Имена пользователей БД хранятся в `sys.database_principals`, представленной в каждой базе данных. Каждое имя пользователя БД связано с идентификатором пользователя БД в столбце `sys.database_principals.uid`.

1. Проверка разрешений на подключение к ОО

При обращении пользователя к ОО, последний осуществляет проверку разрешений на подключение данного субъекта доступа. Для осуществления доступа к ОО для пользователя должна существовать регистрационная запись (имя входа), для которой определены разрешающие или запрещающие права доступа. При этом сначала ОО осуществляет проверку явных запретов на подключение. В случае отсутствия явных запретов на установление соединения ОО проверяет, предоставлено ли пользователю право на доступ к ОО. Если пользователь указал правильный идентификатор имени входа

(login name), для которого уполномоченным администратором определены разрешающие права доступа к ОО, для данного субъекта доступа создается новый сеанс.

При создании нового сеанса пользователя ОО формирует в памяти структуру Process Status Structure (PSS), которая содержит идентификатор безопасности пользователя, выполнившего подключение, идентификаторы безопасности групп безопасности Windows, членами которых он является (если доступ осуществляется с использованием учетной записи пользователя Microsoft Windows), и другую относящуюся к безопасности и состоянию сеанса информацию. Структура PSS предназначена для идентификации контекста безопасности пользователя и является постоянной на всем промежутке времени подключения пользователя к ОО. При многочисленных подключениях одного пользователя к ОО для него формируется такое множество структур PSS, которое эквивалентно количеству открываемых им сеансов.

2. Проверка разрешений на доступ к БД

После того, как ОО проверил подлинность пользователя, он выполняет проверку прав данного пользователя на выполнения различных действий в размещенных на сервере БД. Сам по себе идентификатор регистрационной записи (имени входа) пользователя не дает зарегистрированному пользователю право доступа к различным БД и объектам БД. Он позволяет перейти к следующему этапу – авторизации, т.е. проверке прав зарегистрировавшего пользователя. Такой механизм проверки прав доступа гарантирует, что зарегистрированный пользователь не получит автоматический доступ ко всем БД на сервере БД, с которым он установил соединение. Для обеспечения доступа к БД идентификатор регистрационной записи (имени входа) пользователя должен быть сопоставлен с идентификатором учетной записи пользователя в БД. Сопоставление идентификатора регистрационной записи пользователя и идентификатора учетной записи пользователя в БД выполняется в системном представлении `sys.database_principals` той БД, к которой пользователь имеет права доступа.

Таким образом, при доступе пользователя к базе данных ОО обращается к содержимому системного представления `sys.database_principals` данной БД для определения того, какие полномочия доступа к БД предоставлены указанному пользователю. При этом для поиска записей таблицы, сопоставленных осуществляющему доступ пользователю, используется его идентификатор безопасности SID.

В случае если проверка подлинности осуществлялась средствами ОС, ОО осуществляет последовательный просмотр строк системного представления `sys.database_principals` для каждого идентификатора безопасности (пользователя или группы, членом которой он является), содержащегося в предъявляемом пользователем билете Kerberos (Kerberos ticket), представляющим собой персональное электронное «удостоверение» пользователя.

Если пользователю запрещен доступ к БД, дальнейшее обращение к самой БД и ее объектам невозможно. В противном случае выполняется повторный просмотр содержимого системного представления `sys.database_principals` и осуществляется поиск и выбор всех идентификаторов учетных записей пользователей данной БД, с которыми сопоставлен идентификатор регистрационной записи (имени входа) успешно прошедшего проверку подлинности пользователя.

После успешной авторизации субъекта доступа ОО осуществляет просмотр системного представления `sys.database_role_members` на предмет выявления всей совокупности ролей, участником которых он является. Это позволит при разграничении доступа к объекту учесть разрешения, определенные для ролей, участниками которых являются субъекты доступа. В результате ОО формирует список, который содержит как собственный идентификатор пользователя, так и идентификаторы всей совокупности ролей, участником которых он является.

3. Проверка разрешений на доступ к объектам БД

При осуществлении доступа к объектам БД (таблицам, представлениям, хранимым процедурам и т.д.) ОО осуществляет проверку разрешений доступа, основываясь на информации, представленной в системном представлении **`sys.database_permissions`** текущей БД. При этом формирование набора предоставленных прав доступа (granted access rights) осуществляется путем просмотра тех строк представления `sys.database_permissions`, в которых соответствующее поле данных совпадает со значением идентификатора учетной записи пользователя, осуществляющего доступ к объектам БД.

Проверка разрешений доступа выполняется до первого запрета на какую-либо запрашиваемую операцию. В случае наличия запрещающего правила для субъекта доступа, выполнение требуемых действий с указанным объектом запрещается. В противном случае, т.е. при отсутствии запрещающего правила и наличии строк,

определяющих разрешающие права доступа для указанного субъекта доступа, доступ к объекту предоставляется. При повторном обращении данного субъекта доступа к тем же самым объектам доступа (объектам БД) повторная проверка прав доступа не осуществляется. Данная возможность обеспечивается посредством механизма кэширования набора предоставленных прав доступа, реализуемого ОО.

Объект оценки обеспечивает кэширование разрешений доступа к объектам (object permissions) на время установления сессии, что позволяет избежать затрат на проверку разрешений доступа при повторном обращении субъекта к тем же самым объектам доступа. В отличие от структуры PSS, которая является неизменной с момента открытия новой сессии, кэш прав доступа изменяется с течением времени и всегда содержит последний эффективный набор предоставленных прав доступа. Данная возможность обеспечивается использованием счетчика версий.

При первичной проверке разрешений доступа к объекту ОО устанавливает начальный номер версии. В случае изменения прав доступа, определяемых для данного объекта доступа, ОО увеличивает номер версии. Каждый раз при осуществлении доступа к объекту происходит сравнение текущего значения счетчика версий со значением, хранимым в кэше. В случае получения отрицательного результата их сравнения, набор предоставленных прав доступа, хранимый в кэше, обнуляется и осуществляется формирование нового эффективного набора предоставленных прав доступа.

Цепочка владельцев

Понятие цепочки владельцев определяет порядок проверки ОО разрешений доступа пользователя при попытке выполнения им действий с использованием объектов БД (представлений или хранимых процедур) относительно данных, содержащихся в базовых объектах (таблицах БД), к которым данный пользователь не имеет прав доступа. Например, если владелец представления или хранимой процедуры отличен от пользователя, которому принадлежит таблица, возникает «прерывание цепочки владельцев» (broken ownership chain), что принуждает ОО осуществлять проверку разрешений на доступ, определенных для каждого объекта в цепочке, по отдельности. Таким образом, если субъекту предоставлен доступ к представлению, которое в свою очередь базируется на таблице БД, и при этом право доступа к ней определено только для владельца данного представления, то проверка разрешений на доступ для субъекта будет осуществляться ОО в два этапа - сначала для запрашивающего субъекта будут проверены

разрешения на доступ к представлению, впоследствии – разрешения на доступ к таблице БД.

Кроме того, ОО обеспечивает возможность поддержки цепочки владения между конкретными БД или всеми БД внутри одного экземпляра SQL Server.

Организация цепочек владения является механизмом авторизации, с помощью которого ОО автоматически авторизует одного пользователя для доступа к объектам другого пользователя при условии, что первый имеет разрешение на исполнение программных модулей (хранимых процедур или функций), которыми владеет второй пользователь. Однако, кроме механизма организации цепочек владения, ОО обеспечивает другой механизм управления разрешениями пользователя во время доступа к зависимым объектам – управление контекстом выполнения.

Управление контекстом выполнения

Контекст выполнения определяется полномочиями подключенного к сеансу пользователя или же выполняющимся (вызывающим) модулем. При этом контекст определяет идентификатор того, чьи разрешения на выполнение инструкций или совершение каких-либо действий в ОО должны быть проверены. Контекст выполнения представляется парой маркеров безопасности: маркером регистрационной записи пользователя (имени входа) и маркером пользователя БД. Эти маркеры идентифицируют первичного и вторичного участников безопасности, для которых проверяются разрешения, а также источник, использующийся для проверки подлинности маркеров безопасности. У пользователя, которой осуществляет подключение к экземпляру SQL Server, имеется один маркер регистрационной записи и один (или более) маркеров пользователя БД, в зависимости от числа баз данных, к которым обладает доступом данный пользователь.

Маркер регистрационной записи пользователя, определяемой на уровне сервера БД, действителен в пределах экземпляра SQL Server. Он содержит первичный и вторичный идентификаторы, для которых проверяются разрешения, связанные с ними на уровне сервера и на уровне базы данных. Регистрационная запись является первичным идентификатором. Вторичный идентификатор включает разрешения, унаследованные от предопределенных фиксированных ролей сервера БД, в состав которых включена регистрационная запись пользователя.

Маркер пользователя БД действителен только в пределах конкретной базы данных. Он также содержит первичный и вторичный идентификаторы, для которых проверяются разрешения, связанные с ними на уровне базы данных. Имя учетной записи пользователя БД само по себе является первичным идентификатором. Вторичный идентификатор содержит разрешения, унаследованные групп. членом которой является пользователь. Маркер пользователя не содержит членства в предопределенных фиксированных ролях сервера БД, и идентификаторы маркеров пользователя не могут получать разрешения уровня сервера, в том числе те, которые предоставляются участникам серверной роли public.

По умолчанию сеанс запускается при входе пользователя в систему и завершается при выходе пользователя из системы. Все выполняемые пользователем операции во время сеанса подлежат проверке на наличие у него соответствующих разрешений. При этом ОО обеспечивает возможность изменения контекста выполнения модуля, например, например хранимой процедуры, триггера или пользовательской функции, явным указанием имени регистрационной записи пользователя или имени учетной записи пользователя БД, в чьем контексте он должен выполняться. После контекстного переключения ОО осуществляет проверку разрешений уже той регистрационной записи и маркеров безопасности пользователя, чьи реквизиты указаны при вызове инструкции EXECUTE AS. Далее выполнение модуля осуществляется в контексте указанного пользователя до завершения, или когда происходит явное восстановление контекстного переключения.

Используя механизм контекстного переключения, ОО позволят указывать, учетные данные каких пользователей следует использовать при проверке разрешений на объекты, на которые ссылается вызываемый модуль. Это повышает гибкость и безопасность управления разрешениями на цепочки владения между пользовательскими модулями и объектами, на которые они ссылаются. При этом пользователям необходимо будет предоставлять только разрешения на сам модуль, без выдачи явных разрешений на объекты, на которые он ссылается.

Объект оценки позволяет задавать контекст выполнения хранимых процедур и пользовательских функций (UDF) — исключая макрофункции внутри таблиц — с помощью выражения EXECUTE AS, помещенного в заголовок определения модуля (неявное олицетворение), или с помощью автономной инструкции EXECUTE AS (явное олицетворение). Данный механизм предоставляет разработчику приложений возможность более строгого контроля аутентификации, позволяя одному пользователю выполнять

действия внутри модуля таким образом, если бы он аутентифицировался как другой пользователь.

4. Проверка разрешений на выполнение операторов

В случае необходимости создания пользователем как самих баз данных, так и их объектов, ОО осуществляет проверку предоставленных пользователю разрешений на выполнение инструкций языка DDL (Transact-SQL). Разрешения на выполнение инструкций DDL – это разрешения на выполнение административных действий с самой БД или ее объектами (например, создание БД, схемы или ее объектов, таких как таблицы, представления и хранимые процедуры). Если разрешения на выполнения инструкций языка DDL (Transact-SQL), а фактически на создание объектов доступа, предоставлены не были, пользователь получит отказ в доступе.

Обеспечение защиты через устанавливаемые по умолчанию права доступа

Объект оценки обеспечивает применение устанавливаемых по умолчанию прав доступа ко всем создаваемым объектам. При создании новых объектов для них определяется соответствующие права доступа, обеспечивая по умолчанию доступ для следующих категорий субъектов доступа:

- владельца объекта, т.е. субъекта создавшего объект. Владелец объекта наследует все связанные с объектом разрешения доступа, включая право предоставлять разрешение на работу с данным объектом;
- участников предопределенной фиксированной роли сервера БД «System Administrators». Участники данной роли могут выполнять любые действия в любой БД, поскольку идентификаторы их регистрационных записей автоматически сопоставляются с учетной записью пользователя БД «dbo» (database owner), являющегося владельцем БД.

Предоставление разрешений посредством назначения пользователю роли

Объект оценки обеспечивает предоставление разрешений пользователю посредством включения его регистрационной записи (имени входа) или учетной записи в состав соответствующих ролей, представляющих собой логическую группировку пользователей, имеющих одинаковые права доступа. В ОО предусмотрены следующие типы ролей:

– предопределенные фиксированные роли сервера БД;
– роли БД.

В свою очередь роли БД разделяются на следующие роли:

– фиксированные роли БД;
– роли, определяемые пользователем.

Роли, определяемые пользователем, позволяют группировать пользователей согласно выполняемым ими функциям и назначать каждой группе специальные разрешения на выполнение требуемой совокупности действий с объектами БД. К ролям, определяемым пользователем, относятся стандартная роль и роль приложения.

