МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное бюджетное образовательное учреждение высшего образования

«РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ ГИДРОМЕТЕОРОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Кафедра Информационных технологий и систем безопасности

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА

(дипломная работа)

На тему «Методика обеспечения безопасности информационной системы на основе мандатной модели доступа»

Исполнитель Качур Евгения Дмитриевна

(фамилия, имя, отчество)

Руководитель Попов Николай Николаевич

(фамилия, имя, отчество)

«К защите допускаю»
Заведующий кафедрой

(подпись)

Завгородний Владимир Николаевич

(фамилия, имя, отчество)

«___»_____20___г.

Санкт–Петербург

2019

РЕФЕРАТ

Дипломная работа: 83 страницы, 22 рисунков, 5 таблиц, 7 приложения, 38 источников литературы.

МАНДАТНАЯ МОДЕЛЬ РАЗГРАНИЧЕНИЯ ДОСТУПА, ДИСКРЕЦИОННАЯ МОДЕЛЬ РАЗГРАНИЧЕНИЯ ДОСТУПА, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, ОС СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ ASTRA LINUX SPECIAL EDITION, ПРОЕКТИРОВАНИЕ И РЕАЛИЗАЦИЯ БД, СУБД POSTGRESQL.

Объект исследования – мандатная модель разграничения доступа.

Предмет исследования – особенности работы мандатного механизма разграничения доступа в среде Astra Linux Special Edition на основе спроектированной базы данных.

Целью данной работы является разработка мандатной модели разграничения доступа на основе спроектированной базы данных.

В дипломной работе проводится анализ руководящих документов по классификации автоматизированных систем, классификации и дальнейшему выбору средств вычислительной техники для реализации мандатного механизма разграничения доступа.

Разрабатывается база данных. Проектируется на ее основе мандатная и дискреционная модели разграничения доступа. Работа базы данных и моделей разграничения

осуществляется на основе системы управления базами данных PostgreSQL в среде Astra Linux Special Edition.

Демонстрируется принцип работы одного из методов защиты информации, содержащей государственную тайну до грифа «совершенно секретно» включительно, от несанкционированного доступа на основе спроектированной базы данных, моделей дискреционного и мандатного разграничения доступа.

«РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ ГИДРОМЕТЕОРОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ»

Кафедра Информационных технологий и систем безопасности

«УТВЕРЖДАЮ»
Заведующий кафедрой
_____ Завгородний В.Н.
(подпись) (фамилия, имя, отчество)

« _ »_____2019 года

Задание на выпускную квалификационную работу

студенту_____Качур Евгении Дмитриевне_____
(фамилия, имя, отчество)

1. Тема Методика обеспечения безопасности информационной системы на основе мандатной модели доступа_____

закреплена приказом ректора Университета от «___» _____2018 года, № _____

2. Срок сдачи законченной работы «___» _____2019 года

3.Исходные данные к выпускной квалификационной работе:

«Руководящие документы ФСТЭК по автоматизированным системам и средствам вычислительной техники»

«Документация к операционной системе специального назначения Astra Linux Special Edition»

«Стенд с развернутой операционной системой и прикладными пакетами, реализующими моделирование работы комплекса разрабатываемого решения на объекте автоматизации Министерства Обороны Российской Федерации»

3. Перечень вопросов, подлежащих разработке (краткое содержание работы (проекта):

Введение. Актуальность темы, цели и задачи выпускной квалификационной работы

Глава 1. Теоретические основы
(наименование главы)

Глава 2. Проектирование

(наименование главы)

Глава 3. Реализация

(наименование главы)

Глава 4. Тестирование

(наименование главы)

Заключение Выводы по работе, практические рекомендации

4.Перечень материалов, представляемых к защите:

- Пояснительная записка;
- Требования к АС и СВТ, необходимые для обработки сведений, составляющих государственную тайну до грифа «совершенно секретно» включительно;
- Схемы запросов на чтение и запись разноуровневых пользователей к разноуровневым таблицам в теории и на практике;
- Логическая и физическая схемы спроектированной БД;
- Описание сущностей и их атрибутов БД;
- Дискреционная и мандатная модели разграничения доступа;
- SQL-код для создания БД.

5.Дата выдачи задания: «_____»____2018 года

Руководитель выпускной квалификационной работы

к.т.н., доцент Попов Николай Николаевич

(должность, ученая степень, ученое звание, фамилия, имя, отчество)

(подпись)

Задание принял к исполнению «_____»_____2018 года

Студент Качур Евгения Дмитриевна

(фамилия, имя, отчество, учебная группа)

(подпись)

ОГЛАВЛЕНИЕ

СПИСОК СОКРАЩЕНИЙ И УСЛОВНЫХ ОБОЗНАЧЕНИЙ

АО – акционерное общество;

АС – автоматизированная система;

БК – беспилотный корабль;

БД – база данных;

ВНИИНС – Всероссийский научно–исследовательский институт автоматизации управления в непромышленной сфере имени В. В. Соломатина;

ГАС ГОЗ – государственная автоматизированная система гособоронзаказа;

ГОСТ – межгосударственный стандарт;

ГП – группа планирования;

ЗАО – закрытое акционерное общество;

ИПС – изолированная программная среда;

ИСО/МЭК – Международная организация по стандартизации/Международная электротехническая комиссия;

КСЗ – комплекс средств защиты;

КСС – комплекс средств связи;

МВД – Министерство внутренних дел;

МО – Министерство обороны

МСВС – Мобильная система Вооружённых сил;

НИЦ СПб ЭТУ – Научно–инженерный центр Санкт–Петербургского электротехнического университета;

НПО РусБИТех – Научно–производственное объединение Русские базовые информационные технологии;

НСД – несанкционированный доступ;

НСИ – нормативно–справочная информация;

ОС – операционная система;

ОС СН – операционная система специального назначения;

ПО – программное обеспечение;

ПС – программное средство;

ПРД – правило разграничения доступа;

ПУ – пункт управления;

ПЭ – пункт эксплуатации;

Роскосмос – Российская корпорация, управляющая космической областью страны;

РФ – Российская Федерация;

СВТ – средство вычислительной техники;

СЗИ – средство защиты информации;

СС – средство связи;

СТР – специальные требования и рекомендации;

СУБД – система управления базами данных;

ФСБ – Федеральная служба безопасности;

ФСИН – Федеральная служба исполнения наказаний;

ФСО – Федеральная служба охраны РФ;

ФСТЭК – Федеральная служба по техническому и экспортному контролю;

ФТС – Федеральная таможенная служба;

ХРУ – модель Харрисона–Руззо–Ульмана;

ЭВМ – электронно–вычислительные машины;

SQL – structured query language

ACL – Access control list;

Astra Linux SE – Astra Linux Special Edition;

BPMN – Business Process Model and Notation;

DAC – Discretionary Access Control;

JDBC – Java DataBase Connectivity;

MAC – Mandatory Access Control;

NRU – Not Read Up;

NWD – Not Write Down;

UML – Unified Modeling Language.

ВВЕДЕНИЕ

Вопрос обеспечения безопасности информации в части ее сохранности от несанкционированного доступа (НСД) является наиболее важным при проектировании автоматизированной системы (АС), предназначенной для обработки конфиденциальной информации. Необходимость усиления защиты данных от возможного доступа к ней посторонних лиц появилось в то время, когда число электронно-вычислительных машин (ЭВМ), обрабатывающих, хранящих и передающих информацию в больших объемах, и число пользователей, работающих с данными ЭВМ, сильно возросло. В соответствие с этим и возник один из методов защиты информации – разграничение доступа[1].

Разграничение доступа используется в большинстве коммерческих организаций и является обязательным при обработке, хранение и передаче персональных данных и служебной тайны. В таком случае достаточно *дискреционного разграничения доступа*. Но, при работе со сведениями, составляющими государственную тайну, в государственных и военных структурах дискреционного разграничения не достаточно. Согласно требованиям Федеральной службы по техническому и экспортному контролю (ФСТЭК) обязательным методом в представленной ситуации является *мандатное разграничение доступа*, которое осуществляется в совокупности с дискреционным. Данный механизм – это одна из составляющих системы

защиты информации от НСД (СЗИ НСД) в нашей стране, обеспечивающая сохранность важных для страны ресурсов.

Данная работа выполнена в АО «НИЦ СПб ЭТУ» в рамках проектов, направленных на автоматизацию и информатизацию бизнес-процессов выбранных управлений Министерства Обороны Российской Федерации (МО РФ). По этой причине данная тема является актуальной.

Целью данной работы является обеспечение безопасности доступа к базе данных (БД) путем разработки и реализации мандатной модели разграничения доступа. В соответствие с целью были поставлены следующие задачи:

- выбрать платформу для реализации на ее основе мандатно-разграниченной БД;
- спроектировать модель БД и мандатную модель разграничения доступа к данной БД;
- реализовать спроектированные модель БД и мандатную модель разграничения доступа к данной БД;
- проверить корректность работы разграничения доступа в реализованной БД.

1. ТЕОРЕТИЧЕСКИЕ ОСНОВЫ

1.1. Классификация СВТ и АС по защите информации

Согласно руководящему документу «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации» ФСТЭК (Федеральной службы по техническому и экспортному контролю) существуют два относительно самостоятельных и, следовательно, имеющих отличие направления в проблеме защиты информации от НСД: направление, связанное со средствами вычислительной техники (СВТ), и направление, связанное с автоматизированными системами (АС)[2].

Под СВТ понимается совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем[3].

АС – это система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций[2].

Отличаются данные направления тем, что СВТ являются отдельными компонентами, а АС представляет собой функционально ориентированную совокупность СВТ. И так как СВТ самостоятельно не обеспечивает выполнение прикладных задач, то они не содержат пользовательский информации.

В связи с таким делением классификация по защите информации в АС и СВТ описывается в двух разных руководящих документах Гостехкомиссии России. Классификация необходима для более детальной разработки требования по защите от НСД с учетом специфических особенностей этих систем.

1.1.1. Классификация СВТ

В документе «Средства вычислительной техники. Защита от несанкционированного доступа информации. Показатель защищенности от несанкционированного доступа к информации» от 30 марта 1992 года СВТ делятся на 7 классов защищенности от НСД к информации. Классы делятся на 4 группы:

- первая группа содержит только 7 класс;
- вторая группа содержит 6 и 5 классы и характеризуется дискреционной защитой
- третья группа содержит 4, 3 и 2 классы и характеризуется мандатной защитой;
- четвертая группа содержит только 1 класс и характеризуется верифицированной защитой.

1.1.2. Классификация АС

Согласно документу «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» от 30 марта 1992 года АС делятся на девять классов. Каждый класс характеризуется

определенной минимальной совокупностью требований по защите. Классы делятся на три группы:

- третья группа включает в себя АС, где работает только один пользователь, имеющий допуск ко всей информации в системе. Информация в такой АС хранится на носителях одного уровня конфиденциальности. Группа включает в себя два класса – 3Б и 3А;
- вторая группа включает в себя АС, где работают пользователи, имеющие одинаковые права допуска ко всей информации в системе. Информация в такой АС хранится на носителях разного уровня конфиденциальности. Группа включает в себя два класса – 2Б и 2А;
- первая группа включает в себя АС, где работают пользователи, имеющие разные права допуска ко всей информации в системе. Информация в такой АС хранится на носителях разного уровня конфиденциальности. Группа включает в себя два класса – 1Д, 1Г, 1В, 1Б и 1А.[2]

Выбор СВТ с определенным классом защищенности зависит от грифа секретности обрабатываемой в АС информации, условий эксплуатации и расположения объектов системы.

В данном случае будет рассмотрена первая группа – многопользовательская и разноуровневая.

1.2. Уровни секретности АС и СВТ для обработки информации, содержащей государственную тайну

Исходя из Закона РФ от 21 июля 1993 года № 5485–I «О государственной тайне» (с изменениями и дополнениями) государственная тайна – это защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации [4].