Стандартная роль используется для управления разграничением доступа к объектам БД. Основное назначение стандартной роли – логическая группировка пользователей в соответствии с предоставленными им разрешениями на доступ.

Роль приложения используется для ограничения доступа пользователей к данным при работе с конкретным приложением. Ограничение доступа пользователей предупреждает возможность запуска ими некорректно составленных запросов и получение информации, доступ к которой ограничен. Когда пользователь активизирует роль приложения в пределах конкретной БД, предоставляемые ему права доступа к данной БД ограничиваются назначенными для этой роли разрешениями. Таким образом, если доступ к БД осуществляется через роль приложения, существующие разрешения доступа пользователя к БД (или их отсутствие) игнорируются. После того, как роль приложения была активирована, она не может быть деактивирована. Единственным способом получения пользователем своих исходных полномочий является завершение сеанса с ОО и установление нового сеанса без использования приложения. Роль приложения поддерживает оба режима проверки подлинности, реализуемых ОО.

Основные различия между ролью приложения и стандартными ролями БД заключаются в следующем:

– роль приложения может быть защищена паролем, а стандартные роли, определяемые пользователем, - нет. Если роль приложения защищена паролем, то для ее активации необходимо ввести пароль;
– роль приложения не назначается пользователю БД непосредственно, т.е. он не может являться ее участником. Пользователи просто активизируют роль приложения в пределах конкретной БД.

Отделение пользователя от схемы

Под понятием схема (schema) понимается набор объектов БД, принадлежащий одному владельцу и образующий единое пространство имен. Схема — это контейнер, который содержит таблицы, представления, процедуры и т.д. Каждый защищаемый объект в конкретной схеме имеет уникальное имя. Полностью указанное имя защищаемого объекта, содержавшегося в схеме, включает имя этой схемы.

В ОО отсутствует неявная связь между пользователями базы данных и схемами. Отделение схемы от владельца объекта позволяет обеспечить удаление пользователей из БД без обязательного удаления объектов, которые принадлежат данному пользователю, или смены их владельца.

В ОО схемы существуют независимо от создавшего их пользователя базы данных, поэтому права владения схемами могут быть переданы без изменения имен самих схем.

Отделение пользователя от схем предоставляет ряд преимуществ:

- одной схемой могут владеть несколько пользователей, что расширяет функциональность управления объектами;
- удаление пользователей из баз данных значительно упрощается;
- для удаления пользователей из баз данных не требуется переименовывать объекты, содержащихся в схеме данного пользователя. Таким образом, отсутствует необходимость в проверке и тестирование приложений, явно ссылающихся на содержащиеся в схеме защищаемые объекты, после удаления создавшего их пользователя;
- несколько пользователей могут совместно использовать одну схему по умолчанию для унифицированного разрешения имен;
- общие схемы по умолчанию позволяют разработчикам хранить общие объекты в схеме, специально созданной для данного приложения;
- улучшенное управление разрешениями на схемы и содержащимися в них защищаемыми объектами .

База данных учетных записей пользователей БД

Объект оценки поддерживает базу данных, в которой полностью определены учетные записи пользователей, имеющих доступ к БД (база учетных записей пользователей БД, представлена содержимым системного представления `sys.database_principals`). При этом база данных учетных записей пользователей

поддерживается отдельно для каждой существующей БД, для которой определены права доступа. Каждая учетная запись представлена в данной базе следующим набором атрибутов (см. таблицу 6.5).

Таблица 6.5.

Имя столбца	Тип данных	Описание
name	**sysname**	Имя учетной записи пользователя БД , уникальное в пределах базы данных.
principal_id	**int**	Идентификатор субъекта, уникальный в пределах базы данных.
type	**char(1)**	Тип участника: S = пользователь SQL; U = пользователь Windows; G = группа Windows; A = роль приложения; R = роль базы данных; C = пользователь сопоставлен с сертификатом; K = пользователь сопоставлен с асимметричным ключом;
type_desc	**nvarchar(60)**	Описание типа участника. SQL_USER WINDOWS_USER WINDOWS_GROUP APPLICATION_ROLE DATABASE_ROLE CERTIFICATE_MAPPED_USER ASYMMETRIC_KEY_MAPPED_USER
default_schema_name	**sysname**	Имя, используемое в случае, когда схема не определяется именем SQL. NULL для участников с типами, отличными от S, U или A.
create_date	**datetime**	Время создания учетной записи пользователя БД.
modify_date	**datetime**	Время последнего изменения учетной записи

Имя столбца	Тип данных	Описание
		пользователя БД.
owning_principal_id	**int**	Идентификатор субъекта, являющегося владельцем для данной учетной записи пользователя БД. Владельцем всех участников, кроме ролей баз данных, должен быть объект **dbo**.
sid	**varbinary(85)**	Идентификатор безопасности (SID), если пользователь БД сопоставлен с внешней регистрационной записью (именем входа) (типы S, U и G). В ином случае равен NULL.
is_fixed_role	**bit**	Если значение равно 1, в данной строке представляется запись для одной из фиксированных ролей БД: – db_owner; – db_accessadmin; – db_datareader; – db_datawriter; – db_ddladmin; – db_securityadmin; – db_backupoperator; – db_denydatareader; – db_denydatawriter.

Сопоставление с ФТБ

Функции безопасности «Защита данных пользователя» удовлетворяют следующим функциональным требованиям безопасности:

- FDP_ACC.1 – в ОО реализован механизм дискреционного управления доступом для субъектов – процессов, действующих от имени пользователей, именованных объектов различных уровней и всех операций между субъектами и объектами;
- FDP_ACF.1 – ФБО обеспечивают доступ к объектам, основываясь на ассоциированных с субъектом идентификаторе учетной записи пользователя,

принадлежности к роли (ролям). Описание правил, определяющих порядок доступа к объектам, представлено в алгоритме реализации дискреционного управления доступом.

6.1.3 Функции безопасности «Идентификация и аутентификация»

Объект оценки требует, чтобы каждый пользователь был идентифицирован и аутентифицирован до того момента, как от его имени в системе будут выполнены какие-либо действия, и независимо от того выполняет ли он интерактивный вход в ОО либо осуществляет доступ к ОО через сеть.

6.1.3.1 Типы входа в ОО

Объект оценки поддерживает два типа доступа пользователя к ОО:

- интерактивный – локальный доступ пользователя к ОО;
- сетевой – доступ к ОО через сеть.

Интерактивный доступ предусматривает доступ пользователя в ОО через локальную консоль и предполагает работу пользователя с ОО в интерактивном режиме. Сетевой доступ используется при удаленном обращении пользователя к серверу БД для доступа к его активам.

6.1.3.2 Режимы проверки подлинности в ОО

Каждый пользователь, осуществляющий попытку доступа к БД, должен быть идентифицирован и аутентифицирован. Для обеспечения доступа пользователя к БД и выполнения в ней каких-либо действий, в ОО должна существовать регистрационная запись пользователя (имя входа), для которой уполномоченный администратор определяет права доступа к ОО и назначает соответствующие разрешения на доступ к целевой БД. При этом регистрационная запись пользователя может быть ассоциирована с определенной группой безопасности или учетной записью пользователя операционной системы Microsoft® Windows Server 2003™, под управлением которой функционирует ОО, либо с учетной записью пользователя ОО (учетной записью SQL Server). Хранение регистрационных записей пользователей, для которых определен доступ к ОО, осуществляется в БД `master` в системном представлении `sys.server_principals`. Данное представление является единственным в рамках всего ОО и содержится только в БД `master`.

Объект оценки требует, чтобы все пользователи уникально идентифицировались при входе в систему с помощью ввода идентификатора пользователя. При этом проверка подлинности субъекта доступа может осуществляться двумя способами:

- проверка подлинности средствами операционной системы;
- проверка подлинности средствами ОО.

Чтобы пользователь смог осуществить доступ в систему, ОО выполняет проверку того, является ли он зарегистрированным в ОО пользователем и имеет ли право устанавливать с ним соединение, т.е. осуществляет проверку регистрационных данных субъекта доступа.

Проверка подлинности средствами операционной системы

Данный способ предполагает проверку подлинности регистрационных данных субъекта доступа средствами операционной системы Microsoft® Windows Server 2003™, под управления которой функционирует ОО. В дальнейшем при осуществлении доступа к ОО, повторная проверка подлинности не осуществляется, поскольку ОО доверяет результатам проверки, выполненной при регистрации пользователя в операционной системе. Таким образом, доступ к ОО осуществляется на основании пароля и имени пользователя, указанных им при входе в операционную систему. При этом для идентификации пользователя, осуществляющего доступ к ОО, используется билет Kerberos (Kerberos ticket), представляющий собой персональное электронное «удостоверение» пользователя. В последующем, ОО извлекает из билета Kerberos идентификаторы безопасности SID, однозначно идентифицирующие пользователя и группы безопасности Windows, участниками которых он является, и осуществляет их сравнение с имеющимся списком идентификаторов пользователей и групп пользователей, которым разрешен доступ к ОО, и на основании результатов сравнения предоставляет или отказывает в доступе. Такой тип подключения, которое использует средства проверки подлинности Windows, называется доверенным (trusted connection).

Использование данного механизма проверки подлинности регистрационных данных пользователя позволяет обеспечить:

- передачу контроллеру домена, реализующему логику проверки регистрационных данных пользователя и принимающему решение об

успешной или неуспешной регистрации, имени входа и пароля пользователя в защищенном виде;

- передачу объекту оценки билета Kerberos, принадлежащего пользователю, прошедшему проверку, в защищенном виде;
- задание и верификацию критериев качества аутентификационной информации пользователя (использование политики паролей для определения требований сложности, минимальной длины, максимального времени действия и других характеристик пароля пользователя);
- использование политики блокировки учетных записей, определяющей допустимое число неудачных попыток ввода пароля пользователя, при превышении которых учетная запись пользователя будет заблокирована;
- доверенный маршрут передачи идентификационной и аутентификационной информации при первоначальном интерактивном входе пользователя в операционную систему, под управлением которой функционирует ОО. Доверенный маршрут вызывается одновременным нажатием клавиш Ctrl+Alt+Del, что всегда фиксируется функциями безопасности операционной системы Microsoft® Windows Server 2003™, т.е. данное действие не может быть прервано или перехвачено недоверенным процессом.

Таким образом, при использовании данного способа проверки подлинности задействуются расширенные возможности обеспечения безопасности, реализуемые механизмами безопасности операционной системы, под управлением которой функционирует ОО.

Проверка подлинности средствами ОО

Данный способ предполагает проверку подлинности регистрационных данных субъекта доступа средствами ОО. Если подключающийся пользователь не прошел проверку подлинности в домене или подключается с использованием учетной записи SQL Server, ОО может осуществить проверку подлинности собственными средствами на основе указанных пользователем имени входа и пароля. При проверке подлинности собственными средствами ОО сравнивает переданное имя пользователя с перечнем имеющихся регистрационных записей (имен входа). Если ОО находит имя пользователя в системном представлении `sys.server_principals`, он хэширует пароль и сравнивает

его с хэшем пароля в данной таблице. По результатам сравнения ОО принимает решение о предоставлении или отказе в доступе подключающемуся пользователю.

Использование данного способа проверки подлинности регистрационных данных пользователя не позволяет обеспечить:

- передачу регистрационных данных пользователя в защищенном виде (при условии отсутствия дополнительных средств защиты сетевого трафика);
- задание и верификацию критериев качества аутентификационной информации пользователя;
- использование политики блокировки учетных записей, определяющей допустимое число неудачных попыток ввода пароля пользователя, при превышении которых учетная запись пользователя будет заблокирована;
- доверенный маршрут передачи идентификационной и аутентификационной информации.

Наличие указанных недостатков механизма проверки подлинности средствами ОО не позволяет обеспечить при его использовании адекватную защиту от попыток нарушения безопасности ОО даже нарушителями с низким потенциалом нападения.

Рекомендации об отказе от использования данного способа проверки подлинности представлены в технической документации (Microsoft TechNet) по Microsoft® SQL Server™ 2005 Standard Edition.

В тоже время ОО позволяет обеспечить возможность применения к учетным записям SQL Server, используемым для прямого подключения к ОО, требований политики паролей и политики блокировки учетной записи, задаваемых через механизм групповой политики средой ОО. Однако данная возможность может быть реализована только при условии функционирования ОО в среде ОС семейства Microsoft® Windows Server™ 2003 (благодаря поддержки последними API-интерфейса `NetValidate PasswordPolicy`).

При задании требования о необходимости удовлетворения паролей критериям сложности, вновь задаваемые для учетных записей пользователей SQL Server пароли будут удовлетворять следующим метрикам качества:

- не содержать частично или полностью имя учетной записи пользователя (часть имени учетной записи определяется как три или более последовательных алфавитно-цифровых символа, ограниченных с обеих сторон пробельными символами (пробелом, символом табуляции, символом новой строки) или

любым из следующих символов: запятая (,), точка (.), дефис (-), подчеркивание (_) или решетка (#));

- длина пароля будет составлять не менее 8 (восьми) символов;
- пароль будет содержать символы, соответствующие трем из следующих четырех категорий символов:
  - прописные буквы латинского алфавита (A-Z);
  - строчные буквы латинского алфавита (a-z);
  - цифры (0-9);
  - не алфавитно-цифровые символы (такие как: !, $, #, &? %),

При этом используемые пароли пользователей могут состоять не более чем из 128 символов.