1.2.1. Уровни секретности АС

Как уже было сказано, классификация АС представляет собой 9 классов, делящихся на 3 группы. В таблице сопоставлены уровни секретности информации и классы АС первой группы, приведенные в соответствие с документом СТР «Специальными требованиями и рекомендациями по защите информации, составляющей государственную тайну, от утечки по техническим каналам», утвержденным Государственной Технической Комиссией при Президенте РФ от 23 мая 1997 года № 55 [5]:

Таблица 1 – Уровни секретности 1 группы АС

Уровни секретности	*Классы АС*
Особой важности	1А
Совершенно секретно	1Б

Секретно	1В
Для служебного пользования	1Г
Персональные данные	1Д

К сведениям особой важности следует относить сведения в области военной, внешнеполитической, экономической, научно-технической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб интересам Российской Федерации в одной или нескольких из перечисленных областей.

К совершенно секретным сведениям следует относить сведения в области военной, внешнеполитической, экономической, научно-технической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб интересам министерства (ведомства) или отрасли экономики Российской Федерации в одной или нескольких из перечисленных областей.

К секретным сведениям следует относить все иные сведения из числа сведений, составляющих государственную тайну. Ущербом безопасности Российской Федерации в этом случае считается ущерб, нанесенный интересам предприятия, учреждения или организации в военной, внешнеполитической, экономической, научно–технической, разведывательной,

контрразведывательной или оперативно–розыскной области деятельности[6].

К служебной информации ограниченного распространения относится несекретная информация, касающаяся деятельности организаций, ограничения на распространение которой диктуются служебной необходимостью, а также поступившая в организации несекретная информация, доступ к которой ограничен в соответствии с федеральными законами[7].

К персональным данным относится любая информация, касающаяся прямо или косвенно определенного или определяемого физического лица (субъекта персональных данных);

Сведения, составляющие государственную тайну, представляют собой информацию, содержащую данные с грифами «секретно», «совершенно секретно» и «особой важности».

1.2.2. Требования к сертификации СВТ для использования в АС, где обрабатывается информация, содержащая государственную тайну.

Требования к СВТ, используемые в АС предъявляемые СТР № 55 трактуются следующим образом:

- СВТ, используемые в АС класса 1А, должны быть не ниже 2 класса;
- СВТ, используемые в АС класса 1Б, должны быть не ниже 3 класса;

- СВТ, используемые в АС класса 1В, должны быть не ниже 4 класса[5].

Таким образом, так как в представленной работе проектируется АС, содержащая сведения с грифом «совершенно секретно» (класс 1Б), то все СВТ, включенные в данную АС, должны быть не ниже 3 класса защищенности.

1.3. Требования Министерства РФ для АС и СВТ, где обрабатывается информация, содержащая государственную тайну с грифом «совершенно секретно» включительно

Исходя из вышесказанного произведен анализ требований МО к АС и СВТ. Для обработки информации, содержащей уровни секретности вплоть до грифа «совершенно секретно», АС и СВТ, входящим в состав АС, необходимо соответствовать минимальной совокупности требований по защите, описанным в п. 1.3.1. –1.3.2.

1.3.1. Требования к АС для класса 1Б

Требования по защите информации от НСД реализуются в рамках системы защиты информации от НСД АС и состоят из четырех подсистем:

- управления доступом;
- регистрации и учета;
- криптографической;
- обеспечения целостности[2].

Подробно требования описаны в приложение А.

1.3.2. Требования к СВТ для 3 класса защищенности

Перечень показателей защищенности СВТ и совокупность описывающих их требований следующие:

- Дискреционный принцип контроля доступа;
- Мандатный принцип контроля доступа;
- Очистка памяти;
- Изоляция модулей;
- Маркировка документов;
- Защита ввода и вывода на отчуждаемый физический носитель информации;
- Сопоставление пользователя с устройством;
- Идентификация и аутентификация;
- Гарантии проектирования;
- Регистрация;
- Взаимодействие пользователя с КСЗ;
- Надежное восстановление;
- Целостность КСЗ;
- Тестирование;
- Руководство для пользователя;
- Тестовая документация;
- Конструкторская (проектная) документация.

Подробно требования описаны в приложение А.

При соответствии представленным выше требованиям СВТ и АС оформляется документ (сертификат), который удостоверяет соответствие СВТ и АС требованиям по защите информации, составляющей государственную тайну

с грифом «совершенно секретно», и дает право разработчику на использование и/или распространение их как защищенных[3].

1.3.3. Требования к СВТ, касающиеся мандатного принципа контроля доступа

Рассмотрим подробнее требования мандатного принципа контроля доступа, представленные в пункте 1.3.2:

- должны сопоставляться классификационные метки каждого субъекта и каждого объекта, которые отражают их место в соответствующей иерархии;
- должны назначаться классификационные уровни субъектам и объектам, которые являются комбинациями иерархических и неиерархических категорий. Данные метки являются основой мандатного принципа разграничения доступа;
- КСЗ должен запрашивать и получать от санкционированного пользователя классификационные метки вводимых новых данных;
- должно осуществляться сопоставление классификационных меток нового субъекта, занесенного в список пользователей;
- должно осуществляться соответствие внешних классификационных меток (субъекты, объекты) внутренним меткам (внутри КСЗ);
- КСЗ должен реализовывать мандатный принцип контроля доступа применительно ко всем объектам

при явном и скрытом доступе со стороны любого из субъектов:

1. субъект может читать объект, только если иерархическая классификация в классификационном уровне субъекта не меньше, чем иерархическая классификация в классификационном уровне объекта, и неиерархические категории в классификационном уровне субъекта включают в себя все иерархические категории в классификационном уровне объекта;
2. субъект осуществляет запись в объект, только если классификационный уровень субъекта в иерархической классификации не больше, чем классификационный уровень объекта в иерархической классификации, и все иерархические категории в классификационном уровне субъекта включаются.

- реализация мандатных ПРД должна предусматривать возможности сопровождения: изменения классификационных уровней субъектов и объектов специально выделенными субъектами;
- должен быть реализован диспетчер доступа, то есть средство, осуществляющее перехват всех обращений субъектов к объектам, а также разграничение доступа в соответствии с заданным принципом разграничения доступа в СВТ;
- должно приниматься решение о санкционированности запроса на доступ только при одновременном

разрешении его и дискреционными, и мандатными ПРД. Таким образом, должен контролироваться не только единичный акт доступа, но и потоки информации.

- в неиерархические категории в классификационном уровне объекта.

1.4. Разграничение доступа

При разграничении доступа каждый пользователь системы имеет доступ только к тем объектам системы, к которым ему предоставлен доступ в соответствии с текущей политикой безопасности. Под политикой безопасности организации международный стандарт ГОСТ ИСО/МЭК 15408–1–2008 подразумевает совокупность руководящих принципов, правил, процедур и практических приемов в область безопасности, которыми руководствуется организация в своей деятельности[8].

Основными понятиями процесса разграничения доступа к объектами являются «объект доступа», «субъект доступа» и «метод доступа субъекта к объекту»[9].

Объект доступа (Access object) – единица информационного ресурса автоматизированной системы, доступ к которой регламентируется правилами разграничения доступа. Под объектами доступа понимаются технические ресурсы (принтеры, сегменты памяти, диски, ленты, процессоры) и программные (папки, файлы, программы), то есть все ресурсы, доступ к которым подлежит контролю.

Субъект доступа (Access subject) – лицо или процесс, действия которого регламентируются правилами разграничения доступа. Под субъектами доступа могут пониматься и процессы, выполняющиеся в система, и пользователи, от имени которого будет выполняться процесс[8].

Метод доступа к объекту – операция, определенная для объекта. Тип такой операции зависит от объекта. Это может быть метода доступа «чтение», «запись», «добавление» для файла, процессор может только выполнять команды, считыватель может только читать и тому подобное.

Говоря кратко, объект доступа – это то, к чему осуществляется доступ, субъект доступа – тот, кто осуществляет доступ, метод доступа – то, каким образом осуществляется доступ[9].

Чтобы иметь возможность на осуществление методов доступа необходимо иметь права доступа. Правом доступа к объекту называют право на выполнение доступа к объекту по некоторому методу или группе методов. Например, если пользователь может записывать некую информацию в файл, то это означает, что он имеет право на запись.

Исходя из вышесказанного разграничения доступа субъектов к объектам – это совокупность правил для каждой комбинации объект–субъект–метод определяющая, разрешен ли доступ данного субъекта к данному объекту по данному методу или же запрещен. Такой способ разрешенных прав доступа субъектов к объектам

регламентируется политикой управления доступом и информационными потоками, являющейся составной частью политики безопасности организации [10].

Политика безопасности организации – это совокупность руководящих принципов, правил, процедур и практических приемов в области безопасности, которыми руководствуется организация в своей деятельности[11].

В настоящее время существует две основные политики управления доступом:

- дискреционная (избирательная) политика управления доступом (Discretionary Access Control, DAC);
- мандатная (полномочная) политика управления доступом (Mandatory Access Control, MAC).[12]

Кроме политик дискреционного и мандатного управления доступом так же существуют ролевая политика, политика безопасности информационных потоков и изолированная программная среда (ИПС).

1.4.1. Дискреционная политика управления доступом

Дискреционная политика управления доступом – политика, соответствующая следующим требованиям управления доступом:

- каждой сущности должен быть присвоен уникальный идентификатор;
- должна быть задана матрица доступа, где в столбцах указаны объекты, в строках – субъекты, ячейки, находящиеся на пересечение, содержат список прав доступа субъекта к объекту;

- субъект должен обладать правами доступа к объекту тогда и только тогда, когда в ячейке матрицы доступов, соответствующей субъекту и сущности, содержится право на доступ[9].

Большинство распространенных систем поддерживают данную политику из-за простоты реализации, что, несомненно, является ее главным достоинством.

К недостаткам такой политики относится наличие администратора, который имеет доступ абсолютно ко всем объектам, а так же при создании объекта права назначаются автоматически, и, как правило, доступ к созданному объекту могут иметь все пользователи, находящиеся в системе [13].

Модели с дискреционным управлением доступа:

- модель матрицы доступов Харрисона-Руззо-Ульмана;
- модель распространения прав доступа Take-Grant;
- дискреционная ДП-модель.

Модель матрицы доступов Харрисона-Руззо-Ульмана используется для анализа систем защиты, которые реализуют дискреционную политику управления доступом.

Модель распространения прав доступа Take-Grant ориентирована на анализ путей распространения прав доступа в системах дискреционного управления доступом.

Дискреционная ДП-модель построена для анализа условий передачи прав доступа и реализации информационных потоков между сущностями.

Рассмотрим подробнее модель матрицы доступов Харрисона-Руззо-Ульмана (ХРУ). Данная модель была разработана в 1971 году и названа в честь ее авторов:

Майкла Харрисона, Уолтера Руззо и Джеффри Ульмана. Она является моделью управления доступом субъектов к объектам, реализована с помощью матрицы доступов. Матрица доступа – таблица, описывающая права доступа субъектов к объектам. (Таблица 2)

Таблица 2 Матрица доступа в модели ХРУ

	объект 1	*объект 2*	*...*	*объект n*
субъект 1	rd			
субъект 2		rx		
...				
субъект n	rwx			

Где r (read) означает чтение;

w (write) – запись;

x (execute) – выполнение (данные права представляют собой общий набор действий, изменяющийся в зависимости от реализации).

Из таблицы видно, что строки матрицы соответствуют субъектам, а столбцы – объектам. На пересечении строк и столбцов указаны права доступа определенного субъекта к определенному объекту. Например, субъект 2 имеет права на чтение, выполнение, загрузки, удаления объекта 2.

При создании объекта его владельцем назначается субъект, который создал объекта. Далее, субъект, имеющий необходимые права, может назначать объекту нового владельца. В таком случае субъект, желающий изменить владельца объекта, может назначить владельцем только себя. Представленное ограничение необходимо для того,

чтобы субъект, получивший владение над объектом, не смог снять с себя ответственности за некорректные действия с объектом, назначив ему другого владельцы.

1.4.2. Мандатная политика управления доступом

Мандатная политика управления доступом – политика, соответствующая следующим требованиям управления доступом:

- у каждого объекта существует владелец;
- владелец имеет право полностью ограничить доступ для других субъектов к своему объекту;
- возможность доступа для каждой четверки объект–субъект–метод–процесс определена в каждый момент времени. Так как состояние процесса изменяется со временем, то возможность доступа так же может измениться;
- в системе существует хотя бы один привилегированный пользователь, который имеет возможность удалить объект;
- каждый объект имеет гриф секретности. Чем выше гриф, тем секретнее объект. Нулевое значение грифа секретности означает, что объект несекретный;
- каждый субъект имеет уровень допуска. Нулевое значение уровня допуска означает, что субъект не имеет уровня допуска к любым секретным объектам;
- доступ субъекта к объекту запрещен в том случае, если субъект открывает объект, имеющий мандатную метку, в режиме, допускающем чтение, при этом гриф

секретности объекта выше уровня допуска субъекта. Данное правило называется правилом NRU (Not Read Up – нет чтения вверх);

- доступ субъекта к объекту запрещен в том случае, если субъект открывает объект, имеющий мандатную метку, в режиме, допускающем запись, при этом гриф секретности объекта ниже уровня допуска субъекта. Данное правило называется правилом NWD (Not Write Down – нет записи вниз);
- все процессы ОС имеет определенный уровень конфиденциальности, который соответствует максимальному из грифов секретности объектов, открытых процессом на всю длительность своего существования;
- гриф секретности объекта может понизить только тот субъект, который имеет доступ на чтение объекта и обладает привилегией, которая позволяет ему понижать гриф.

Существуют три модели с мандатным разграничением доступа:

- модель Белла–ЛаПадулы;
- модель систем военных сообщения;
- мандатная ДП–модель[9].

Модель Белла–ЛаПадулы является основной моделью, которая предназначена для анализа систем защиты, реализующих мандатный механизм разграничения доступа.

Модель систем военных сообщений построена на основе модели Белла–ЛаПадулы. Данная модель

ориентирована на систему приема, передачи, обработки почтовых сообщений, которые реализуют мандатную политику управления доступом.

Рассмотрим подробнее модель Белла–ЛаПадулы. Представленная модель была разработана в 1972–1975 годах американскими специалистами – Дэвидом Беллом и Леонардо ЛаПадулой (D. Elliott Bell, Leonard J.LaPadula), являвшимися сотрудниками MITRE Corporation. Представленная модель и была названа в честь их имен[13].

Модель Белла–ЛаПадулы является классической мандатной моделью разграничения доступа. Она базируется на правилах секретного документооборота, которая используется правительственными учреждениями во многих странах.

Объектом контроля в такой модели являются отдельные элементы информационного потока – транзакты (файлы, пакеты). Управление информационными потоками – это контроль не только самих транзактов, но и направления, по которым они двигаются в информационном потоке. Транзакты снабжаются уникальными метками. Метки представляют собой определенную иерархию, которая варьируются от «несекретно» до «особой важности». Пример иерархии уровней доступа приведен на рисунке 1.

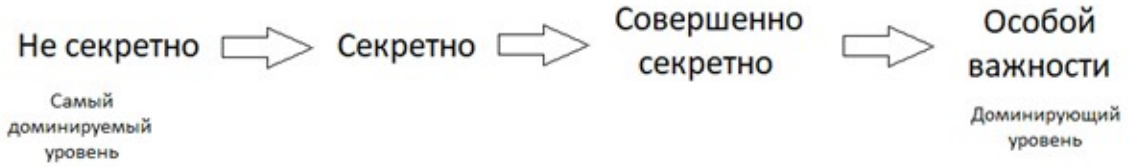

Рисунок 1 – Пример иерархии уровней доступа

Таким образом, уровни доступа упорядочиваются по доминированию одного уровня над другим.

Уже рассмотренные правила NRU и NWD представлены на рисунке 2.

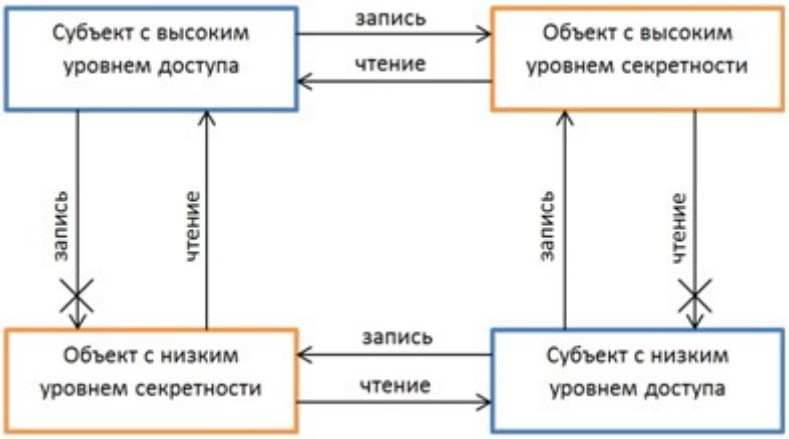

Рисунок 2 – Правила мандатного разграничения доступа к защищенным файлам

На картинки отображены возможные информационные потоки в мандатной модели разграничения доступа, отражающие правила NRU и NWD. Первое правило является очевидным, так как работнику нельзя получить информацию, уровень секретности которой выше уровня допуска пользователя. Второе правило ставит под сомнение, так как пользователь с более высоким уровнем допуска уже знает информацию, хранимую в документах с более низким уровнем секретности, он лишь сделает запись известных ему сведений. Но в таком случае велика вероятность происхождения утечки информации со стороны высокоуровневого пользователя, так как он может внести известные ему сведения с более высоким грифом секретности в документы с более низким грифом

секретности, которые в свою очередь могут прочитать низкоуровневые пользователи[12].

В представленном случае разграничение является *иерархическим*, так как при сравнение меток доступа от результата сравнения зависит, получит ли пользователь доступ на чтение, запись или же на то и другое. Также существует такой вид разграничения, как *неиерархический*, где результатом сравнения меток является их совпадение или несовпадение. Если метки совпадают, пользователь получает право на чтение и запись. Если метки не совпадает пользователь не получает доступа к объекту.

Однако, у мандатной модели есть два существенных недостатка. Первый недостаток – отсутствие каких–либо ограничений для пользователей одного уровня. Другими словами, любой объект определенного уровня допуска имеет доступ к любому объекту с соответствующим грифом секретности, что приводит в большинстве случаев к избыточности прав доступа для определенных пользователей. Данное обстоятельство противоречит самому понятию «разграничение доступа». Для устранения подобного недостатка мандатное разграничение доступа используется совместно с дискреционным, что позволяет разграничить доступ к объектам одного уровня безопасности.

Вторым недостатком является сложность реализации. Классифицировать необходимо абсолютно все файлы: каждую программу, документ, носитель информации, все комбинации доступа. Исходя из этого, при реализации

подобной системы, пользователь вынужден использовать АС, разработанную с учетом этой модели[13].

1.5. Выбора ОС

В настоящее время выбор операционных систем, снабженных средствами реализации механизма мандатного разграничения доступа, достаточно широк, что связано с необходимостью более тщательной защиты информационных ресурсов. Примерами таких ОС являются:

- Flask;
- openSUSE;
- Ubuntu;
- Astra Linux Special Edition (Astra Linux SE);
- МСВС;
- Red Hat Linux;
- CentOS;
- Fedora;
- Gentoo;
- ArchLinux;
- Альт Линукс СПТ.

В связи с постановлением Правительства РФ от 16 ноября 2015 года № 1236 «Об установлении запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд» установлен запрет на допуск программ для ЭВМ, БД и программного обеспечения (ПО), происходящих из иностранных государств, для целей осуществления

закупок для обеспечения государственных и муниципальных нужд. Исключение делается только в двух случаях:

- если в едином реестре российских программ для электронных
  вычислительных машин и баз данных отсутствуют сведения о ПО того же класса, что и ПО, планируемое для закупки;
- если ПО, сведения о котором включено в единый реестр российских программ для электронных вычислительных машин и баз данных, и класс требуемого ПО соответствует классу закупаемого ПО, но по своим функциональным, техническим и/или эксплуатационным характеристикам не соответствует требованиям, установленным заказчиком[15].

Исходя из представленного постановления, в работе могут использоваться только Astra Linux SE, Альт Линукс СПТ. ОС МСВС отсутствует в реестре лишь по той причине, что она разработана специально для Министерства Обороны РФ, и не доступна для свободного распространения. Но ее так же можно отнести к данному списку. Представленные ОС относятся к ОС, произведенные отечественными исполнителями[18].

Далее рассмотрим данные ОС на предмет соответствия классу защищенности СВТ, подходящий для работы с информацией, содержащей государственную тайну с грифом «совершенно секретно», – третьему классу (п. 1.2.2):

- ОС специального назначения «Astra Linux SE» соответствует требованиям к ОС третьего класса защиты (сертификация ФСТЭК);
- ОС «Альт Линукс СПТ» соответствует требованиям к ОС четвертого класса защиты (сертификация ФСТЭК);
- ОС «МСВС» соответствует требованиям к ОС третьего класса защиты (сертификат МО)[19].

Из представленных ОС исключается Альт Линукс СПТ. Astra Linux SE и МСВС соответствуют необходимым для работы требованиям. Рассмотрим их подробнее.

1.5.1. ОС Astra Linux SE

Операционная система специального назначения (ОС СН) Astra Linux Special Edition – операционная система специального назначения на базе ядра Linux, предназначенная для применения в АС в защищенном исполнение, обрабатывающих информацию, которая составляет государственную тайну с грифом секретности «совершенно секретно» [21]. ОС разработана открытым акционерным обществом «Научно–производственное объединение Русские базовые информационные технологии» (НПО РусБИТех) в 2010 году. За последующие несколько лет вплоть до текущего года было выпущено еще 5 версий ОС до 1.6 (дата выхода – 26 сентября 2018 года) [22].

ОС Astra Linux SE прошла проверку на соответствие требованиям и имеет следующие сертификаты:

- сертификат ФСТЭК России № 2557 от 27.01.2012. Действителен до 2018 года;
- сертификат ФСБ СФ/14–2579 от 20.03.2015. Действителен до 2018 года;
- сертификат Минобороны России № 1339 от 24.09.2010. Действителен до 2018 года.

В 2013 году Приказом Министра обороны Российской Федерации № 475 ОС СН принята на снабжение Вооруженных Сил Российской Федерации[23].

Данная ОС используется в таких министерствах, ведомствах, агентствах и специальных службах, как Минобороны России, ФСБ России, ФСО России, МВД России, ФСИН России, ФТС России, Роскосмос, Внутренние войска МВД России. Так же данную системы используют межведомственная информационная система ГАС ГОЗ, национальный центр управления обороной РФ, госкорпорации, предприятия оборонно–промышленного комплекса, и прочие коммерческие предприятия, заботящиеся о безопасности своих информационных ресурсов.

В ОС Astra Linux SE дискреционное разграничение доступа обеспечивает необходимую проверку дискреционных правил доступа, которые формируются в виде базовых ПРД ОС семейства Linux. Для формирования дискреционных правил доступа Astra Linux использует списки контроля доступа (Access control list – ACL), а также механизм системных привилегий Linux. В состав ОС СН включены защищенные комплексы программ системы

управления базами данных (СУБД), гипертекстовой обработки данных и электронной почты[21].

В защищенных комплексах программ гипертекстовой обработки данных и электронной почты объектами защиты являются объекты файловой системы. Дискреционный механизм разграничения доступа реализуется к ним так же, как и к прочим объектам системы.

Реализация мандатного механизма разграничения доступа, как и дискретного механизма разграничения доступа, осуществлена в ядре ОС и СУБД. Допуск или запрет допуска субъекта к объекту принимаются на основе операций чтения, записи и исполнения, мандатного уровня допуска субъекта и мандатного уровня секретности объекта.

Мандатный механизм разграничения доступа в защищенных комплексах программ электронной почты, гипертекстовой обработки данных и в других сервисах осуществлен на основе PARSEC, программного интерфейса библиотек подсистемы безопасности[24].