Политика истечения срока действия паролей используется для управления продолжительностью действия пароля учетной записи пользователя SQL Server. Когда ОО применяет политику истечения срока действия паролей, пользователи получают уведомления о необходимости изменения старых паролей, а учетные записи с истекшим сроком действия паролей отключаются.

Применение политики паролей может быть настроено отдельно для каждой учетной записи пользователя SQL Server, используемой для прямого подключения к ОО.

Использование проверки подлинности регистрационных данных пользователя средствами ОО не позволяет обеспечить:

- передачу регистрационных данных пользователя в защищенном виде (при условии отсутствия дополнительных средств защиты сетевого трафика);
- доверенный маршрут передачи идентификационной и аутентификационной информации.

Сетевые библиотеки и проверка подлинности

Для обеспечения взаимодействия между сервером БД и клиентскими приложениями с использованием требуемого сетевого протокола ОО реализует поддержку соответствующей пары сетевых библиотек (клиентской и серверной сетевой библиотеки), которые должны быть активны соответственно на клиенте и на сервере.

При использовании сетевых библиотек Named Pipes и Multiprotocol требуется, чтобы пользователь первоначально прошел проверку подлинности в домене Active Directory, и только после этого он может подключиться к ОО, используя средства

проверки подлинности операционной системы или ОО. При попытке недоверенного подключения (non-trusted connection) с использованием сетевых библиотек Named Pipes и Multiprotocol в подключении к ОО будет отказано. Для этой цели должна быть использована сетевая библиотека TCP/IP Sockets. Пользователь (или приложение) может попытаться подключиться к ОО, используя сетевой протокол TCP/IP и библиотеку TCP/IP Sockets, с любого компьютера, который может установить соединение с ОО.

Делегирование учетной записи пользователя

Объект оценки обеспечивает поддержку механизма делегирования учетной записи пользователя, предоставляющего ОО возможность использовать регистрационные данные пользователя для предоставления ему доступа к защищаемы активам, не относящимся к данному ОО. Благодаря поддержке механизма делегирования, доступ к активам предоставляется по имени и паролю прошедшего проверку подлинности пользователя, а не системной или доменной учетной записи, используемой для запуска служб ОО. Возможность делегирования учетной записи пользователя обеспечивается за счет полноценной поддержки ОО протокола аутентификации Kerberos v5.0 (основной протокол аутентификации, используемый в сетях построенных на базе службы каталогов Microsoft Active Directory. Его можно использовать для интерактивного входа по паролю или смарт-карте).

6.1.3.3 База данных регистрационных записей пользователей ОО

Описание регистрационных записей пользователей

Объект оценки поддерживает базу данных, в которой полностью определены регистрационные записи пользователей, имеющих доступ к ОО (база данных регистрационных записей пользователей представлена содержимым системного представления `sys.server_principals`). Каждая учетная запись представлена в данной базе следующим набором атрибутов (см. таблицу 6.6).

Таблица 6.6.

Имя столбца	Тип данных	Описание
name	**sysname**	Имя регистрационной записи пользователя (имя входа). Данное имя уникально в пределах сервера БД.

Имя столбца	Тип данных	Описание
principal_id	**int**	Идентификатор субъекта доступа. Идентификатор уникален в пределах сервера БД.
sid	**varbinary(85)**	Идентификатор безопасности SID учетной записи пользователя SQL Server. В случае сопоставления регистрационной записи (имени входа) с учетной записью пользователя (или группы безопасности) Windows соответствует идентификатору безопасности SID, определяемому ОС Windows.
type	**char(1)**	Тип субъекта доступа: S = учетная запись SQL; U = учетная запись пользователя Windows; G = группа безопасности Windows; R = серверная роль; C = имя входа, сопоставленное сертификату; K = имя входа, сопоставленное асимметричному ключу.
type_desc	**nvarchar(60)**	Описание типа субъекта доступа: SQL_LOGIN WINDOWS_LOGIN WINDOWS_GROUP SERVER_ROLE CERTIFICATE_MAPPED_LOGIN ASYMMETRIC_KEY_MAPPED_LOGIN
is_disabled	**int**	1 = регистрационная запись запрещена.
create_date	**datetime**	Время создания регистрационной записи пользователя.
modify_date	**datetime**	Время последнего изменения регистрационной записи пользователя.
default_database_name	**sysname**	Имя БД, используемой по умолчанию для подключающегося пользователя.

Имя столбца	Тип данных	Описание
default_language_name	**sysname**	Язык, используемый пользователем по умолчанию.
credential_id	**int**	Идентификатор учетных данных, связанный с регистрационной записью. Если с участником не связаны никакие учетные данные, идентификатор **credential_id** будет иметь значение NULL.

Сопоставление с ФТБ

Функции безопасности «Идентификация и аутентификация» удовлетворяют следующим функциональным требованиям безопасности:

- FIA_AFL.1 (1) – ФБО обнаруживают, когда происходит установленное администратором ОО число (не более 10) неуспешных попыток аутентификации с момента последней успешной попытки аутентификации пользователя, при достижении установленного числа неуспешных попыток аутентификации ФБО осуществляют блокировку регистрационной записи пользователя ОО;
- FIA_AFL.1 (2) – функции безопасности среды ИТ обнаруживают, когда происходит установленное администратором ОС число (не более 10) неуспешных попыток аутентификации с момента последней успешной попытки аутентификации пользователя, при достижении установленного числа неуспешных попыток аутентификации функции безопасности среды ИТ осуществляют блокировку регистрационной записи пользователя ОО на 30 минут;
- FIA_ATD.1 – ФБО поддерживают базу данных регистрационных и учетных записей пользователей, в которой определены поддерживаемые для пользователей ОО атрибуты безопасности: идентификатор регистрационной записи пользователя, идентификатор учетной записи пользователя и принадлежность к роли;
- FIA_SOS.1 – функции безопасности среды ИТ предоставляют механизм для верификации качества паролей на доступ к ОО;

- FIA_UAU.2 (1) – ФБО обеспечивают аутентификацию до любых действий субъектов доступа к ОО и объектам ОО;
- FIA_UAU.2 (2) – функции безопасности среды ИТ обеспечивают аутентификацию до любых действий субъектов доступа к ОО и объектам ОО;
- FIA_UID.2 – ФБО осуществляют идентификацию субъектов доступа к ОО и объектам ОО до разрешения любого действия, выполняемого при посредничестве ФБО от имени этого субъекта доступа;
- FIA_USB.1 – ФБО осуществляют ассоциирование соответствующих атрибутов безопасности субъекта доступа с субъектами, действующими от имени этого субъекта доступа.

6.1.4 Функции безопасности «Управление безопасностью»

Объект оценки обеспечивает возможность управления ролями, а также предоставляет определенный набор функций управления различными политиками и характеристиками безопасности.

6.1.4.1 Роли

Представление ролей в рамках ОО реализовано через механизм назначения учетной записи пользователя полномочий посредством включение ее в состав предопределенных фиксированных ролей сервера БД (fixed server role), фиксированных ролей БД (fixed database role) или ролей БД, определяемых пользователем (user-defined database role). При осуществлении доступа к ОО пользователю присваивается определенная роль, для которой определено членство и установлены соответствующие полномочия. Несмотря на то, что в ОО могут быть определены различные роли, фактически рассматриваются две логические роли: уполномоченного администратора и уполномоченного пользователя.

Роль администратора может быть представлена любой учетной записью, для которой назначены соответствующие полномочия (например, право создания, изменения и удаления любой БД и ее объектов). Полномочия на выполнение требуемых действий для указанной учетной записи пользователя могут быть назначены напрямую посредством инструкций языка DDL (Transact-SQL) либо посредством добавления данной учетной записи в одну из нескольких предустановленных ролей, например, предопределенную фиксированную роль сервера «Server Administrators». Пользователю будут даны

полномочия уполномоченного администратора только в том случае, если он зарегистрируется под учетной записью, для которой определены соответствующие полномочия, или которая является участником соответствующей предопределенной роли сервера или фиксированной роли БД.

Объект оценки поддерживает ряд предопределенных фиксированных ролей сервера БД, создаваемых в момент установки. Членство в данных ролях предоставляет право выполнять ряд административных и системных задач, таких как управление файлами и устройствами резервного копирования, установка и изменение параметров конфигурации удаленных и связанных серверов, изменение параметров сервера БД и т.д. В таблице 6.7 перечислены предопределенные роли сервера БД и представлено описание их возможностей.

Таблица 6.7 – Возможности предопределенных фиксированных ролей сервера БД

№ п/п	Роль сервера	Функциональные возможности
1.	Sysadmin (System administrators)	Участники данной предопределенной роли могут выполнять любые административные задачи при управлении сервером БД, а также в любой базе данных. По умолчанию участниками данной роли является встроенная учетная запись администратора ОО «sa», а также все участники локальной группы безопасности Windows «BUILTIN\Администраторы». Участникам данной роли предоставлены следующие разрешения на уровне сервера БД: CONTROL SERVER.
2.	Serveradmin (Server administrators)	Участники данной предопределенной роли могут выполнять любые операции по конфигурированию ОО с помощью системной хранимой процедуры sp_configure, а также управлять службами ОО. Участникам данной роли предоставлены следующие разрешения на уровне сервера БД: ALTER ANY ENDPOINT, ALTER RESOURCES, ALTER SERVER STATE, ALTER SETTINGS,

№ п/п	Роль сервера	Функциональные возможности
		SHUTDOWN, VIEW SERVER STATE.
3.	Setupadmin (Setup administrators)	Участники данной предопределенной роли могут устанавливать и изменять параметры конфигурации удаленных и связанных серверов, а также параметры репликации. Кроме того, участники данной роли могут включать некоторые хранимые процедуры в число процедур, выполняемых при запуске системы. Участникам данной роли предоставлены следующие разрешения на уровне сервера БД: ALTER ANY LINKED SERVER.
4.	Securityadmin (Security administrators)	Участники данной предопределенной роли могут выполнять все операции, связанные с безопасностью, включая управление разрешениями на использование оператора CREATE DATABASE, контроль над учетными записями сервера БД и чтение журнала ошибок ОО. Члены фиксированной роли сервера БД **securityadmin** могут предоставлять разрешения как на уровне сервера, так и на уровне базы данных. Участникам данной роли предоставлены следующие разрешения на уровне сервера БД: ALTER ANY LOGIN.
5.	Processadmin (Process administrators)	Участники данной предопределенной роли могут управлять процессами в системе, удалять пользовательские процессы, применяющие некорректные запросы. Участникам данной роли предоставлены следующие разрешения на уровне сервера БД: ALTER ANY CONNECTION, ALTER SERVER STATE.

№ п/п	Роль сервера	Функциональные возможности
6.	Dbcreator (Database creators)	Участники данной предопределенной роли могут выполнять операции создания, изменения и удаления БД. Участникам данной роли предоставлены следующие разрешения на уровне сервера БД: CREATE DATABASE.
7.	Diskadmin (Disk administrators)	Участники данной предопределенной роли могут управлять файлами и устройствами резервного копирования. Участникам данной роли предоставлены следующие разрешения на уровне сервера БД: ALTER RESOURCES.
8.	Bulkadmin (Bulk insert administrators)	Участники данной предопределенной роли могут выполнять операторы BULK INSERT. Данная роль также позволяет участникам роли sysadmin распределять задачи копирования, не наделяя их правами роли sysadmin. Участникам данной роли предоставлены следующие разрешения на уровне сервера БД: ADMINISTER BULK OPERATIONS.

Помимо предопределенных фиксированных ролей сервера БД в ОО создаются фиксированные роли БД, для которых предопределены полномочия для работы с БД. Каждая БД в ОО содержит девять фиксированных ролей, связанных с разрешениями, определяемыми на уровне БД. Данные роли не могут быть удалены, для них также не могут быть переопределены их полномочия. В таблице 6.8 перечислены фиксированные роли БД и описаны их возможности.

Таблица 6.8 – Возможности фиксированных ролей БД

№ п/п	Роль БД	Функциональные возможности
1.	db_owner	Участники данной фиксированной роли могут выполнять все действия по конфигурации и обслуживанию базы данных. члены данной роли базы могут также удалять БД.
2.	db_accessadmin	Участники данной фиксированной роли могут добавлять или удалять права удаленного доступа для пользователей и групп безопасности Windows, а также пользователей SQL Server.
3.	db_securityadmin	Участники данной фиксированной роли могут управлять разрешениями, членством в ролях, записями участников ролей и владельцев объектов в БД с использованием операторов GRANT, REVOKE и DENY.
4.	db_ddladmin	Участники данной фиксированной роли могут добавлять, изменять и удалять объекты в БД, выполняя любые команды языка определения данных (DDL) в базе данных.
5.	db_backupoperator	Участники данной фиксированной роли могут выполнять консольные команды DBCC, инициировать процесс фиксации транзакций, создавать резервные копии, используя операторы DBCC, операторы CHECKPOINT и BACKUP языка Transact-SQL.
6.	db_datareader	Участникам данной фиксированной роли предоставлены разрешения на считывание данных из всех пользовательских таблиц и представлений в БД. Для выполнения указанных действий данным пользователям предоставлено право выполнение оператора SELECT.