В состав дистрибутива Astra Linux SE входит СУБД PostgreSQL, доработанная в части мандатного разграничения доступа к информации (пункт 1.6) НПО РусБИТех.

1.5.2. ОС МСВС

ОС МСВС (Мобильная Система Вооружённых Сил) – защищенная операционная система общего назначения, предназначенная для построения мобильных и

стационарных защищенных АС. обрабатывающих информацию, которая составляет государственную тайнуы с грифом секретности «совершенно секретно». ОС разработана ЗАО «концерн ВНИИНС (Всероссийский научно–исследовательский институт автоматизации управления в непромышленной сфере имени В. В. Соломатина)» на основе дистрибутива Red Hat Linux в 2002 году. Последним релизом стала ОС МСВС 5.0 изм. № 7 в 2013 году.

ОС МСВС 3.0 имеет сертификацию МО РФ №2074 от 15.01.2013. ОС МСВС 5.0 имеет сертификацию МО РФ №2227 от 18.10.2013.

Приказом Министра обороны Российской Федерации № 475 в 2002 году ОС МСВС 3.0 принята на снабжение Вооруженных Сил Российской Федерации.

Данная операционная система была разработана по заказу МО РФ для Вооруженных сил РФ, следовательно, применяется преимущественно на различных военных объектах[18].

Модель дискреционного разграничения доступа в ОС МСВС представляет собой стандартную ХРУ модель. В модели существует 3 категории пользователей при доступе к файлу:

- владелец – пользователь, определяющий права владельца файла;
- группа–владелец – пользователь, определяющий права группы пользователей, которой принадлежит файл;
- остальные пользователи – пользователи, которых нельзя отнести к вышеперечисленным категориям.

Так же существуют следующие права :

- право на чтение – r (Read);
- право на запись – w (Write);
- право на исполнение – x (eXecute).

Каждый субъект (пользователь) входит в определенную категорию пользователей и имеет определенный набор правил доступа к объекту (файлу), или вовсе его отсутствие. Для подобных целей ОС МСВС использует списки контроля доступа (Access control list – ACL), как и ОС Astra Linux SE.

В основе механизма мандатного разграничения доступа лежит мандатная модель безопасности Белла–ЛаПадулы. В модели рассмотрены условия, при которых нет возможности создания информационных потоков от субъектов с более высоким уровнем доступа к субъектам с более низким уровнем доступа. Так же выполняются два основных правила NRU (Not Read Up – нет чтения вверх) и NRU (Not Write Down – нет записи вниз).

ВНИИНС разработал СУБД Линтер–ВС целенаправленно для включения ее в дистрибутив ОС МСВС. Данная СУБД была основана на PostgreSQL, путем добавления к ней мандатной модели разграничения доступа[25].

1.5.3. Сравнение Astra Linux SE и МСВС

Проведя сравнительный анализ двух ОС можно сделать заключение о том, что для достижения

поставленных задач наилучшим образом подходит ОС Astra Linux SE, так как:

1) данная ОС имеет наиболее современный программный и пользовательский интерфейс, расширяющий тем самым круги использующих его организаций и технического оборудования для организации АС на основе Astra Linux SE;
2) специалистов по СУБД PostgreSQL значительно больше, чем по СУБД Линтер-ВС, так как PostgreSQL работает на различных UNIX–подобных платформах, в то время как Линтер-ВС работает в основном на МСВС.

Более того, основываясь на мнение пользователей интернет-сообществ обеих ОС, было выявлено, что среднее время поиска решения и устранения проблемы меньше у ОС Astra Linux SE из–за развитого сообщества, что является немаловажным при развертывание системы на конечном объекте[26].

1.6. СУБД PostgreSQL

PostgreSQL – это объектно–реляционная СУБД, основанная на POSTGRES Version 4.2 – программе, разработанной на факультете компьютерных наук Калифорнийского университета в Беркли. Данная СУБД поддерживает множество стандартов SQL множество современных функции в 1989 году.

PostgreSQL – это одна из самых популярных баз данных, к которой добавлены такие виды стандартов, как

SQL–92, SQL:1999, SQL:2003, SQL:2008, SQL:2011. Также PostgreSQL поддерживает не только 160 из 179 обязательных возможностей, но и большое количество необязательных.

Нельзя оставить без внимания и вопрос безопасности. Данная СУБД позволяет работать по защищенному SSL–соединению, поддерживает многие методы аутентификации: аутентификация по паролю, клиентским сертификатам и с помощью ключей внешних сервисов (RADIUS, LDAP, PAM, Kerberos).

При управлении доступом субъектов к объектам PostgreSQL представляет следующие возможности:

- создание и управление, как пользователями, так и групповыми ролями;
- разграничение доступа к объектам базы данных (отдельные пользователи и группы);
- управление доступом на уровне строк и столбцов;
- поддержка SELinux через встроенную функциональность мандатного управления доступом – SE – PostgreSQL[27].

PostgreSQL 9.2 была включена в состав ОС Astra Linux SE 1.4 в качестве защищенной СУБД. Она была доработана в соответствии с требованиями интеграции с данной ОС в части мандатного разграничения доступа[21].

Astra Linux SE вместе с PostgreSQL содержат в сборке специальный патч, который позволяет взаимодействовать с системой, поддерживающей мандатное разграничение, PARCES. СУБД использует механизмы мандатного разграничения ОС для получения пользователем тех же

меток, что и пользователь ОС, который выполнил вход с соответствующими мандатными атрибутами[25].

В основе мандатного механизма находится управление доступом к БД, используя иерархические и неиерархические метки доступа, что позволяет осуществить реализацию многоуровневой защиты. Таким образом, обеспечивается управление информационными потоками и разграничение доступа пользователей к ресурсам БД. При использовании СУБД в ОС в качестве иерархических и неиерархических меток доступа используются метки безопасности ОС. Сама СУБД PostgreSQL не снабжена специальным механизмом хранения, назначения, модификации пользовательских меток. Для этого она использует механизмы ОС.

При создании новых пользователей в системе для них устанавливается минимальный и максимальный допустимый мандатный уровень. При входе в систему определяется текущая метка сессии. В одной сессии может быть только одна метка конфиденциальности[21].

СУБД PostgreSQL в составе ОС Astra Linux SE (далее PostgreSQL) прошла проверку на соответствие требованиям и имеет следующие сертификаты:

- сертификат ФСТЭК России № 2557 от 27.01.2012. Действителен до 27.01.2018 года;
- сертификат ФСБ СФ/14–2234 от 04.10.2013. Действителен до 04.10.2018 года;
- сертификат Минобороны России № 1339 от 24.09.2010. Действителен до 15.09.2018 года.

Основным пользователь рассматриваемой СУБД является Министерство Обороны РФ[29].

2. ПРОЕКТИРОВАНИЕ

2.1. Общие принципы работы с БД

2.1.1. PostgreSQL – объектно-реляционная СУБД

Так как PostgreSQL является объектно-реляционной СУБД, следует рассмотреть подробнее значение данного описания.

Объектно-реляционная СУБД – это реляционная СУБД, которая поддерживает технологии, реализующие объектно-ориентированные расширения, такие как классы, объекты, наследование. Данные подходы реализованы в структуре БД и языке запросов[29].

Реляционная СУБД – это система управления реляционными БД. Данные в такой БД организованы в виде физического набора взаимосвязанных между собой таблиц, каждая из которых содержит информацию об объектах определенного вида, или логической проекции нескольких таблиц[30]. На представленном ниже рисунке показаны таблицы «Пункт эксплуатации (ПЭ)», «Тип пункта эксплуатации», «Вид пункта эксплуатации» и взаимосвязи между ними. (Рисунок 3)

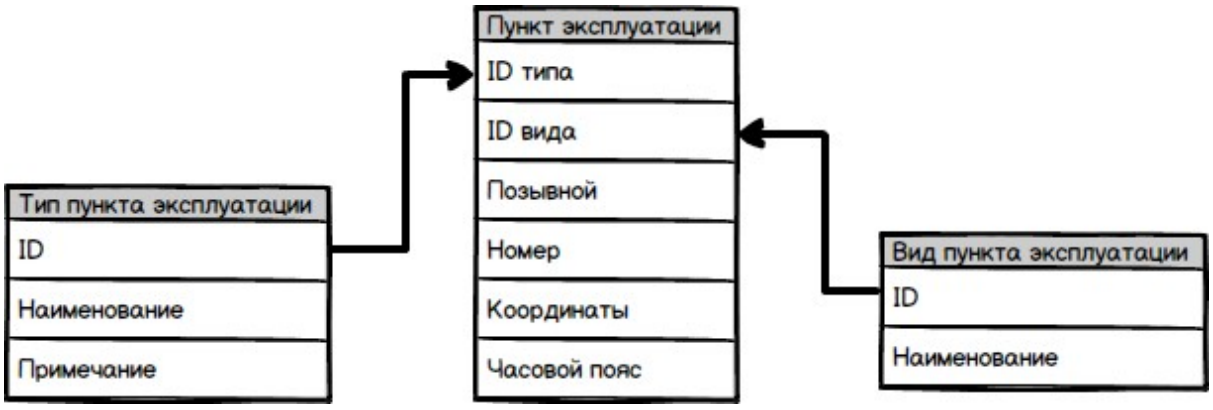

Рисунок 3 – Реляционная СУБД

Говоря о мандатном разграничение доступа, следует отметить, что реляционные СУБД имеют несколько уровней разграничения, включая самые малые уровни: запись таблицы (см. п. 2.1.2). В этом заключается преимущество реляционных СУБД перед объектно-ориентированными СУБД в части организации мандатной политики (см. п. 2.1.3).

Реляционная СУБД является наиболее распространенной. По результатам исследований компании IDC в 2009 году на основе реляционной СУБД создано большое количество крупных проектов. Около 7% – проекты, использующие СУБД нереляционного типа[31].

Объектно-ориентированные расширения реализуются собственно в объектно-ориентированной СУБД. Информация в такой БД представлена в виде объектов и их свойств, то есть каждая таблица является объектом, а каждое поле в таблице – свойством объекта. (Рисунок 4)

Пункт эксплуатации	Позывной	Номер	Координаты	Часовой пояс	Тип	Вид
ПЭ1	БАРС-15	512	57.98480802; 36.97998047	UTC+3	Гражданский	Наземный
ПЭ2	ЛУЧ-3	33	59.32198054; 45.39550781	UTC+4	Военный	Воздушный
ПЭ3	ОРЕЛ-8П	645	54.36455783; 29.73610057	UTC+2	Гражданский	Воздушный

Рисунок 4 – Объектно-ориентированная СУБД

На рисунке изображена таблица, содержащая пункты эксплуатации и их свойства (позывной пункта, номер, координаты его расположения, часовой пояс, тип и вид пункта). Такой подход хранения данных зачастую используется в тех случаях, когда необходима высокая производительность обработки данных, которые имеют сложную структуру. Но при организации мандатной

политики на уровне записей таблицы возникают некоторые трудности, которые не всегда позволяют правильно реализовать данный вид разграничения доступа (пункт 2.1.3).

Основными объектными расширениями считаются:

- возможность определения пользовательских типов данных, в том числе структурных;
- использование коллекций объектов.

Средства, при помощи которых происходит определение типов данных, скорее снимают ограничения с прежних реализаций реляционных моделей данных, чем расширяет их теоретическое представление. Возможность создания структурных типов данных означает, что в БД могут быть созданы, например, геометрические объекты, такие как точки, прямые и так далее.

Под коллекциями подразумеваются наборы объектов определенного типа. Также существуют функции, которые преобразуют коллекции в виртуальные таблицы, а результаты запросов позволяют записывать в качестве значений коллекции.

На данный момент большинство высокопроизводительных систем, включая PostgreSQL, осуществляют реализацию объектного расширения, таким образом, они являются объектно-реляционными БД.

2.1.2. Подходы к проектированию БД в части мандатного разграничения доступа

При проектировании БД существуют две основные проблемы, которые решаются в процессе проектирования:

- Как именно отобразить объекты предметной области в объекты базы данных, чтобы последние не противоречили смысловому значению предметной области, и было наилучшим ее представлением. Зачастую данную проблему проектирования называют логическим проектированием;
- Каким образом обеспечить эффективное выполнение запросов к БД, то есть, как в конкретной БД расположить данные во внешней памяти, какие дополнительные структуры потребовать и тому подобное? Представленную проблему называют проблемой физического проектирования БД[32].

Если в части логического проектирования можно использовать стандартный принцип проектирования для всех СУБД, то при физическом проектировании многое зависит от используемой СУБД.

Рассмотрим, каким образом при физическом проектировании осуществляется хранения данных, содержащих метки конфиденциальности, и доступ к этим данным пользователей с определенным уровнем допуска в доработанной СУБД PostgreSQL, входящей в состав ОС Astra Linux SE.

Существует 4 видов разграничения доступа в СУБД:

- сервер СУБД;

- БД;
- таблица;
- запись таблиц[33].

Максимальным уровнем разграничения в PostgreSQL является БД, минимальным – запись в таблице[27].

Разграничение на уровне БД представлено на рисунке 5.

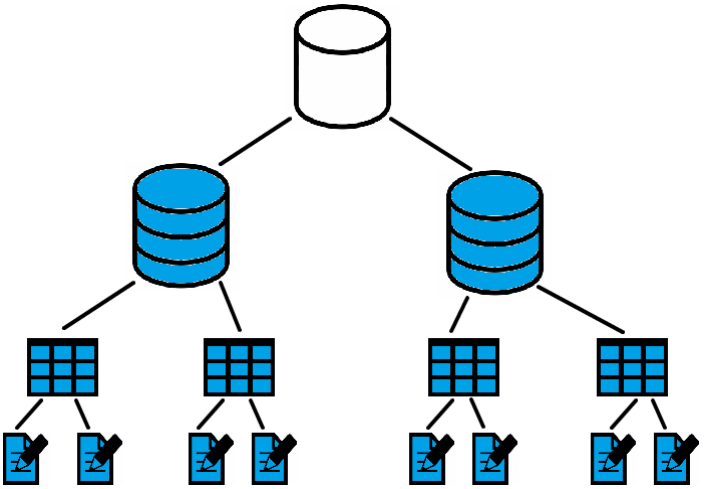

Рисунок 5 – Разграничение доступа на уровне БД

В данном случае для каждого уровня конфиденциальности существует своя БД. Пользователь, обладающий правами доступа к БД, также обладает правами доступа к каждому элементу БД.

Разграничение на уровне таблиц означает, что для каждого уровня конфиденциальности выделена своя схема и набор таблиц. Пользователь обладает правами только к тем таблицам, метки конфиденциальности которых соответствуют меткам допуска пользователя. (Рисунок 6)

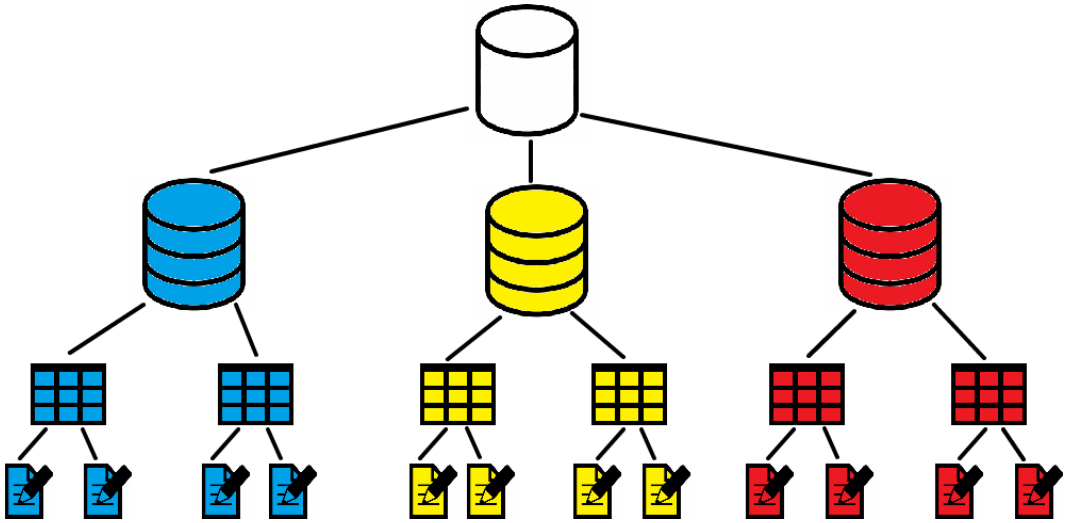

Рисунок 6 – Разграничение доступа на уровне таблиц

Разграничение на уровне записей таблицы представлено следующим образом: схемы таблиц БД и сами таблицы могут содержать в себе строки, относящиеся к разным уровням конфиденциальности. Метка конфиденциальности таблицы соответствует самой высокой метке хранимой в ней записи. Пользователь имеет права допуска только к тем записям, метки конфиденциальности которых соответствуют меткам допуска пользователя. (Рисунок 7)

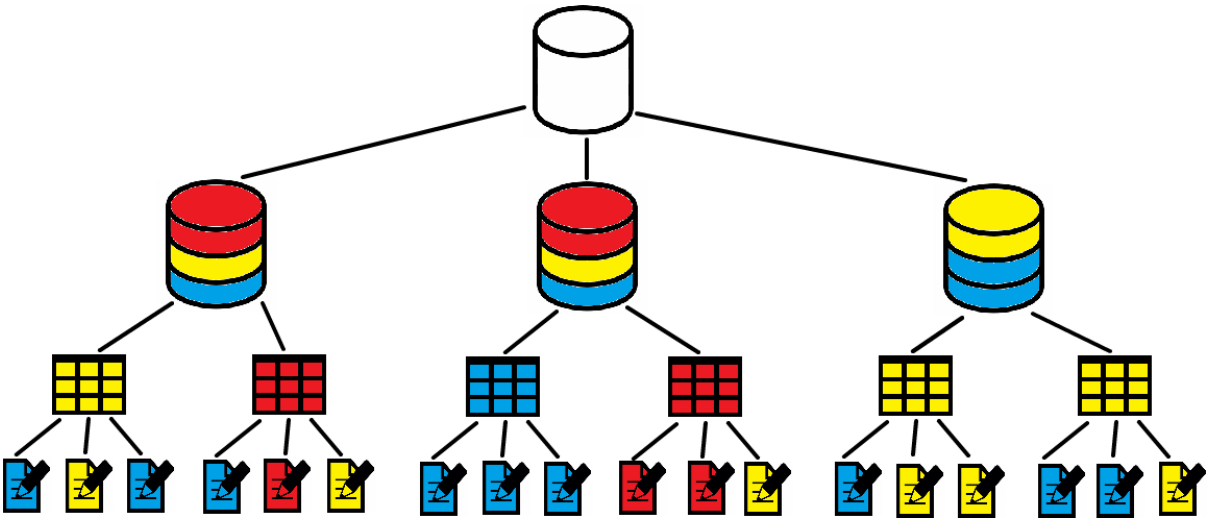

Рисунок 7 – Разграничение доступа на уровне записей таблиц

В представленной работе разграничение доступа к БД будет происходить на уровне таблицы (пункт 2.2.2).

2.1.3. Реализация мандатной модели разграничения доступа на уровне таблиц

2.1.3.1. Сравнение реляционной БД и объектно-ориентированной БД в части разграничения доступа на уровне записи в таблице.

Возвращаясь к вопросу преимущества реляционных СУБД перед объектно-ориентированными в части разграничения доступа рассмотрим мандатное разграничения доступа на уровне записей, которое наиболее ярко отражает разницу между двумя видами БД.

В реляционной БД мандатная метка присваивается каждой единице конкретного уровня конфиденциальности и имеет определенное значение. В представленной работе рассмотрено 3 значения: «совершенно секретно» (2), «секретно» (1) и «несекретно» (0). (Рисунок 8)

Рисунок 8 – Таблица реляционной БД

Из рисунка видно, что поля «Номер» и «Часовой пояс» ПЭ представляют собой несекретные сведения, «Позывной» – секретные, «Координаты» – совершенно секретные. Следовательно, допуск к ним имеют пользователи, имеющие соответствующую метку конфиденциальности.

В объектно-ориентированной БД осуществить мандатное разграничение доступа на уровне записей не так просто. Трудность состоит в том, что нельзя выделить поле и присвоить ему мандатную метку. Мандатная метка может быть присвоена либо определенной строке, либо определенному столбцу. (Рисунок 9)

Пункт эксплуатации	Позывной	Номер	Координаты	Часовой пояс	Тип	Вид
ПЭ1	БАРС-15	512	57.98480802; 36.97998047	UTC+3	Гражданский	Наземный
ПЭ2	ЛУЧ-3	33	59.32198054; 45.39550781	UTC+4	Военный	Воздушный
ПЭ3	ОРЕЛ-8П	645	54.36455783; 29.73610057	UTC+2	Гражданский	Воздушный

Рисунок 9 – Таблица объектно-ориентированной БД

Решением является выделение некоторых свойств объектов в отдельную таблицу, обращаться к которой основная таблица будет при помощи назначенного идентификатора. В таком случае, мандатное разграничение накладывается на строки или столбцы выделенной таблицы. Но данная реализация требует достаточно больших затрат времени, соответственно, и денег, что не каждая организация может себе позволить. Поэтому, когда речь заходит об АС, обрабатывающих информацию, которая содержит государственную тайну, целесообразнее проектировать БД, основываясь на реляционной модели данных, так как реализация

мандатного механизма разграничения доступа будет необходима[13].

2.1.3.2. Мандатное разграничение доступа на уровне таблиц

Учитывая два основных правила мандатной политики («нет чтения вверх» и «нет записи вниз») можно описать ряд возможных ситуаций пользовательских запросов с разным уровнем допуска к разноуровневой информации:

1) Запрос на чтение

- при запросе пользователем данных с грифом секретности, находящимся выше уровня допуска пользователя, система возвращает ошибку доступа;
- при запросе пользователем данных с грифом секретности, не находящимся выше уровня допуска пользователя, система возвращает запрошенные данные;
- при запросе пользователем данных, составляющих совокупность данных с более высоким и соответствующим уровню допуска пользователя грифом секретности, система возвращает ошибку (Приложение Б).

2) Запрос на запись

- при запросе пользователем данных с грифом секретности, находящемся ниже уровня допуска пользователя, система возвращает ошибку доступа;
- при запросе пользователем данных с грифом секретности, не находящимся ниже уровня допуска

пользователя, система возвращает запрошенные данные;

- при запросе пользователем данных, составляющих совокупность данных с более низким и соответствующим уровню допуска пользователя грифом секретности, система возвращает ошибку (Приложение Б).

2.2. Описание предметной области и составление концептуальной модели БД

Предметной областью в данной работе является «управление беспилотными кораблями (БК)». В связи с развитием областей применения беспилотных аппаратов во многих сферах человеческой деятельности становится актуальной задача планирования управления такими аппаратами. Управление БК осуществляется с наземных пунктов управления, которые выдают программы работ на БК через сеть наземных средств связи (СС), размещенных на ПЭ.

Управление происходит следующим образом:

- заказчик подает заявку на сеанс связи с БК (СС, БК, дата и время, когда он хочет осуществить связь);
- перечень таких заявок формируется в некий план, составляющий перечень сеансов связи, кораблей, определенных СС в определенное время и передается на ПЭ;
- заказчику отправляется выписка из плана, содержащая сведения о сеансе связи;

- ПЭ в свою очередь осуществляет сеансы связи с БК через СС связи, которые размещены на нем.

Представленные действия осуществляются в связи с тем, что количество СС, управляющих кораблями существенно меньше, чем количество кораблей, а количество сеансов связи значительно. В результате необходимо координировать сеансы связи между разными БК. Таким образом, составляется план, в котором разрешаются конфликты между разными заявками от заказчика.

Разные корабли обслуживаются разными типами СС, которые могут быть объединены в комплекс СС (КСС).