№ п/п	Роль БД	Функциональные возможности
7.	db_datawriter	Участники данной фиксированной роли могут добавлять, изменять или удалять данные из всех пользовательских таблиц и представлений в БД. Для выполнения указанных действий данным пользователям предоставлено право выполнения операторов INSERT, UPDATE и DELETE.
8.	db_denydatareader	Участникам данной фиксированной роли запрещено считывать данные из всех пользовательских таблиц и представлений в БД.
9.	db_denydatawriter	Участники данной фиксированной роли не могут изменять или удалять данные из пользовательских таблиц в БД.

Любой пользователь, осуществивший вход в ОО и не являющийся участником какой-либо из фиксированных ролей БД, рассматривается как участник системной роли `public`, которая существует к каждой БД. Участниками роли `public` автоматически являются все пользователи, которым разрешен доступ к БД. Данная роль обладает минимальным набором полномочий, достаточным для работы с БД и ее объектами.

6.1.4.2 Функции управления безопасностью

Объект оценки поддерживает набор политик и характеристик безопасности, которые требуют соответствующего управления. За некоторым исключением, функции по управлению безопасностью предоставлены только уполномоченному администратору. Данное ограничение реализуется через использование ролей и механизмов управления доступом. ОО поддерживает функции управления безопасностью для следующих политик и характеристик безопасности:

Политика аудита – функции управления политикой аудита предоставляют уполномоченным администраторам возможность разрешать или запрещать аудит событий безопасности, выполнять настройку классов событий безопасности, которые будут подвергнуты аудиту, управлять размером журнала регистрации событий аудита.

Политика аутентификации – функции управления политикой аутентификации предоставляют уполномоченному администратору возможность определять, каким образом будет осуществляться проверка подлинности пользователей при доступе к ОО, а также определять необходимость соответствия аутентификационной информации метрикам качества.

Политика назначения разрешений пользователя на доступ к ОО – функции управления политикой назначения разрешений пользователя на доступ к ОО позволяют уполномоченному администратору управлять (назначать или запрещать) доступом пользователей к ОО, а также базой данных регистрационных записей пользователей.

Политика назначения разрешений пользователя на доступ к БД – функции управления политикой назначения разрешений пользователя позволяют уполномоченному администратору управлять базой данных учетных записей пользователей БД, а также назначать или отзывать для конкретных учетных записей пользователей БД разрешения на доступ к БД и их объектам и разрешения на выполнение определенных инструкций языка DDL (Transact-SQL).

Тестирование оборудования и ФБО – функции управления тестированием оборудования и ФБО позволяют уполномоченному администратору определять условия тестирования.

Использование ресурсов – функции управления использованием ресурсов позволяют уполномоченному администратору управлять размером дискового пространства, доступного для БД, и объемом выделяемой для ОО физической памяти.

Сопоставление с ФТБ

Функции безопасности «Управление безопасностью» удовлетворяют следующим функциональным требованиям безопасности:

- FMT_MOF.1 – ФБО предоставляют возможность определять и модифицировать режим выполнения аудита и аутентификации субъектов доступа только администратору ОО;
- FMT_MSA.1 – ФБО предоставляют возможность модифицировать и удалять атрибуты безопасности, используемые при реализации политики дискреционного управления доступом, только администратору ОО;
- FMT_MSA.3 – ФБО обеспечивают ограничительные значения по умолчанию для атрибутов безопасности, которые используются для осуществления

политики дискреционного управления доступом и возможность для администратора ОО и пользователя ОО, являющегося владельцем объекта, определять альтернативные значения для отмены значений по умолчанию;

- FMT_MTD.1 – ФБО предоставляют возможность выполнять операции над данными ФБО согласно таблице 5.3 только уполномоченному администратору ОО;
- FMT_REV.1 (1) – ФБО предоставляют возможность отмены атрибутов безопасности, ассоциированных с пользователями ОО и объектами, только уполномоченному администратору ОО и осуществляют правила отмены полномочий у пользователей ОО на доступ к объектам, а также отмены прав доступа к объекту (модификацию списка дискреционного доступа);
- FMT_REV.1 (2) – ФБО предоставляют возможность отмены атрибутов безопасности, ассоциированных с объектами, только пользователю ОО, являющемуся владельцем объекта, и осуществляют правила отмены полномочий у пользователей ОО на доступ к объектам, а также отмены прав доступа к объекту (модификацию списка дискреционного доступа);
- FMT_SMR.1 – ОО поддерживает ролевую модель, определяя роль администратора ОО и пользователя ОО.

6.1.5 Функции безопасности «Защита ФБО»

Функции безопасности ОО «Защита ФБО» обеспечивают:

- целостность ФБО;
- отделение домена;
- службу времени.

6.1.5.1 Целостность ФБО

Аппаратная платформа, обеспечивающая функционирование ОО, протестирована с целью определения поддержки функций безопасности. Тесты были направлены на определение правильности функционирования системной платы, а также периферийных устройств, таких как модули памяти, жесткий магнитный диск, видеоадаптер, порты I/O (ввода/вывода). Данные тесты были разработаны, чтобы убедиться в корректной реализации тех возможностей, которые положены в основы функций безопасности (например, обработка прерываний, управление памятью, управление заданиями и т.д.).

6.1.5.2 Отделение домена

Объект оценки обеспечивают изоляцию процессов и поддерживают домен безопасности для собственного безопасного выполнения. Домены безопасности состоят из следующих компонентов:

- аппаратных средств;
- доверенных процессов пользовательского режима;
- инструментальных средств администрирования процессов пользовательского режима.

Управление аппаратными средствами ФБО осуществляется программным обеспечением режима ядра операционной системы, под управлением которой функционирует ОО. Аппаратные средства ФБО не могут быть модифицированы недоверенными субъектами. Защита программного обеспечения ФБО режима ядра от модификации обеспечивается посредством контроля состояния функционирования аппаратных средств и защитой памяти. Аппаратные средства обеспечивают инструкции, генерирующие программные прерывания, позволяющие переходить из состояния режима пользователя в состояние режима ядра. Программное обеспечение режима ядра осуществляет обработку всех прерываний и определяет обоснованность сделанных вызовов в режиме ядра. Механизм защиты памяти реализован таким образом, что напрямую обращаться к памяти могут только компоненты в режиме ядра. Прямое взаимодействие с памятью внешних подсистем и приложений пользовательского режима невозможно.

Среда функционирования (операционная система) обеспечивает изоляцию всех процессов пользовательского режима посредством контекста выполнения, контекста безопасности и ограничения выделенного им адресного пространства (использование механизма виртуального адресного пространства). Структура данных, определяемая адресным пространством процесса, контекстом выполнения и контекстом безопасности, храниться в защищенной памяти режима ядра.

Инструментальные средства администрирования ОО реализуют функции управления в контексте безопасности процесса, запущенного от имени уполномоченного администратора. Процессы, выполняемые в контексте учетной записи администратора, защищены таким же образом, как и другие процессы пользовательского режима, т.е. через изоляцию посредством виртуального адресного пространства.

Пользовательские процессы также исполняются в собственном виртуальном адресном пространстве, что, собственно, обеспечивает их защищенность друг от друга.

6.1.5.3 Служба времени

Поддерживаемая ОО аппаратная платформа включает контроллер часов реального времени, представляющий устройство, доступ к которому может быть возможен только через функции, предоставляемые средой функционирования (операционной системой) ОО. В частности, среда функционирования обеспечивает функции, которые позволяют пользователям, включая сам ОО, запрашивать время, а также возможность синхронизации времени с внешним источником времени. Возможность запроса времени ничем не ограничена, в то время как изменение системного времени требует полномочий на выполнение данной операции. Данная привилегия предоставлена только уполномоченным администраторам операционной системы с целью обеспечения непротиворечивости службы времени.

Сопоставление с ФТБ

Функции безопасности «Защита ФБО» удовлетворяют следующим функциональным требованиям безопасности:

- FPT_RVM.1 (1) – ФБО обеспечить, чтобы функции, осуществляющие ПБО, вызывались и успешно выполнялись прежде, чем разрешается выполнение любой другой функции в пределах ОДФ;
- FPT_SEP.1 (1) – ФБО обеспечить поддержание домена безопасности для собственного выполнения, защищающего их от вмешательства и искажения недоверенными субъектами;
- FPT_RVM.1 (2) – функции безопасности среды ИТ обеспечивают, чтобы функции, осуществляющие ПБО, вызывались и успешно выполнялись прежде, чем разрешается выполнение любой другой функции в пределах ОДФ;
- FPT_SEP.1 (2) – функции безопасности среды ИТ обеспечивают поддержание домена безопасности для собственного выполнения, защищающего их от вмешательства и искажения недоверенными субъектами;
- FPT_STM.1 – функции безопасности среды ИТ предоставляют надежные метки времени для использования ФБО.

6.1.6 Функции безопасности ОО «Управление доступом к ОО»

Функции безопасности ОО «Управление доступом к ОО» обеспечивают:

- возможность ограничения открытия сеанса доступа на основе идентификатора регистрационной записи пользователя;
- возможность ограничения количества одновременно открытых сеансов доступа к ОО.

6.1.6.1 Ограничения на открытие сеанса доступа на основе идентификатора регистрационной записи пользователя

При обращении пользователя к ОО ФБО осуществляют проверку разрешений на подключение данного субъекта доступа. Проверка осуществляется на основе идентификатора регистрационной записи пользователя (имени входа), для которого администратором определены разрешающие или запрещающие права доступа к ОО. При этом идентификатор регистрационной записи пользователя может быть сопоставлен как с учетной записью пользователя операционной системы, так и с учетной записью пользователя ОО (SQL Server).

Для идентификации пользователя Windows, осуществляющего доступ к ОО, используется предъявляемый им билет Kerberos (Kerberos ticket), представляющий собой персональное электронное «удостоверение» пользователя. В последующем, ОО извлекает из билета Kerberos идентификаторы безопасности SID, однозначно идентифицирующие пользователя и группы безопасности Windows, участниками которых он является, и проверяет их наличие в системном представлении `sys.server_principals` базы данных `master`. Если в данном представлении существуют записи, содержащие идентификаторы, совпадающие с идентификаторами SID, извлеченными из билета Kerberos, ОО определяет возможность доступ субъекта к экземпляру SQL Server.

В случае если для регистрационной записи пользователя определены запрещающие права доступа либо пользователь не имеет действительной регистрационной записи в ОО, в доступе к ОО будет отказано.

6.1.6.2 Ограничение на количество одновременно открытых сеансов доступа к ОО

Объект оценки обеспечивает управление параметрами клиентских соединений, определяя число пользователей, которые могут одновременно подключаться к ОО. По умолчанию количество параллельных пользовательских соединений устанавливается

автоматически и изменяется динамически. Если в системе зарегистрировано 10 пользователей, то существует 10 установленных пользовательских соединений. При регистрации в системе еще одного пользователя, автоматически будет создано еще одно пользовательское соединение и так вплоть до разрешенного максимального количества этих соединений. Максимальное количество пользовательских соединений, поддерживаемых ОО, составляет 32767. В случае превышения указанного количества соединений система выдаст сообщение об ошибке и в создании нового подключения пользователем будет отказано.

Сопоставление с ФТБ

Функции безопасности «Управление доступом к ОО» удовлетворяют следующему функциональному требованию безопасности:

- FTA_TSE.1 – ФБО способны отказать в открытии сеанса доступа к ОО пользователю с указанным администратором ОО идентификатором регистрационной записи, а также всем субъектам доступа в случае превышения установленного администратором ОО количества открытых сеансов доступа к ОО.

6.1.7 Функции безопасности ОО «Использование ресурсов ОО»

Функции безопасности ОО «Использование ресурсов ОО» обеспечивают:

- управление размером доступного для БД дискового пространства;
- управление объемом выделяемой ОО физической памяти.

6.1.7.1 Управление размером доступного для БД дискового пространства

В ОО предусмотрен ряд механизмов управления размером БД, предоставляющих возможность ограничивать объем доступного для БД дискового пространства.

При создании пользовательской БД по умолчанию выбирается автоматическое увеличение размера файлов данных и файлов журналов транзакций при их заполнении, что приводит к существенному снижению производительности системы и неконтролируемому росту указанных файлов. При каждом увеличении размера файла нагрузка на систему существенно возрастает. Кроме того, частое увеличение дискового пространства, выделенного для файлов БД, приводит к дефрагментации диска, особенно при его совместном использовании другими прикладными программами.

Размер файлов БД можно не только автоматически увеличивать, но и уменьшать. Уполномоченный администратор может устанавливать параметры пользовательской БД таким образом, чтобы её размер автоматически уменьшался, если в файле данных или файле журнала транзакций будет много свободного дискового пространства. По умолчанию автоматическое уменьшение размера БД не используется. Как и в случае автоматического увеличения размера файлов БД, при использовании возможности автоматического уменьшения размера файлов БД производительность системы может существенно снизиться.

Устанавливаемый по умолчанию для файлов данных и файлов журналов транзакций минимальный размер равен 1 Mb (space allocated – 1Mb), максимальный размер файлов неограничен (maximum file size – unrestricted file growth), величина приращения файлов – 10% от общего объема файла (file growth – by percent 10).

Чтобы контролировать рост файлов БД и объем свободного дискового пространства, ОО предоставляет возможность ограничивать объем доступного для БД дискового пространства, что исключает неограниченное увеличение ее размера. При этом предельный размер выделяемой квоты может быть установлен для файлов данных и файлов журнала транзакций БД. Уполномоченному администратору предоставлена возможность управления минимальным и максимальным размером, величиной приращения и параметром автоматического увеличения размера для каждого (основного и дополнительного) файла данных и файла журнала транзакций БД.

6.1.7.2 Управление объемом выделяемой ОО физической памяти

Функции безопасности ОО обеспечивают статическое или динамическое управление объемом физической памяти, используемой ОО в качестве буферного пула.

При использовании динамического управления ОО автоматически распределяет и освобождает память для обеспечения повышенной производительности. Если вся доступная физическая память уже передана какому-либо серверному приложению, ОО выполняет перераспределение памяти между приложениями. По умолчанию физическая память распределяется ОО динамически.

Объект оценки позволяет администратору ОО изменять параметры конфигурации памяти таким образом, чтобы ОО мог использовать фиксированный либо динамически изменяемый объем физической памяти. Кроме того, уполномоченному администратору ОО предоставлена возможность управления минимальным и максимальным размером

памяти, используемым ОО для буферного пула, а также дополнительным объемом физической памяти, позволяющим резервировать заданный объем памяти от распределения между другими приложениями.

Сопоставление с ФТБ

Функции безопасности «Управление доступом к ОО» удовлетворяют следующему функциональному требованию безопасности:

- FRU_RSA.2 (1) – ФБО обеспечиваю возможность реализации минимальных и максимальных квот для объема физической памяти, который ОО может использовать в процессе функционирования;
- FRU_RSA.2 (2) – ФБО обеспечиваю возможность реализации минимальных и максимальных квот для объема дискового пространства, который базы данных могут использовать одновременно.

6.2 Меры доверия к безопасности ОО

Для удовлетворения требований доверия к безопасности согласно ОУД1, усиленному компонентом AVA_SOF.1 (Оценка стойкости функции безопасности), применены следующие меры доверия к безопасности ОО:

- управление конфигурацией;
- предоставление руководств;
- предоставление проектной документации;
- тестирование;
- оценка стойкости функций безопасности.

6.2.1 Управление конфигурацией

Меры управления конфигурацией, применяемые корпорацией Microsoft®, обеспечивают уникальную идентификацию версий ОО.

Корпорация Microsoft® осуществляет уникальную маркировку ОО, позволяющую отличать разные версии ОО. Это достигается маркированием упаковки, носителей. Кроме того, ОО может отображать свое название и номер версии при запуске программы или в ответ на запрос через командную строку или графический интерфейс.

Корпорация Microsoft® использует многократную маркировку ОО – к названию и номеру версии добавляются номера пакетов исправлений и пакетов обновлений; при этом

применяемые корпорацией Microsoft® меры управления конфигурацией обеспечивают согласованность меток вследствие непересечения областей значения меток.

Корпорация Microsoft® применяет меры управления конфигурацией, связывающие маркированные руководства, поставляемые в составе ОО, с данным ОО.

Сопоставление с ТДБ

Меры доверия, связанные с управлением конфигурацией, удовлетворяют следующему требованию доверия:

– ACM_CAP.1.

6.2.2 Представление руководств

Корпорация Microsoft® предоставляет руководства безопасной установки, генерации и запуска. В процедурах установки, генерации и запуска описаны шаги, необходимые для получения безопасной конфигурации ОО, описанной в ЗБ.

Корпорация Microsoft® предоставляет руководства администратора и пользователя, в которых описываются действия по выполнению функций безопасности ОО и приводятся предупреждения уполномоченным администраторам и пользователям о действиях, которые могут скомпрометировать безопасность ОО.

Сопоставление с ТДБ

Меры доверия, связанные с представлением руководств, удовлетворяют следующим требованиям доверия:

– ADO_IGS.1;
– AGD_ADM.1;
– AGD_USR.1.

6.2.3 Представление проектной документации

Проектная документация ОО, предоставляемая на оценку, включает функциональную спецификацию. Функциональная спецификация является неформальной.

В функциональной спецификации определены все внешние (то есть, видимые для пользователя или администратора) интерфейсы функций безопасности ОО, описаны режимы функционирования ОО на каждом внешнем интерфейсе, включая описание результатов, нештатных ситуаций и сообщений об ошибках.

Материалы анализа соответствия между краткой спецификацией ОО и функциональной спецификацией направлены на отображения соответствия функций безопасности, представленных в функциональной спецификации, функциям безопасности, идентифицированным в краткой спецификации.

Сопоставление с ТДБ

Меры доверия, связанные с представлением проектной документации, удовлетворяют следующим требованиям доверия:

– ADV_FSP.1;
– ADV_RCR.1.

6.2.4 Тестирование

Корпорация Microsoft® предоставляет ОО, пригодный для тестирования, с соответствующей документацией, это позволяет провести независимое тестирование ФБО и сделать заключение, выполняются ли ФБО в соответствии со спецификациями.

Сопоставление с ТДБ

Меры доверия, связанные с тестированием, удовлетворяют требованию доверия:

– ATE_IND.1.

6.2.5 Оценка стойкости функций безопасности

Для механизма парольной защиты, являющегося вероятностным, предоставляется материал анализа стойкости функции безопасности (аутентификации). Анализ стойкости функции безопасности представлен в документе «Материалы анализа стойкости функций безопасности системы управления базами данных Microsoft® SQL Server™ 2005 Standard Edition».

Сопоставление с ТДБ

Меры доверия, связанные с оценкой стойкости функций безопасности, удовлетворяют следующему требованию доверия:

– AVA_SOF.1.

7 Утверждения о соответствии ПЗ

В данном разделе излагается утверждение о соответствии ОО конкретному профилю защиты и приводится обоснование этих утверждений.

7.1 Ссылка на ПЗ

Объект оценки соответствует профилю защиты СУБД.СУБД_МП.ПЗ «Безопасность информационных технологий. Системы управления базами данных. Системы управления базами данных масштаба предприятия. Профиль защиты. Версия 1.0, 2005». Данное утверждение о соответствии подразумевает, что ОО отвечает всем требованиям ПЗ.

7.2 Конкретизация ПЗ

Все требования безопасности, сформулированные в ПЗ СУБД.СУБД_МП.ПЗ «Безопасность информационных технологий. Системы управления базами данных. Системы управления базами данных масштаба предприятия. Профиль защиты. Версия 1.0, 2005», включены в настоящее ЗБ. Некоторые из них были подвергнуты дальнейшей конкретизации.

Профиль защиты СУБД.СУБД_МП.ПЗ «Безопасность информационных технологий. Системы управления базами данных. Системы управления базами данных масштаба предприятия. Профиль защиты. Версия 1.0, 2005» содержит ряд функциональных требований, операции над которыми при разработке ЗБ нуждались в завершении. Эти операции завершены в настоящем ЗБ в полном объеме (см. таблицу 7.1 – компоненты требований с пометкой «завершено»).

Кроме того, исходя из особенностей рассматриваемого ОО, по отношению к ряду функциональных требований, взятых из ПЗ, в настоящем ЗБ была применена операция уточнения (см. таблицу 7.1 – компоненты требований с пометкой «уточнено»).

Функциональные требования, операции над которыми были завершены, а также требования, уточненные в ЗБ относительно ПЗ, приведены в таблице 7.1.

Таблица 7.1 – Конкретизация функциональных требований по отношению к ПЗ СУБД.СУБД_МП.ПЗ «Безопасность информационных технологий. Системы управления базами данных. Системы управления базами данных масштаба предприятия. Профиль защиты. Версия 1.0, 2005»

Наименование требования	Изменение
Функциональные требования ОО	
FAU_GEN.1	завершено уточнено
FAU_GEN.2	уточнено
FAU_SAR.3	завершено уточнено
FAU_SEL.1	завершено уточнено
FAU_STG.3	завершено
FAU_STG.4	завершено
FDP_ACC.1	завершено
FDP_ACF.1	завершено уточнено
FIA_ATD.1	завершено уточнено
FIA_UID.2	уточнено
FMT_MOF.1	завершено
FMT_MSA.1	завершено
FMT_MSA.3	завершено
FMT_MTD.1	завершено уточнено
FMT_REV.1 (1)	завершено
FMT_REV.1 (2)	завершено
FMT_SMR.1	завершено

Наименование требования	Изменение
FTA_TSE.1	завершено уточнено
Функциональные требования среды ИТ	
FIA_AFL.1	завершено
FIA_SOS.1	завершено
FIA_UAU.2	уточнено

7.3 Дополнение ПЗ

В настоящее ЗБ включена следующая дополнительная угроза, которой противостоит ОО, не вошедшая в ПЗ СУБД.СУБД_МП.ПЗ «Безопасность информационных технологий. Системы управления базами данных. Системы управления базами данных масштаба предприятия. Профиль защиты. Версия 1.0, 2005»:

T.UnauthExecProc&Fanc

1. Аннотация угрозы – выполнение хранимых процедур и определяемых функций неуполномоченными на это пользователями ОО.

2. Источники угрозы – пользователи ОО.

3. Способ реализации угрозы – осуществление доступа к хранимым процедурам и определяемым функциям с использованием приложений, поддерживающих возможность взаимодействия с ОО, и запуск их на выполнение.

4. Используемые уязвимости – недостатки механизмов разграничения доступа к объектам ОО, связанные с возможностью выполнения хранимых процедур и определяемых функций неуполномоченным на это пользователям ОО.

5. Вид активов, потенциально подверженных угрозе – хранимые процедуры и определяемые функции.

6. Нарушаемое свойство безопасности активов – несанкционированное выполнение.

7. Возможные последствия реализации угрозы – несанкционированное ознакомление с информацией, выдаваемой после отработки хранимых процедур и функций; нарушение режимов функционирования ОО и БД.

В настоящее ЗБ включены следующие дополнительные политики безопасности организации, не вошедшие в ПЗ СУБД.СУБД_МП.ПЗ «Безопасность информационных технологий. Системы управления базами данных. Системы управления базами данных масштаба предприятия. Профиль защиты. Версия 1.0, 2005»:

P.Resourse

Для уполномоченного администратора ОО должна быть обеспечена возможность управления надлежащим распределением ресурсов ОО.

P.TOEAuth

Должна обеспечиваться аутентификация субъектов, осуществляющих попытку доступа к ОО с рабочих станций и серверов под управлением ОС, не имеющих совместно с ОС (являющейся средой функционирования ОО) централизованного управления параметрами безопасности, механизмами самого ОО.

P.ManageAuthData

В случае аутентификации субъектов, осуществляющих попытку доступа к ОО, с использованием механизмов самого ОО, операционная система должна предоставлять механизмы управления качеством аутентификационных данных, обеспечивающие адекватную защиту ОО от прямого или умышленного нарушения безопасности нарушителями с умеренным потенциалом нападения.

В настоящее ЗБ включены следующие дополнительные цели безопасности для ОО, не вошедшие в ПЗ СУБД.СУБД_МП.ПЗ «Безопасность информационных технологий. Системы управления базами данных. Системы управления базами данных масштаба предприятия. Профиль защиты. Версия 1.0, 2005»:

O.TOEAuth

Аутентификация с использованием механизмов ОО

ОО должен обеспечивать аутентификацию субъектов, осуществляющих попытку доступа к ОО с рабочих станций и серверов под управлением ОС, не имеющих совместно с ОС (являющейся средой функционирования ОО) централизованного управления параметрами безопасности.

O.DistrResourse

Распределение ресурсов ОО

ОО должен обеспечивать для уполномоченного администратора ОО возможность надлежащего распределения ресурсов ОО.

В настоящее ЗБ включена следующая дополнительная цель безопасности для среды, не вошедшая в ПЗ СУБД.СУБД_МП.ПЗ «Безопасность информационных технологий. Системы управления базами данных. Системы управления базами данных масштаба предприятия. Профиль защиты. Версия 1.0, 2005»:

OE.ManageAuthData

Управление качеством аутентификационных данных

В случае аутентификации субъектов, осуществляющих попытку доступа к ОО, с использованием механизмов самого ОО, операционная система должна предоставлять механизмы управления качеством аутентификационных данных, обеспечивающие адекватную защиту ОО от прямого или умышленного нарушения безопасности нарушителями с умеренным потенциалом нападения.