Необходимо учесть, что СС периодически требуют ремонта, могут выходить из строя. ПЭ средств могут так же выводиться из эксплуатации для проведения сезонного технического обслуживания. Аппаратура связи на кораблях может оказаться неисправной. Все такие события необходимо учитывать как ограничения. Эти ограничения должны учитываться при планировании задействования СС.

2.2.1. Описание объектов

На основе представленной предметной области построена концептуальная модель данных. (Рисунок 10)

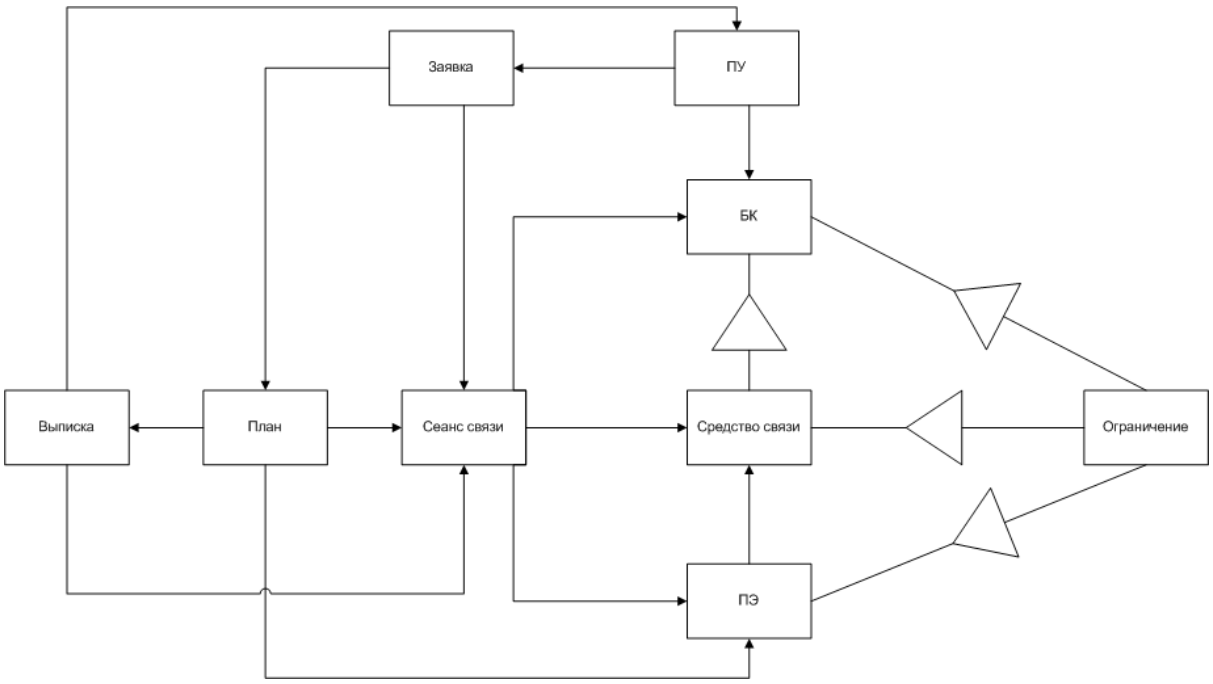

Рисунок 10 – Концептуальная модель данных

Данная модель представляет собой совокупность информационных объектов и их взаимосвязей, исключая способы описания и хранения данных[34].

К объектам модели относятся (Таблица 2):

Таблица 2 – Объекты концептуальной модели

Наименование	*Описание*
БК	Морское или речное судно, оборудованное системой автоматического управления, которое может осуществлять передвижение и выполнение поставленных для него задач без участия человека

Продолжение таблицы 2

Наименование	*Описание*
Заявка	Сообщение о желании заказчика осуществить сеанс связи с кораблем с определенного средства
План	Заранее составленный перечень сеансов связи, где указано, какое СС на каком ПЭ с каким БК в какое время осуществляет сеанс связи
Выписка	Часть плана, содержащая сведения о сеансе связи с кораблем по заявке заказчика
Сеанс связи	Осуществление связи СС с БК в определенный промежуток времени
СС	Средство, предназначенное для поддержки связи и обмена информацией заказчика с БК
ПЭ	Специально подготовленное и оснащенное место, содержащее в себе набор СС, с помощью которых осуществляется сеанс связи с кораблем
Ограничение	Правило, ограничивающие какие-либо действия с ПЭ, БК или СС
П р и м е ч а н и е: ПУ – пункт управления	

Конечной задачей разработки концептуальной модели является установление минимального количества основных таблиц БД[34]. В данном случае существует 9 таблиц.

2.2.2. Описание субъектов

На основе концептуальной модели выделены субъекты БД и создана модель взаимодействия субъектов через объекты. (Рисунок 11)

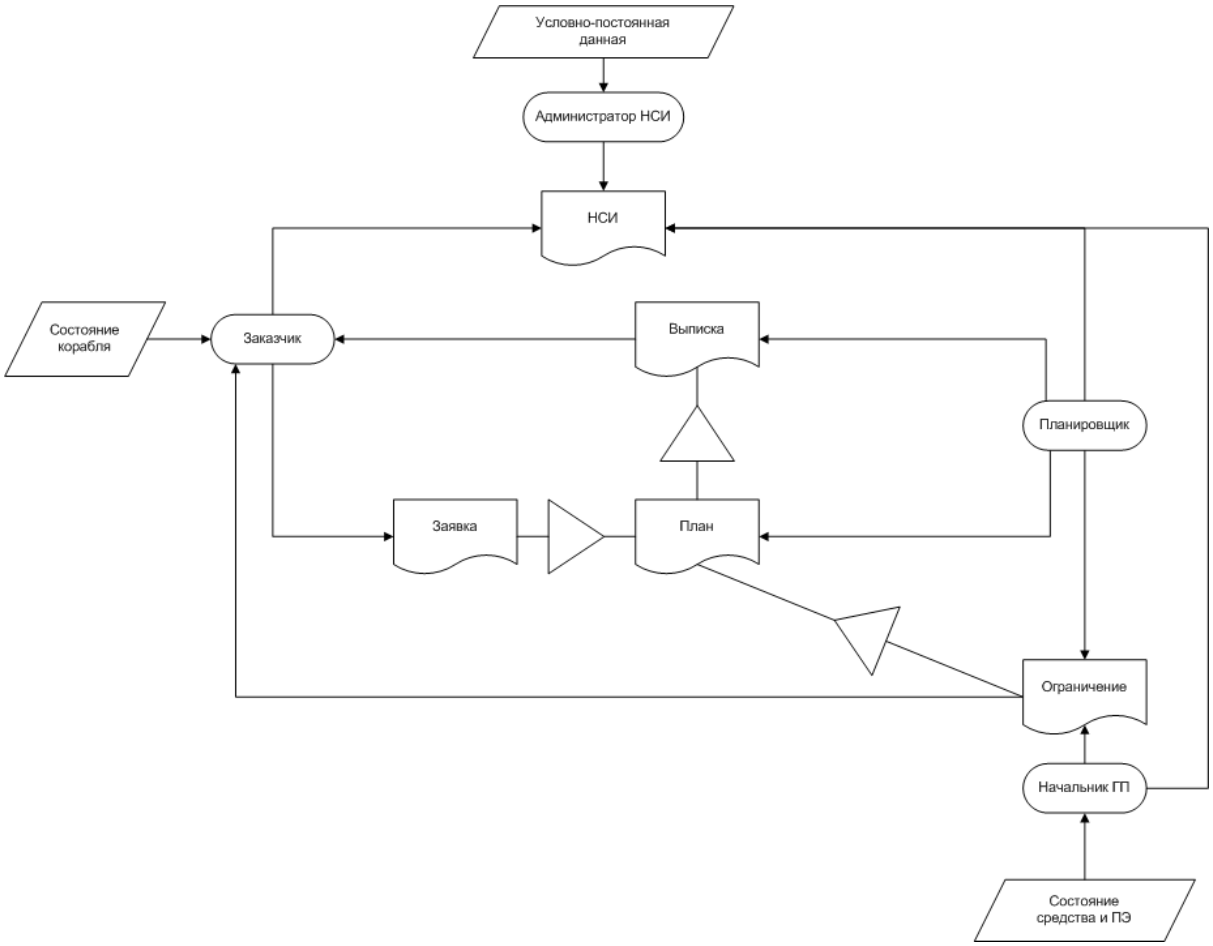

Рисунок 11 – Модель взаимодействия субъектов через объекты

Модель взаимодействия субъектов через объекты отображает перечень задействованных в БД субъектов и используемых ими объектов в процессе управления БК. Описание данной модели представлено в таблице 3.

Таблица 3 – Взаимодействие субъектов с объектами

Наименование субъекта	*Описание субъекта*	*Используемые объекты*
Заказчик	Лицо, заинтересованное в выполнение сеанса связи с кораблем через СС	Отслеживает состояние определенного корабля, создает заявки на получение сеанса связи с кораблем с определенного СС, получает выписку из плана, где указан сеанс связи. Работает на основе НСИ.
Планировщик	Лицо, планирующие сеансы связи	Получает заявки от заказчика и, учитывая ограничения на средства связи и ПЭ, формирует план работы средств. Работает на основе НСИ.
Начальник ГП	Лицо, отвечающее за формирование ограничений на средства связи, ПЭ и корабли,	Получает информацию о состояние средств и ПЭ, формирует ограничения на основе состояния. Работает на

	утверждение и рассылку плана	основе НСИ.

Продолжение таблицы 3

Наименование субъекта	*Описание субъекта*	*Используемые объекты*
Администратор НСИ	Лицо, управляющее ведением нормативно-справочной информации в целях реализации проектных работ	Получает условно-постоянные данные и формирует из них структурированную нормативно–справочную информацию
Примечание: ГП – группа планирования; НСИ – нормативно-справочная информация.		

Из таблицы видно, что субъектов интересуют разные объекты, но им также необходим разный уровень доступа к таблицам других субъектов для осуществления своей деятельности. Руководствуясь этими требованиями, был выбран метод разграничения доступа на уровне таблиц.

2.3. Логическая модель БД

Логическая модель БД отражает логические связи между множеством таблицами. Таблица БД – это двумерный массив, который содержит информацию об одном классе объектов, состоящий из полей (столбцов), записей (строк) и ячеек. Число таблиц в одной базе зависит от следующих основных факторов:

- пользовательский состав БД;

- обеспечение информационной целостности;
- обеспечение наименьшего возможного объема памяти, необходимого для обработки данных, а также минимальное время их обработки.

При проектировании БД необходимо учитывать данные факторы методами нормализации таблиц и установление связей между ними. Нормализация таблиц – это способы разделения таблиц на несколько таблиц, отвечающих представленным выше требованиям. Существует 6 форм нормализации БД, но, как правило, на практике ограничиваются тремя первыми формами. Рассмотрим их подробнее.

Первая нормальная форма. Таблица находится в первой нормальной форме тогда, когда все поля содержат не более одного значения, и все ключевые поля не являются пустыми.

Вторая нормальная форма. Таблица находится во второй нормальной форме тогда, когда она удовлетворяет требованиям первой нормальной формы и все ее поля, которые не являются первичным ключом, связаны полной функциональной зависимостью с первичным ключом.

Третья нормальная форма. Таблица находится в третьей нормальной форме тогда, когда она удовлетворяет требованиям первой и второй нормальных форм и все ее не ключевые поля не зависят функционально от других не ключевых полей.

Ключ (ключевое поле) – это поле, значения которого однозначно определяют значения всех других полей в таблице.

Что касается связей, устанавливающихся между таблицами, существует следующие три типа связей:

- связь «один к одному». Данная связь устанавливается в том случае, когда определенная строка главной таблицы связана только с одной строкой подчиненной таблицы в любой момент времени;
- связь «один ко многим». Данная связь устанавливается в том случае, когда определенной строка главной таблицы связана с несколькими строками подчиненной таблицы в любой момент времени, но любая строка подчиненной таблицы связана только с одной строкой главной таблицы;
- связь «многие ко многим. Данная связь устанавливается в том случае, когда определенная строка главной таблицы связана с несколькими строками подчиненной таблицы в любой момент времени, а любая строка подчиненной таблицы также связана с несколькими строками главной таблицы[34].