В настоящее ЗБ включены следующие дополнительные функциональные требования безопасности ОО, не вошедшие в ПЗ СУБД.СУБД_МП.ПЗ «Безопасность информационных технологий. Системы управления базами данных. Системы управления базами данных масштаба предприятия. Профиль защиты. Версия 1.0, 2005»:

- **FIA_AFL.1 (1)** (Обработка отказов аутентификации);
- **FIA_UAU.2 (1)** (Аутентификация до любых действий пользователя);
- **FRU_RSA.2 (1)** (Минимальные и максимальные квоты);
- **FRU_RSA.2 (2)** (Минимальные и максимальные квоты).

8 Обоснование

В данном разделе дано обоснование целей безопасности, определенных в разделе 4, и требований безопасности, определенных в разделе 5 настоящего ЗБ. В разделе «Обоснование» также демонстрируется справедливость утверждений о СФБ и соответствии ПЗ.

8.1 Обоснование целей безопасности

8.1.1 Обоснование целей безопасности для ОО

В таблице 8.1 приведено отображение целей безопасности для ОО на угрозы и политику безопасности организации.

Таблица 8.1 – Отображение целей безопасности на угрозы и политику безопасности организации

	O.AccessObject	O.AccessTOE	O.TOEAuth	O.AuditEvents	O.ProtectAudit	O.AdminManage	O.ProtectResTSF	O.DistrResourse
T.UnauthAccessData	X							
T.UnauthExecProc&Fanc	X							
T.UnauthAccessTOE		X						
T.MasqAdmin&User		X						
T.UnauthAccessAuditData					X			
T.LostAuditDataOverStg					X			
T.LostAuditDataOverDisk					X			
T.UnauthAccessTSF							X	
T.UnauthUsageRes							X	
P.Manage						X		
P.Audit				X				
P.Resourse								X
P.Access	X							

	O.AccessObject	O.AccessTOE	O.TOEAuth	O.AuditEvents	O.ProtectAudit	O.AdminManage	O.ProtectResTSF	O.DistrResourse
P.TOEAuth			**X**					

O.AccessObject

Достижение этой цели безопасности необходимо в связи с противостоянием угрозам **T.UnauthAccessData, T.UnauthExecProc&Fanc** и реализацией политики безопасности организации **P.Access**, так как обеспечивает доступ к объектам ОО только уполномоченным пользователям ОО, а также обеспечивает возможность уполномоченным пользователям ОО определять доступность объектов ОО для других пользователей ОО.

O.AccessTOE

Достижение этой цели безопасности необходимо в связи с противостоянием угрозам **T.UnauthAccessTOE** и **T.MasqAdmin&User**, так как обеспечивает доступ к ОО только уполномоченным на это пользователям.

O.TOEAuth

Достижение этой цели безопасности необходимо в связи с реализацией политики безопасности организации **P.TOEAuth**, так как обеспечивает аутентификацию субъектов, осуществляющих попытку доступа к ОО с рабочих станций и серверов под управлением ОС, не имеющих совместно с ОС (являющейся средой функционирования ОО) централизованного управления параметрами безопасности.

O.AuditEvents

Достижение этой цели безопасности необходимо в связи с реализацией политики безопасности организации **P.Audit**, так как обеспечивает наличие надлежащих механизмов регистрации и предупреждения администратора ОО о любых событиях, относящихся к безопасности ОО. Механизмы регистрации предоставляют

администраторам ОО возможность выборочного ознакомления с информацией о произошедших в ОО событиях.

O.ProtectAudit

Достижение этой цели безопасности необходимо в связи с противостоянием угрозам **T.UnauthAccessAuditData, T.LostAuditDataOverStg** и **T.LostAuditDataOverDisk**, так как обеспечивает доступ к данным аудита только уполномоченным администраторам ОО и предотвращает потерю данных аудита в случае переполнения их хранилища, а также в случае невозможности дальнейшего ведения аудита вследствие исчерпания свободного дискового пространства.

O.AdminManage

Достижение этой цели безопасности необходимо в связи с реализацией политики безопасности организации **P.Manage**, так как обеспечивает наличие надлежащих корректно функционирующих средств администрирования, доступных только уполномоченным администраторам ОО.

O.ProtectResTSF

Достижение этой цели безопасности необходимо в связи с противостоянием угрозам **T.UnauthAccessTSF** и **T.UnauthUsageRes**, так как обеспечивает защиту данных ФБО и ресурсов ОО, поддерживая домен для функционирования ФБО.

O.DistrResourse

Достижение этой цели безопасности необходимо в связи с реализацией политики безопасности организации **P.Resourse**, так как обеспечивает для уполномоченного администратора ОО возможность надлежащего распределения ресурсов ОО.

8.1.2 Обоснование целей безопасности для среды

В таблице 8.2 приведено отображение целей безопасности для среды на предположения безопасности, угрозы и политику безопасности организации.

Таблица 8.2 – Отображение целей безопасности для среды на предположения безопасности, угрозы и политику безопасности организации

	OE.ImpossibleModif	OE.Connect	OE.Peer	OE.TOEConfig	OE.OSAuth	OE.Environment	OE.ManageAuthData	OE.Locate	OE.NoEvilAdm	OE.NoEvilUser	OE.ProtectResTSF	OE.GenerateTime	OE.ProtectFileSystem	OE.RecoverySafeState
A.ImpossibleModif	X													
A.Connect		X												
A.Peer			X											
A.TOEConfig				X										
A.OSAuth					X									
A.Environment						X								
A.RecoverySafeState														X
A.Locate								X						
A.NoEvilAdm									X					
A.NoEvilUser										X				
TE.UnauthAccessTOE					X									
TE.MasqAdmin&User					X									
TE.UnauthAccessTSF											X			
TE.UnauthUsageRes											X			
TE.UnauthAccessData													X	
P.GenerateTime												X		
P.ManageAuthData							X							

OE.ImpossibleModif

Достижение этой цели безопасности необходимо в связи с реализацией предположения безопасности **A.ImpossibleModif,** так как обеспечивает отсутствие на компьютере с установленным ОО нештатных программных средств, позволяющих осуществить несанкционированную модификацию ОО.

OE.Connect

Достижение этой цели безопасности необходимо в связи с реализацией предположения безопасности **A.Connect,** так как обеспечивает осуществление доступа к ОО только из санкционированных точек доступа, размещенных в контролируемой зоне, т.е. охраняемой территории и помещении, оборудованной средствами и системами физической защиты и охраны (контроля и наблюдения) и исключающей возможность бесконтрольного пребывания посторонних лиц.

OE.Peer

Достижение этой цели безопасности необходимо в связи с реализацией предположения безопасности **A.Peer,** так как обеспечивает взаимодействие ОО только с доверенными системами ИТ, ПБО которых скоординированы с ПБО рассматриваемого ОО.

OE.TOEConfig

Достижение этой цели безопасности необходимо в связи с реализацией предположения безопасности **A.TOEConfig,** так как обеспечивает установку конфигурирование и управление ОО в соответствии с руководствами и согласно оцененным конфигурациям.

OE.OSAuth

Достижение этой цели безопасности необходимо в связи с реализацией предположения безопасности **A.OSAuth** и противостояния угрозам **TE.UnauthAccessTOE** и **TE.MasqAdmin&User,** так как обеспечивает осуществление аутентификации субъектов, осуществляющих попытку доступа к ОО, с использованием механизмов ОС, под управлением которой функционирует ОО.

OE.Environment

Достижение этой цели безопасности необходимо в связи с реализацией предположения безопасности **A.Environment,** так как обеспечивает осуществление функционирования ОО в среде функционирования (ОС), предоставляющей механизм аутентификации, обеспечивающий адекватную защиту от прямого или умышленного нарушения безопасности нарушителями с умеренным потенциалом нападения.

OE.ManageAuthData

Достижение этой цели безопасности необходимо в связи с реализацией политики безопасности организации **P.ManageAuthData,** так как в случае аутентификации субъектов, осуществляющих попытку доступа к ОО, с использованием механизмов самого ОО, обеспечивает предоставление операционной системой механизмов управления качеством аутентификационных данных, обеспечивающих адекватную защиту ОО от прямого или умышленного нарушения безопасности нарушителями с умеренным потенциалом нападения.

OE.Locate

Достижение этой цели безопасности необходимо в связи с реализацией предположения безопасности **A.Locate,** так как обеспечивает, для предотвращения несанкционированного физического доступа, размещение компьютера с установленным ОО в контролируемой зоне, т.е. охраняемой территории и помещении, оборудованной средствами и системами физической защиты и охраны (контроля и наблюдения) и исключающей возможность бесконтрольного пребывания посторонних лиц.

OE.NoEvilAdm

Достижение этой цели безопасности необходимо в связи с реализацией предположения безопасности **A.NoEvilAdm,** так как обеспечивает прохождение персоналом, ответственным за администрирование ОО, проверок на благонадежность и компетентность, а также деятельность согласно соответствующей документации.

OE.NoEvilUser

Достижение этой цели безопасности необходимо в связи с реализацией предположения безопасности **A.NoEvilUser,** так как обеспечивает прохождение уполномоченными на доступ к ОО пользователями проверок на благонадежность, а их совместные действия, направлены исключительно на выполнение своих функциональных обязанностей.

OE.ProtectResTSF

Достижение этой цели безопасности необходимо в связи с противостоянием угрозам **TE.UnauthAccessTSF** и **TE.UnauthUsageRes,** так как обеспечивает защиту данных ФБО и ресурсов ОО, а также поддержку домена для функционирования ФБО.

OE.GenerateTime

Достижение этой цели безопасности необходимо в связи с реализацией политики безопасности организации **P.GenerateTime,** так как обеспечивает поддержку средств аудита, используемых в ОО, и предоставление для них надлежащего источника меток времени.

OE.ProtectFileSystem

Достижение этой цели безопасности необходимо в связи с противостоянием угрозе **TE.UnauthAccessData,** так как обеспечивает защиту данных, размещаемых в БД, на уровне файлов файловой системы ОС от несанкционированного доступа.

OE.RecoverySafeState

Достижение этой цели безопасности необходимо в связи с реализацией предположения безопасности **A.RecoverySafeState,** так как обеспечивает выполнение мероприятий, направленных на восстановление безопасного состояния ОО в случае сбоя (отказа) программного и аппаратного обеспечения ОО.

8.2 Обоснование требований безопасности

8.2.1 Обоснование требований безопасности для ОО

8.2.1.1 Обоснование функциональных требований безопасности ОО

В таблице 8.3 представлено отображение функциональных требований безопасности ОО на цели безопасности для ОО.

Таблица 8.3 – Отображение функциональных требований безопасности для ОО на цели безопасности для ОО

	O.AccessObject	O.AccessTOE	O.TOEAuth	O.AuditEvents	O.ProtectAudit	O.AdminManage	O.ProtectResTSF	O.DistrResourse
FAU_GEN.1				X				
FAU_GEN.2				X				
FAU_SAR.1				X				
FAU_SAR.2					X			
FAU_SAR.3				X				
FAU_SEL.1				X				
FAU_STG.1					X			
FAU_STG.3					X			
FAU_STG.4					X			
FDP_ACC.1	X							
FDP_ACF.1	X							
FIA_AFL.1 (1)			X					
FIA_ATD.1	X	X		X		X		
FIA_UAU.2 (1)			X					
FIA_UID.2	X	X						
FIA_USB.1	X	X		X				
FMT_MOF.1						X		
FMT_MSA.1	X					X		

	O.AccessObject	O.AccessTOE	O.TOEAuth	O.AuditEvents	O.ProtectAudit	O.AdminManage	O.ProtectResTSF	O.DistrResourse
FMT_MSA.3	X					X		
FMT_MTD.1						X		X
FMT_REV.1 (1)						X		
FMT_REV.1 (2)	X							
FMT_SMR.1	X				X	X	X	
FPT_RVM.1 (1)							X	
FPT_SEP.1 (1)							X	
FRU_RSA.2 (1)								X
FRU_RSA.2 (2)								X
FTA_TSE.1		X						

FAU_GEN.1 Генерация данных аудита

В требованиях данного компонента выделяются данные, которые должны быть включены в записи аудита для подвергаемых аудиту событий, связанных с ОО. Рассматриваемый компонент сопоставлен с целью **O.AuditEvents** и способствует ее достижению.

FAU_GEN.2 Ассоциация идентификатора пользователя

Выполнение требований данного компонента обеспечивает возможность ассоциировать каждое событие, потенциально подвергаемое аудиту, с идентификатором учетной записи пользователя или идентификатором регистрационной записи пользователя, который был инициатором этого события. Рассматриваемый компонент сопоставлен с целью **O.AuditEvents** и способствует ее достижению.

FAU_SAR.1 Просмотр аудита

Выполнение требований данного компонента обеспечивает возможность предоставления уполномоченному администратору ОО всей информации аудита в

понятном для него виде. Рассматриваемый компонент сопоставлен с целью **O.AuditEvents** и способствует ее достижению.

FAU_SAR.2 Ограниченный просмотр аудита

Выполнение требований данного компонента обеспечивает запрет всем пользователям доступ к чтению записей аудита, за исключением уполномоченных администраторов ОО, которым явно предоставлен доступ для чтения. Рассматриваемый компонент сопоставлен с целью **O.ProtectAudit** и способствует ее достижению.

FAU_SAR.3 Выборочный просмотр аудита

Выполнение требований данного компонента обеспечивает выполнение поиска данных аудита, основанного на определенных критериях в логическом отношении «И» (наименование поля данных, значение поля данных). Рассматриваемый компонент сопоставлен с целью **O.AuditEvents** и способствует ее достижению.

FAU_SEL.1 Избирательный аудит

Выполнение требований данного компонента обеспечивает возможность включения и исключения событий в совокупность событий, подвергающихся аудиту, уполномоченным администратором ОО по таким атрибутам, как категория события, класс события, поле данных. Рассматриваемый компонент сопоставлен с целью **O.AuditEvents** и способствует ее достижению.

FAU_STG.1 Защищенное хранение журнала аудита

Выполнение требований данного компонента обеспечивает защиту хранимых записей аудита от несанкционированного удаления и предотвращает модификацию записей аудита. Рассматриваемый компонент сопоставлен с целью **O.ProtectAudit** и способствует ее достижению.

FAU_STG.3 Действия в случае возможной потери данных аудита

Выполнение требований данного компонента обеспечивает создание нового журнала аудита, если журнал аудита превысит установленный уполномоченным администратором ОО размер. Рассматриваемый компонент сопоставлен с целью **O.ProtectAudit** и способствует ее достижению.

FAU_STG.4 Предотвращение потери данных аудита

Выполнение требований данного компонента обеспечивает игнорирование событий, подвергающихся аудиту, и останов ОО при отсутствии свободного дискового пространства для создания журнала аудита. Рассматриваемый компонент сопоставлен с целью **O.ProtectAudit** и способствует ее достижению.

FDP_ACC.1 Ограниченное управление доступом

Выполнение требований данного компонента обеспечивает реализацию политики дискреционного доступа для субъектов, именованных объектов и всех операций между субъектами и объектами. Рассматриваемый компонент сопоставлен с целью **O.AccessObject** и способствует ее достижению.

FDP_ACF.1 Управление доступом, основанное на атрибутах безопасности

Выполнение требований данного компонента обеспечивает осуществление политики дискреционного доступа, основываясь на атрибутах безопасности, определении правил доступа субъектов к объектам. Рассматриваемый компонент сопоставлен с целью **O.AccessObject** и способствует ее достижению.

FIA_AFL.1 (1) Обработка отказов аутентификации

Выполнение требований данного компонента обеспечивает блокировку регистрационной записи пользователя ОО при превышении установленного числа неуспешных попыток аутентификации при доступе к ОО. Рассматриваемый компонент сопоставлен с целью **O.TOEAuth** и способствует ее достижению.

FIA_ATD.1 Определение атрибутов пользователя

Выполнение требований данного компонента обеспечивает поддержание для каждого пользователя (пользователя ОО и администратора ОО) в качестве атрибутов безопасности идентификатора регистрационной записи пользователя, идентификатора учетной записи пользователя, идентификатора роли, участником которой является пользователь. Рассматриваемый компонент сопоставлен с целями **O.AccessObject, O.AccessTOE, O.AuditEvents, O.AdminManage** и способствует их достижению.

FIA_UAU.2 (1) Аутентификация до любых действий пользователя

Выполнение требований данного компонента обеспечивает выполнение аутентификации **с**убъекта доступа к ОО и объектам ОО до того, как ФБО разрешат ему выполнять любые другие (не связанные с аутентификацией) действия. Рассматриваемый компонент сопоставлен с целью **O.TOEAuth** и способствует ее достижению.

FIA_UID.2 Идентификация до любых действий пользователя

Выполнение требований данного компонента обеспечивает выполнение идентификации **с**убъекта доступа к ОО и объектам ОО до того, как ФБО разрешат ему выполнять любые другие (не связанные с идентификацией) действия. Рассматриваемый компонент сопоставлен с целями **O.AccessObject, O.AccessTOE** и способствует их достижению.

FIA_USB.1 Связывание пользователь-субъект

Выполнение требований данного компонента обеспечивает ассоциирование соответствующих атрибутов безопасности субъекта доступа с субъектами, действующими от имени этого субъекта доступа. Рассматриваемый компонент сопоставлен с целями **O.AccessObject, O.AccessTOE, O.AuditEvents** и способствует их достижению.

FMT_MOF.1 Управление режимом выполнения функций

Выполнение требований данного компонента обеспечивает, что ФБО разрешает модификацию и определение режимов выполнения функций, связанных с аудитом и аутентификацией субъектов доступа, только уполномоченному администратору ОО. Рассматриваемый компонент сопоставлен с целью **O.AdminManage** и способствует ее достижению.

FMT_MSA.1 Управление атрибутами безопасности

Выполнение требований данного компонента обеспечивает возможность модифицировать атрибуты безопасности в правилах политики дискреционного управления доступом только уполномоченному администратору ОО и пользователю ОО, являющемуся владельцем объекта. Рассматриваемый компонент сопоставлен с целями **O.AccessObject, O.AdminManage** и способствует их достижению.

FMT_MSA.3 Инициализация статических атрибутов

Выполнение требований данного компонента обеспечивает ограничительные значения по умолчанию для атрибутов безопасности, которые используются для осуществления политики дискреционного управления доступом, и возможность для уполномоченного администратора ОО и пользователя ОО, являющегося владельцем объекта, определять альтернативные значения для отмены значений по умолчанию. Рассматриваемый компонент сопоставлен с целями **O.AccessObject, O.AdminManage** и способствует их достижению.

FMT_MTD.1 Управление данными ФБО

Выполнение требований данного компонента предоставляет возможность модификации определенных данных ФБО только администратору ОО. Рассматриваемый компонент сопоставлен с целью **O.AdminManage** и **O.DistrResourse** и способствует их достижению.

FMT_REV.1 (1) Отмена

Выполнение требований данного компонента предоставляет возможность отмены атрибутов безопасности, ассоциированных с пользователями ОО и объектами, в пределах ОДФ только уполномоченному администратору ОО. Рассматриваемый компонент сопоставлен с целью **O.AdminManage** и способствует ее достижению.

FMT_REV.1 (2) Отмена

Выполнение требований данного компонента предоставляет возможность отмены атрибутов безопасности, ассоциированных с объектами, в пределах ОДФ только пользователю ОО, являющемуся владельцем объекта. Рассматриваемый компонент сопоставлен с целью **O.AdminManage** и способствует ее достижению.

FMT_SMR.1 Роли безопасности

Данный компонент включен в ЗБ вследствие того, что все другие компоненты из класса FMT зависят от назначения субъекту ролей администратора ОО и пользователя ОО. Рассматриваемый компонент сопоставлен с целями **O.AccessObject, O.ProtectAudit, O.AdminManage, O.ProtectResTSF** и способствует их достижению.

FPT_RVM.1 (1) Невозможность обхода ПБО

Выполнение требований данного компонента обеспечивает, чтобы функции, осуществляющие ПБО, вызывались и успешно выполнялись прежде, чем разрешается выполнение любой другой функции в пределах ОДФ. Рассматриваемый компонент сопоставлен с целью **O.ProtectResTSF** и способствует ее достижению.

FPT_SEP.1 (1) Отделение домена ФБО

Выполнение требований данного компонента обеспечивает для ФБО домен безопасности для собственного выполнения, который защищает их от вмешательства и искажения недоверенными субъектами. Рассматриваемый компонент сопоставлен с целью **O.ProtectResTSF** и способствует ее достижению.

FRU_RSA.2 (1) Минимальные и максимальные квоты

Выполнение требований данного компонента обеспечивает возможность реализации минимальных и максимальных квот для объема физической памяти, который ОО может использовать в процессе функционирования. Рассматриваемый компонент сопоставлен с целью **O.DistrResourse** и способствует ее достижению.

FRU_RSA.2 (2) Минимальные и максимальные квоты

Выполнение требований данного компонента обеспечивает возможность реализации минимальных и максимальных квот для объема дискового пространства, который базы данных могут использовать одновременно. Рассматриваемый компонент сопоставлен с целью **O.DistrResourse** и способствует ее достижению.

FTA_TSE.1 Открытие сеанса с ОО

Выполнение требований данного компонента обеспечивает способность отказа ОО в открытии сеанса доступа к ОО, основываясь на идентификаторе регистрационной записи пользователя и предельном количестве одновременно открытых сеансов доступа к ОО. Рассматриваемый компонент сопоставлен с целью **O.AccessTOE** и способствует ее достижению.

8.2.1.2 Обоснование требований доверия к безопасности ОО

Требования доверия настоящего ЗБ соответствуют ОУД1, усиленному компонентом AVA_SOF.1 (Оценка стойкости функции безопасности), и сформулированы, исходя из соответствия настоящего ЗБ профилю защиты «Безопасность информационных технологий. Системы управления базами данных. Системы управления базами данных масштаба предприятия. Профиль защиты. Версия 1.0, 2005».

Выбор ОУД1 в качестве основы требований доверия в настоящем ЗБ является достаточным при определении допустимости использования ОО при обработке конфиденциальной информации.

8.2.2 Обоснование требований безопасности для среды ИТ

В таблице 8.4 представлено отображение функциональных требований безопасности среды ИТ на цели безопасности для среды.

Таблица 8.4 – Отображение функциональных требований безопасности среды ИТ на цели безопасности для среды

	OE.OSAuth	OE.ManageAuthData	OE.ProtectResTSF	OE.GenerateTime
FIA_AFL.1 (2)	**X**	**X**		
FIA_SOS.1	**X**	**X**		
FIA_UAU.2 (2)	**X**			
FPT_RVM.1 (2)			**X**	
FPT_SEP.1 (2)			**X**	
FPT_STM.1				**X**

FIA_AFL.1 (2) Обработка отказов аутентификации

Выполнение требований данного компонента обеспечивает блокировку регистрационной записи пользователя ОО при превышении установленного числа

неуспешных попыток аутентификации при доступе к ОО. Рассматриваемый компонент сопоставлен с целями **OE.OSAuth, OE.ManageAuthData** и способствует их достижению.

FIA_SOS.1 Верификация секретов

Выполнение требований данного компонента обеспечивает верификацию качества паролей на доступ к ОО. Рассматриваемый компонент сопоставлен с целями **OE.OSAuth, OE.ManageAuthData** и способствует их достижению.

FIA_UAU.2 (2) Аутентификация до любых действий пользователя

Выполнение требований данного компонента обеспечивает выполнение аутентификации **с**убъекта доступа к ОО и объектам ОО до того, как ФБО разрешат ему выполнять любые другие (не связанные с аутентификацией) действия. Рассматриваемый компонент сопоставлен с целью **OE.OSAuth** и способствует ее достижению.

FPT_RVM.1 (2) Невозможность обхода ПБО

Выполнение требований данного компонента обеспечивает, чтобы функции, осуществляющие ПБО, вызывались и успешно выполнялись прежде, чем разрешается выполнение любой другой функции в пределах ОДФ. Рассматриваемый компонент сопоставлен с целью **OE.ProtectResTSF** и способствует ее достижению.

FPT_SEP.1 (2) Отделение домена ФБО

Выполнение требований данного компонента обеспечивает для ФБО домен безопасности для собственного выполнения, который защищает их от вмешательства и искажения недоверенными субъектами. Рассматриваемый компонент сопоставлен с целью **OE.ProtectResTSF** и способствует ее достижению.

FPT_STM.1 Надежные метки времени

Данный компонент включен в ЗБ для удовлетворения зависимости компонента FAU_GEN.1 от наличия в записях аудита точного указания даты и времени. Рассматриваемый компонент сопоставлен с целью **OE.GenerateTime** и способствует ее достижению.

8.2.3 Обоснование зависимостей требований

В таблице 8.5 представлены результаты удовлетворения зависимостей функциональных требований. Зависимости компонентов требований удовлетворены в настоящем ЗБ либо включением компонентов, определенных в части 2 ОК под рубрикой «Зависимости», либо включением компонентов, иерархичных по отношению к компонентам, определенным в части 2 ОК под рубрикой «Зависимости».

Таким образом, столбец 2 таблицы 8.5 является справочным и содержит компоненты, определенные в части 2 ОК в описании компонентов требований, приведенных в столбце 1 таблицы 8.5, под рубрикой «Зависимости».

Столбец 3 таблицы 8.5 показывает, какие компоненты требований были реально включены в настоящий ЗБ для удовлетворения зависимостей компонентов, приведенных в первом столбце таблицы 8.5. Компоненты требований в столбце 3 таблицы 8.5 либо совпадают с компонентами в столбце 2 таблицы 8.5, либо иерархичны по отношению к ним.