Следуя выше представленным правилам нормализации и установления связей между таблицами, концептуальная модель была расширена до уровня логической модели. (Приложение В)

В схеме логической модели продемонстрировано конечное множество таблиц (35), и различные виды связей между ними. Каждая таблица (сущность) имеет ряд свойств (атрибутов), которые будут представлены в виде полей таблиц в БД. Подробное описание таблиц и их свойств приведено в приложение Г.

2.3.1. Дискреционное разграничение доступа на основе логической модели БД

На основе полученной логической модели данных была выявлена дискреционная модель разграничения доступа. (Приложение Д)

Таблица наглядно демонстрирует на какие объекты какие субъекты имеют доступ на чтение (r – read) и/или запись (w – write), а на какие вовсе не имеют каких–либо прав.

2.3.2. Мандатное разграничение доступа на основе логической модели БД и дискреционной модели разграничения доступа

В СУБД PostgreSQL при добавлении нового пользователя к БД, имеющей мандатное разграничение, пользователю назначается диапазон мандатных меток. В том случае, если пользователю не присвоили мандатную метку, то по умолчанию он имеет только нулевую метку, соответствующую минимальному уровню допуска. Так же устанавливается текущая метка сессии при установлении соединения и сохраняется на все время сессии. Таким образом, каждый пользователь имеет 3 метки: минимальная, максимальная и текущая.

При осуществлении доступа к таблицам БД происходит проверка мандатных прав доступа совместно с проверкой дискреционных прав к ней. Такое правило действует для всех пользователей. Для администратора БД

предусмотрены системные привилегии, которые помогают игнорировать механизм мандатного разграничения доступа, так как существует необходимость производить регламентные работы с БД, такие как восстановление резервной копии. В данном случае требуется установка меток данных, сохраненных ранее[35].

Диапазон мандатных меток субъектов в проектируемой БД представлен в приложении Д.

Из таблицы 8 видно, что самым низкоуровневым пользователем является администратор НСИ. Самыми высокоуровневыми являются заказчик и начальник ГП, а данном случае разграничение прав между ними осуществляет дискреционная модель.

Мандатные метки объектов (таблиц) БД представлены в приложении Д.

2.3.3. Сопоставление дискреционной и мандатной моделей разграничения доступа

В данном пункте рассмотрены два варианта работы дискреционной и мандатной моделей разграничения доступа в проектируемой БД.

1 вариант.

В качестве примера субъекта использован Планировщик. Примерами объектов являются Выписка, Состояние ПЭ, Сеанс связи плана, Ограничение. (Таблица 4)

Таблица 4 – Запрос планировщиком некоторых таблиц

Метки сессии субъекта →	*0*	*1*

Объекты с мандатными метками ↓		
Выписка – 0	rw	r
Состояние ПЭ – 2	w	w
Сеанс связи плана – 1	w	rw
Ограничение – 1	–	r

В таблице представлено взаимодействие дискреционной и мандатной моделей. Например, из дискреционной модели следует, что Планировщику разрешен допуск к Выписке на чтение и запись. Но, так как Выписка имеет мандатную метку 0, то Планировщик, имея мандатную метку сессии 1, не может получить доступ к Выписке на запись, а только на чтение. Или, имея мандатную метку сессии 0, Планировщик не может получить доступ на чтение (запись запрещена дискреционной моделью).

Рассмотрим вариант 2.

В качестве примера субъекта использован Начальник ГП. Примерами объектов являются Координаты СС, Состояние БК, Заявка. (Таблица 5)

Таблица 5 – Запрос начальником ГП некоторых таблиц

Метки сессии субъекта → Объекты с мандатными метками ↓	*0*	*1*	*2*
Координаты СС – 1	w	rw	r
Состояние БК – 2	–	–	r
Тип СС – 0	r	r	r

Из данной таблицы также видно взаимодействие дискреционной и мандатной моделей. Например, из дискреционной модели следует, что Начальнику ГП разрешен допуск к Координатам СС на чтение и запись. Имея метку сессии 1 субъект, обладает данными правами. Находясь же в сессии с меткой 0, Начальник ГП имеет права только на запись, а с меткой сессии 2 – только на чтение.

2.4. Физическая модель БД

Физическая модель БД представляет собой описание способов обработки и хранения информации. Существуют два подходу к построению физических моделей БД: физические модели таблиц БД и физические модели хранения данных. В первом случае подход не связан с конкретной СУБД и предполагает описание физических свойств таблиц. Во втором случае подход связан с конкретной СУБД, а также с разработкой архитектуры, организации и хранения данных[34].

В данной работе используется второй подход, так как модель БД разрабатывается конкретно для PostgreSQL. Физическая модель БД представлена в приложение В.

В представленной схеме так же существует 35 таблиц. Их атрибутам, конечное множество которых было выявлено при проектировании логической модели БД, присвоены следующие типы данных:

- serial – автоинкрементирующееся числовое значение, которое занимает 4 байта и может храниться числа от 1 до 2147483647;
- integer (int4) – числовое значение, которое занимает 4 байта и может хранить числа от –2147483647 до 2147483647;
- double precision (float8) – числа с плавающей точкой из диапазона от 1E–307 до 1E+308. Занимает 8 байт.
- character varying(n) (varchar(n)) – строка из фиксированного количества символов. С помощью параметра задается количество символов в строке;
- date – дата от 4713 года до нашей эры до 5874897 года нашей эры, которая занимает 4 байта;
- time – время с точностью до 1 микросекунды с указанием часового пояса. Принимает значения от 00:00:00+1459 до 24:00:00–1459. Занимает 12 байт;
- boolean – переменная, которая хранит одно из двух значений: true и false.

На данном моменте этап проектирования БД и моделей разграничения доступа закончен. Далее следует этап реализации.

3. РЕАЛИЗАЦИЯ

3.1. Описание используемых средств

Для реализации спроектированной модели БД, а также моделей дискреционного и мандатного разграничения доступа были использованы следующие средства:

- ОС Astra Linux Special Edition (SE) – операционная система специального назначения на базе ядра Linux, предназначенная для применения в АС в защищенном исполнение, обрабатывающих информацию, которая составляет государственную тайну с грифом секретности «совершенно секретно» (пункт 1.5.1);
- СУБД PostgreSQL 9.2 – объектно-реляционная СУБД, являющаяся одной из версий PostgreSQL, которая была включена в состав ОС Astra Linux SE и доработана в соответствии с требованиями интеграции с данной ОС в части мандатного разграничения доступа (пункт 1.6);
- Microsoft Visio – векторный графический редактор, редактор диаграмм и блок-схем для Windows. При помощи данной программы была построена концептуальная модель БД и модель взаимодействия субъектов через объекты;
- Visual Paradigm Standard Edition 11.2 – стандартная версия Visual Paradigm, являющаяся инструментом для построения UML–диаграмм (UML –

унифицированный язык моделирования), поддерживающим UML 2, SysML (Unified Modeling Language – язык моделирования систем) и BPMN (Business Process Model and Notation – нотация и модель бизнес-процессов). При помощи данной программы были построены логическая и физическая модели БД;

- postgresql-9.2-1004–jdbc4.pom – плагин PostgreSQL 9.2, позволяющий произвести преобразование UML–диаграмм в SQL–код и его выгрузку в СУБД.

3.2. Преобразование физической модели БД из UML–диаграммы в SQL–код СУБД PostgreSQL 9.2.

Первым действием при создании БД в СУБД PostgreSQL является создание пустой БД. Реализовать это можно выполнением следующего набора SQL-команд в терминале Fly (ОС Astra Linux SE):

- psql –U postgres template1 – данная команда позволяет выполнить подключение к пустой БД template1, на основе которой будет создана спроектированная БД;
- CREATE DATABASE new – команда, необходимая для создания новой БД с именем new;
- \q – выход из template1[36]. (Рисунок 12)

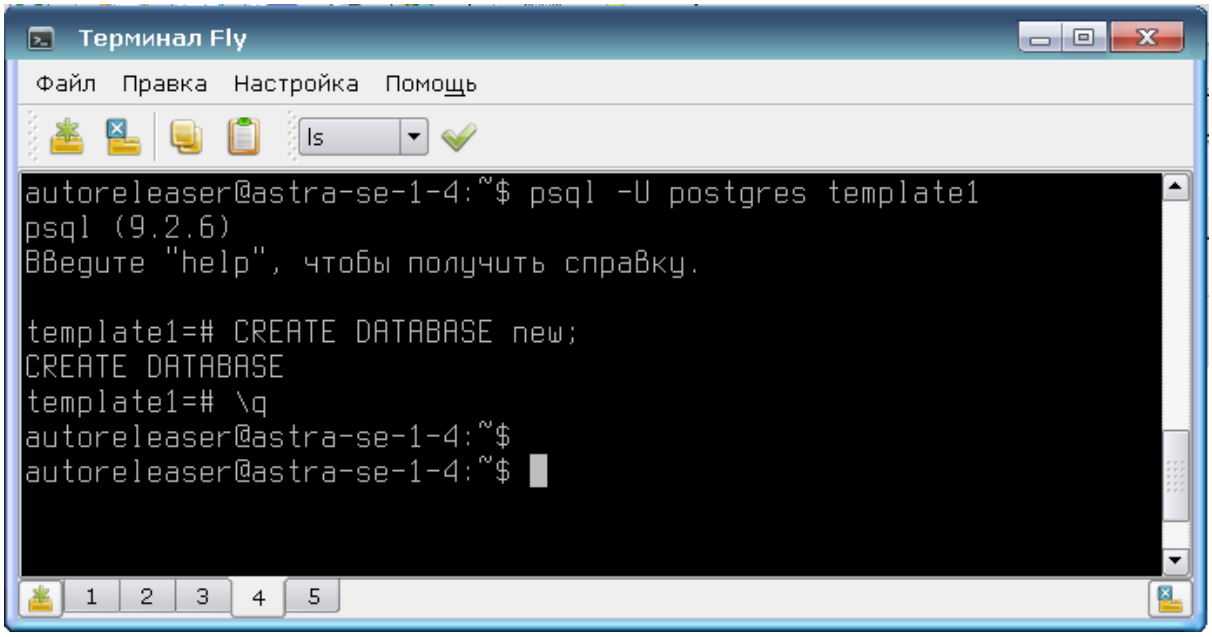

Рисунок 12 – создание БД в СУБД PostgreSQL

Далее в среде Visual Paradigm необходимо соединиться с созданной БД при помощи JDBC соединения. JDBC (Java DataBase Connectivity) – промышленный стандарт взаимодействия Java-приложений с разными СУБД, который не зависит от платформы. Для соединения необходимо ввести IP и порт ОС, а также ее пользователя и пароль. Затем необходимо загрузить плагин postgresql-9.2-1004-jdbc4.pom для данной СУБД. (Рисунок 13)