Таблица 8.5 – Зависимости функциональных требований

Функциональные компоненты	Зависимости по ОК	Удовлетворение зависимостей
Зависимости функциональных требований ОО		
FAU_GEN.1	FPT_STM.1	FPT_STM.1
FAU_GEN.2	FAU_GEN.1, FIA_UID.1	FAU_GEN.1, FIA_UID.2
FAU_SAR.1	FAU_GEN.1	FAU_GEN.1
FAU_SAR.2	FAU_SAR.1	FAU_SAR.1
FAU_SAR.3	FAU_SAR.1	FAU_SAR.1
FAU_SEL.1	FAU_GEN.1, FMT_MTD.1	FAU_GEN.1, FMT_MTD.1
FAU_STG.1	FAU_GEN.1	FAU_GEN.1
FAU_STG.3	FAU_STG.1	FAU_STG.1
FAU_STG.4	FAU_STG.1	FAU_STG.1
FDP_ACC.1	FDP_ACF.1	FDP_ACF.1
FDP_ACF.1	FDP_ACC.1, FMT_MSA.3	FDP_ACC.1, FMT_MSA.3

Функциональные компоненты	Зависимости по ОК	Удовлетворение зависимостей
FIA_AFL.1 (1)	FIA_UAU.1	FIA_UAU.2 (1)
FIA_UAU.2 (1)	FIA_UID.1	FIA_UID.2
FIA_USB.1	FIA_ATD.1	FIA_ATD.1
FMT_MOF.1	FMT_SMR.1	FMT_SMR.1
FMT_MSA.1	[FDP_ACC.1 или FDP_IFC.1], FMT_SMR.1	FDP_ACC.1, FMT_SMR.1
FMT_MSA.3	FMT_MSA.1, FMT_SMR.1	FMT_MSA.1, FMT_SMR.1
FMT_MTD.1	FMT_SMR.1	FMT_SMR.1
FMT_REV.1 (1)	FMT_SMR.1	FMT_SMR.1
FMT_REV.1 (2)	FMT_SMR.1	FMT_SMR.1
FMT_SMR.1	FIA_UID.1	FIA_UID.2
Зависимости функциональных требований среды ИТ		
FIA_AFL.1 (2)	FIA_UAU.1	FIA_UAU.2 (2)
FIA_UAU.2 (2)	FIA_UID.1	FIA_UID.2

Таким образом, все зависимости включенных в ЗБ функциональных требований были удовлетворены.

8.3 Обоснование краткой спецификации ОО

Обоснование краткой спецификации ОО представлено таблицей 8.6 и таблицей 8.7.

Таблица 8.6 – Отображение функциональных требований безопасности на функции безопасности

	Аудит безопасности	Защита данных пользователя	Идентификация и аутентификация	Управление безопасностью	Защита ФБО	Управление доступом к ОО	Использование ресурсов ОО
Функциональные требования ОО							
FAU_GEN.1	X						
FAU_GEN.2	X						
FAU_SAR.1	X						
FAU_SAR.2	X						
FAU_SAR.3	X						
FAU_SEL.1	X						
FAU_STG.1	X						
FAU_STG.3	X						
FAU_STG.4	X						
FDP_ACC.1		X					
FDP_ACF.1		X					
FIA_AFL.1 (1)			X				
FIA_ATD.1			X				
FIA_UAU.2 (1)			X				
FIA_UID.2			X				
FIA_USB.1			X				

	Аудит безопасности	Защита данных пользователя	Идентификация и аутентификация	Управление безопасностью	Защита ФБО	Управление доступом к ОО	Использование ресурсов ОО
FMT_MOF.1				X			
FMT_MSA.1				X			
FMT_MSA.3				X			
FMT_MTD.1				X			
FMT_REV.1 (1)				X			
FMT_REV.1 (2)				X			
FMT_SMR.1				X			
FPT_RVM.1 (1)					X		
FPT_SEP.1 (1)					X		
FRU_RSA.2 (1)							X
FRU_RSA.2 (2)							X
FTA_TSE.1						X	
Функциональные требования среды ИТ							
FIA_AFL.1 (2)			X				
FIA_SOS.1			X				
FIA_UAU.2 (2)			X				
FPT_RVM.1 (2)					X		
FPT_SEP.1 (2)					X		
FPT_STM.1					X		

Таблица 8.7 – Отображение требований доверия на меры безопасности

	Управление конфигурацией	Предоставление руководств	Предоставление проектной документации	Тестирование
ACM_CAP.1	X			
ADO_IGS.1		X		
ADV_FSP.1			X	
ADV_RCR.1			X	
AGD_ADM.1		X		
AGD_USR.1		X		
ATE_IND.1				X

8.4 Обоснование требований к стойкости функций безопасности

Термин «стойкость функции» определен в части 1 ОК как характеристика функции безопасности ОО, выражающая минимальные усилия, предположительно необходимые для нарушения ее ожидаемого безопасного режима при прямой атаке на лежащие в ее основе механизмы безопасности. В части 1 ОК определено три уровня стойкости функции: базовая СФБ, средняя СФБ и высокая СФБ. В настоящем ЗБ выбран уровень стойкости функции – средняя СФБ. Средняя СФБ – это уровень стойкости функции безопасности ОО, на котором функция предоставляет адекватную защиту от прямого или умышленного нарушения безопасности ОО нарушителями с умеренным потенциалом нападения. Выбор СФБ в ЗБ определялся, исходя из возможностей ОО и обеспечения соответствия ОО профилю защиты «Безопасность информационных технологий. Системы управления базами данных. Системы управления базами данных масштаба предприятия. Профиль защиты. Версия 1.0, 2005». Выбор средней СФБ в качестве минимального уровня стойкости функций безопасности является достаточным при определении допустимости использования ОО при обработке конфиденциальной информации.

8.5 Обоснование утверждений о соответствии ПЗ

Объект оценки соответствует профилю защиты СУБД.СУБД_МП.ПЗ «Безопасность информационных технологий. Системы управления базами данных. Системы управления базами данных масштаба предприятия. Профиль защиты. Версия 1.0, 2005». Данное утверждение о соответствии подразумевает, что ОО отвечает всем требованиям ПЗ.

8.5.1 Обоснование конкретизации требований безопасности ИТ

Все требования безопасности, сформулированные в ПЗ СУБД.СУБД_МП.ПЗ «Безопасность информационных технологий. Системы управления базами данных. Системы управления базами данных масштаба предприятия. Профиль защиты. Версия 1.0, 2005», включены в настоящее ЗБ. Некоторые из них были подвергнуты дальнейшей конкретизации.

Профиль защиты СУБД.СУБД_МП.ПЗ «Безопасность информационных технологий. Системы управления базами данных. Системы управления базами данных масштаба предприятия. Профиль защиты. Версия 1.0, 2005» содержит ряд функциональных требований, операции над которыми при разработке ЗБ нуждались в завершении. Операции подобных требований завершены в настоящем ЗБ в полном объеме.

Исходя из особенностей рассматриваемого ОО, по отношению к ряду функциональных требований, взятых из ПЗ, в настоящем ЗБ была применена операция уточнения.

FAU_GEN.1 – уточнен относительно ПЗ в связи с необходимостью генерировать записи аудита, связанные с функциональными возможностями ОО, не включенными в ПЗ.

FAU_GEN.2 – уточнен относительно ПЗ в связи с особенностями ОО – возможностью ассоциировать каждое событие, потенциально подвергаемое аудиту, с идентификатором учетной записи пользователя или идентификатором регистрационной записи пользователя, который был инициатором этого события.

FAU_SAR.3 – уточнен относительно ПЗ в связи с особенностями ОО – возможностью выполнять поиск данных аудита, в том числе, и по наименованию поля данных.

FAU_SEL.1 – уточнен относительно ПЗ в связи с особенностями ОО – возможностью включения событий в совокупность событий, подвергающихся аудиту, в том числе, и по категории событий.

FDP_ACF.1 – уточнен относительно ПЗ в связи с особенностями реализации механизмов дискреционного управления доступом в ОО.

FIA_ATD.1 – уточнен относительно ПЗ в связи с особенностями ОО – поддержкой для каждого пользователя в качестве атрибутов безопасности идентификатора регистрационной записи пользователя, идентификатора учетной записи пользователя, идентификатора роли, участником которой является пользователь.

FIA_UID.2 – уточнен относительно ПЗ в связи с особенностями ОО – осуществлением идентификации субъектов доступа к ОО и объектам ОО.

FMT_MTD.1 – уточнен относительно ПЗ в связи с необходимостью управления данными ФБО, связанными с функциональными возможностями ОО, не включенными в ПЗ.

FTA_TSE.1 – уточнен относительно ПЗ в связи с особенностями ОО – возможностью запрета доступа к ОО на основе идентификатора регистрационной записи пользователя, предельного количества одновременно открытых сеансов доступа к ОО.

FIA_UAU.2 – уточнен относительно ПЗ в связи с особенностями ОО – осуществлением аутентификации субъектов доступа к ОО и объектам ОО.

8.5.2 Обоснование добавления угроз безопасности

В настоящее ЗБ включена следующая дополнительная угроза, которой противостоит ОО, не вошедшая в ПЗ СУБД.СУБД_МП.ПЗ «Безопасность информационных технологий. Системы управления базами данных. Системы управления базами данных масштаба предприятия. Профиль защиты. Версия 1.0, 2005»:

T.UnauthExecProc&Fanc – включена в связи с возможностью ОО, связанной с противостоянием выполнению хранимых процедур и определяемых функций неуполномоченными на это пользователями ОО.

8.5.3 Обоснование добавления политик безопасности организации

В настоящее ЗБ включены следующие дополнительные политики безопасности организации, не вошедшие в ПЗ СУБД.СУБД_МП.ПЗ «Безопасность информационных

технологий. Системы управления базами данных. Системы управления базами данных масштаба предприятия. Профиль защиты. Версия 1.0, 2005»:

P.Resourse – включена в связи с возможностью ОО, связанной с надлежащим распределением ресурсов ОО администратором ОО.

P.TOEAuth – включена в связи с возможностью ОО, связанной с аутентификацией субъектов, осуществляющих попытку доступа к ОО с рабочих станций и серверов под управлением ОС, не имеющих совместно с ОС (являющейся средой функционирования ОО) централизованного управления параметрами безопасности, механизмами самого ОО.

P.ManageAuthData – включена в связи с возможностью (в случае аутентификации субъектов, осуществляющих попытку доступа к ОО, с использованием механизмов самого ОО) операционной системы предоставлять механизмы управления качеством аутентификационных данных, обеспечивающие адекватную защиту ОО от прямого или умышленного нарушения безопасности нарушителями с умеренным потенциалом нападения.

8.5.4 Обоснование добавления целей безопасности для ОО

В настоящее ЗБ включены следующие дополнительные цели безопасности для ОО, не вошедшие в ПЗ СУБД.СУБД_МП.ПЗ «Безопасность информационных технологий. Системы управления базами данных. Системы управления базами данных масштаба предприятия. Профиль защиты. Версия 1.0, 2005»:

O.DistrResourse – ОО должен обеспечивать для уполномоченного администратора ОО возможность надлежащего распределения ресурсов ОО.

Включение данной цели безопасности для ОО связано с добавлением в ЗБ политики безопасности организации **P.Resourse**.

O.TOEAuth – ОО должен обеспечивать аутентификацию субъектов, осуществляющих попытку доступа к ОО с рабочих станций и серверов под управлением ОС, не имеющих совместно с ОС (являющейся средой функционирования ОО) централизованного управления параметрами безопасности.

Включение данной цели безопасности для ОО связано с добавлением в ЗБ политики безопасности организации **P.TOEAuth**.

8.5.5 Обоснование добавления целей безопасности для среды

В настоящее ЗБ включена следующая дополнительная цель безопасности для среды, не вошедшая в ПЗ СУБД.СУБД_МП.ПЗ «Безопасность информационных технологий. Системы управления базами данных. Системы управления базами данных масштаба предприятия. Профиль защиты. Версия 1.0, 2005»:

OE.ManageAuthData – в случае аутентификации субъектов, осуществляющих попытку доступа к ОО, с использованием механизмов самого ОО, операционная система должна предоставлять механизмы управления качеством аутентификационных данных, обеспечивающие адекватную защиту ОО от прямого или умышленного нарушения безопасности нарушителями с умеренным потенциалом нападения..

Включение данных целей безопасности для среды связано с добавлением в ЗБ политики безопасности организации **P.ManageAuthData**.

8.5.6 Обоснование добавления требований безопасности ИТ

В настоящее ЗБ включены следующие дополнительные функциональные требования безопасности ОО, не вошедшие в ПЗ СУБД.СУБД_МП.ПЗ «Безопасность информационных технологий. Системы управления базами данных. Системы управления базами данных масштаба предприятия. Профиль защиты. Версия 1.0, 2005»:

Компонент функциональных требований безопасности FIA_AFL.1 (1) – включен в связи с возможностью ОО обеспечивать блокировку регистрационной записи пользователя ОО при превышении установленного числа неуспешных попыток аутентификации при доступе к ОО.

Компонент функциональных требований безопасности FIA_UAU.2 (1) – включен в связи с возможностью ОО обеспечивать выполнение аутентификации субъекта доступа к ОО и объектам ОО до того, как ФБО разрешат ему выполнять любые другие (не связанные с аутентификацией) действия.

Компонент функциональных требований безопасности FRU_RSA.2 (1) – включен в связи с возможностью ОО квотировать объем физической памяти, который ОО может использовать в процессе функционирования.

Компонент функциональных требований безопасности FRU_RSA.2 (2) – включен в связи с возможностью ОО квотировать объем дискового пространства, который несколько БД могут использовать одновременно.