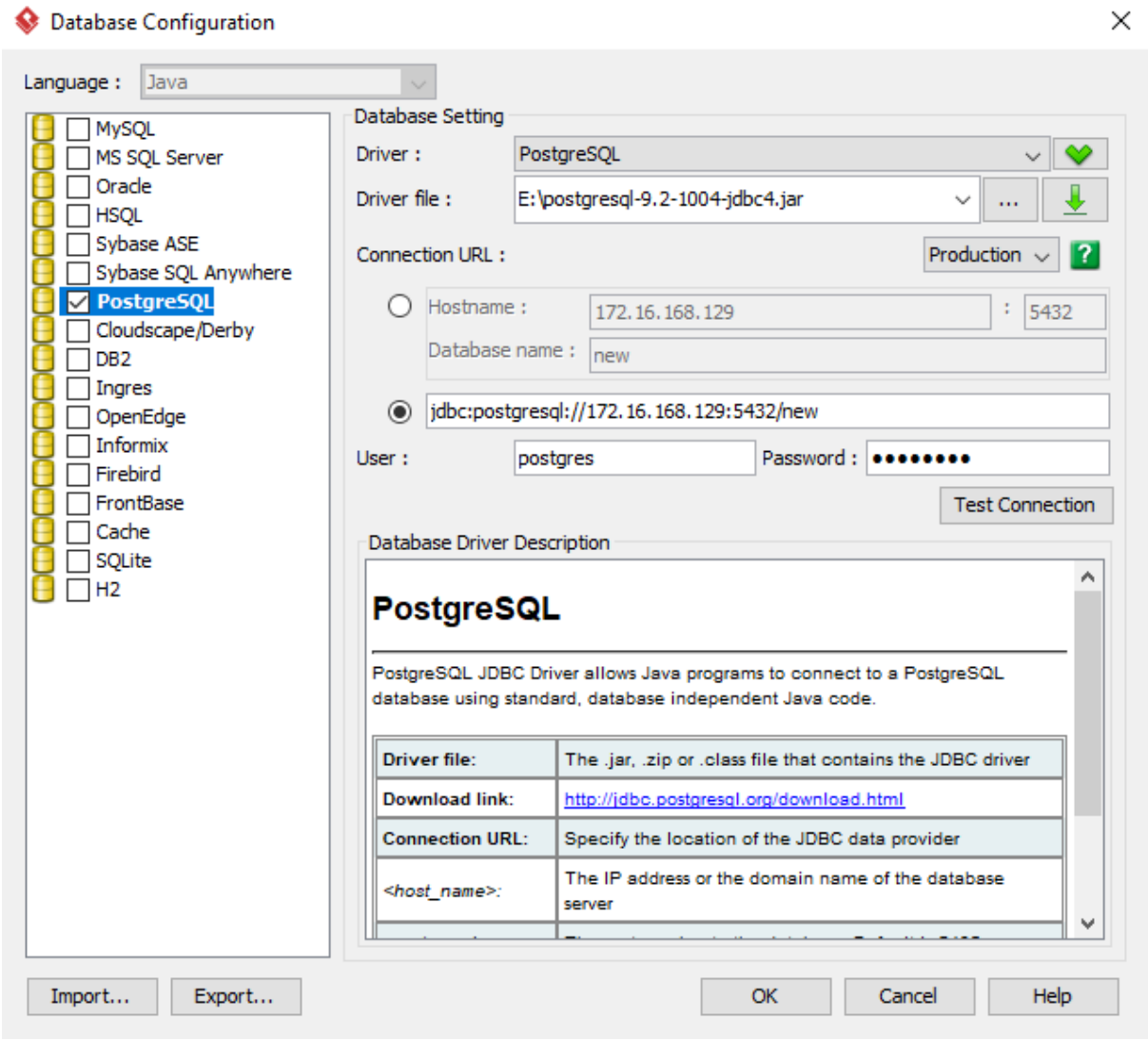

Рисунок 13 – Занесение сетевых данных Astra Linux SE в Visual Paradigm

После происходит проверка соединения Visual Paradigm с базой new на СУБД. (Рисунок 14)

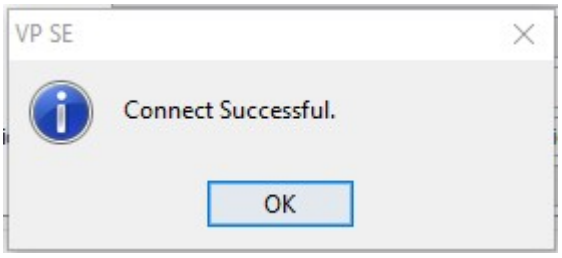

Рисунок 14 – Проверка соединения Visual Paradigm с Astra Linux SE

Из рисунка 14 видно, что соединение прошло успешно. После чего осуществляется генерация SQL кода в СУБД. SQL код представлен в приложение Е.

Из графического интерфейса СУБД pgAdmin III видно, что таблицы были успешно выгружены. (Рисунок 15)

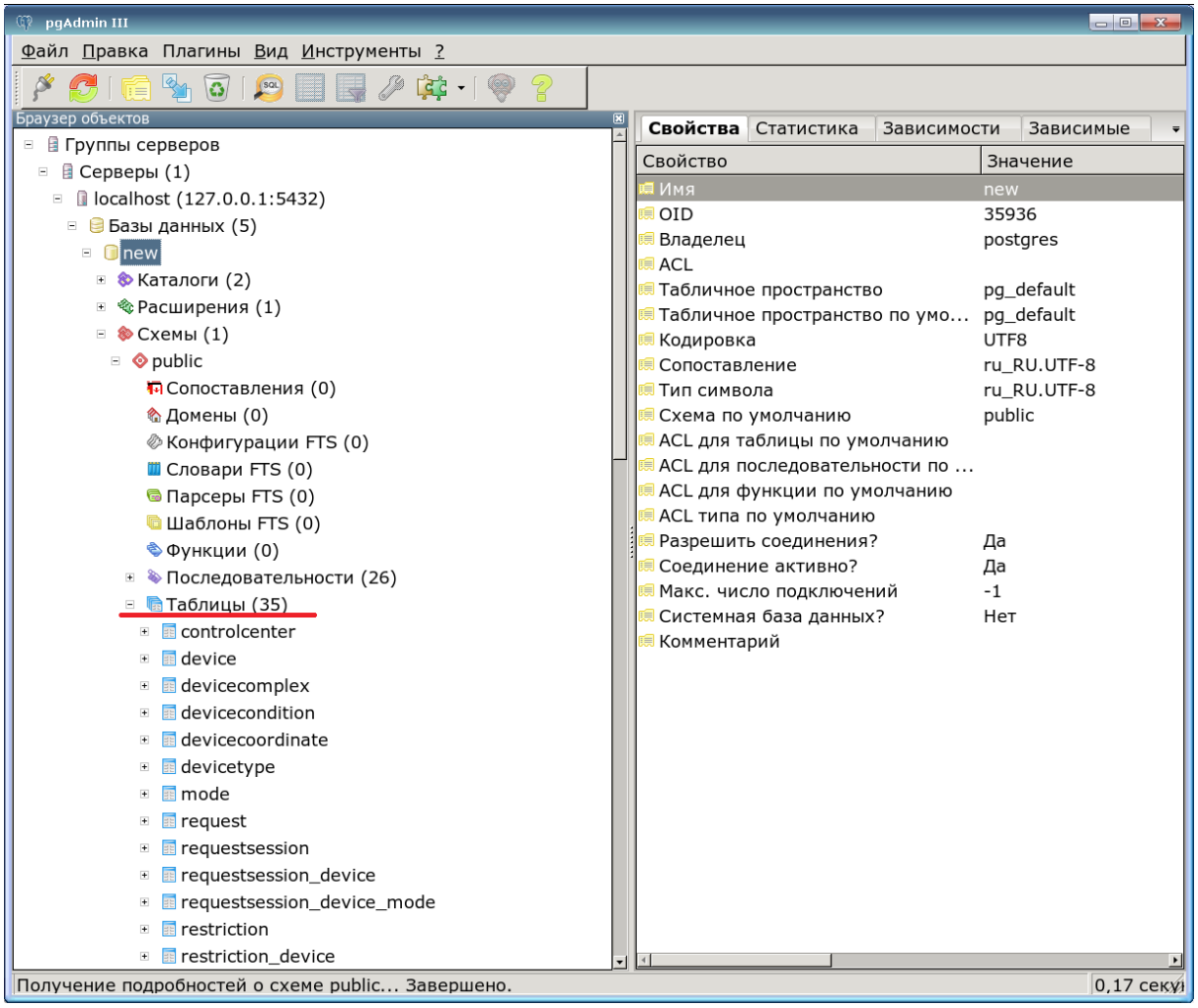

Рисунок 15 – Таблицы спроектированной БД в СУБД PostgreSQL

Далее произведена проверка на корректность таблиц и внесены незначительные правки. После чего таблицы заполняются данными.

3.3. Создание пользователей

Как было сказано в пункте 1.6, СУБД PostgreSQL использует механизм мандатного разграничения ОС для получения пользователем тех же меток, что и пользователь ОС, который выполнил вход с соответствующими мандатными атрибутами. Другими словами, для осуществления работы разноуровневых субъектов с объектами БД необходимо создать пользователей ОС, назначить им диапазон мандатных меток и создать соответствующих пользователям ОС пользователей БД, которые будут использовать метки доступа пользователей ОС.

Таким образом, при попытке пользователя подключиться к БД под своей учетной записью в ОС, система будет требовать авторизацию 2 раза: в ОС и в БД. В БД можно сохранить пароль, но, в целях обеспечения безопасности, этого делать не стоит.

Пользователь ОС

Создание пользователя ОС осуществляется с помощью панели управления Astra Linux SE. Пользователю присваивается Имя и Пароль. (Рисунок 16)

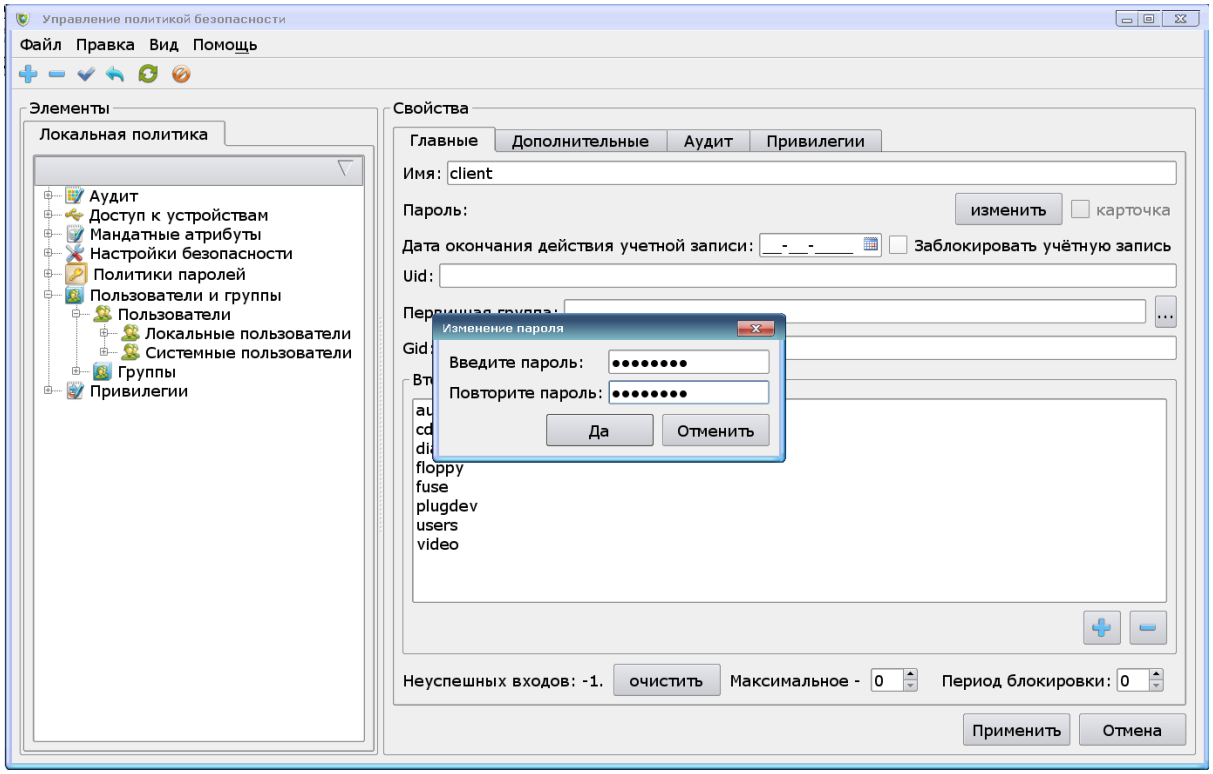

Рисунок 16 – Создание пользователя в ОС Astra Linux SE

П р и м е ч а н и е:

- client – Заказчик;
- planner – Планировщик;
- leader_pt (Planning Team) – Начальник ГП (Группы Планирования);
- administrator_rbi (Regulatory Background Information) – Администратор НСИ (Нормативно-Справочной Информации).

Далее происходит присвоение пользователю максимальной и минимальной мандатной метки в соответствии с таблицей 7. (Рисунок 17)

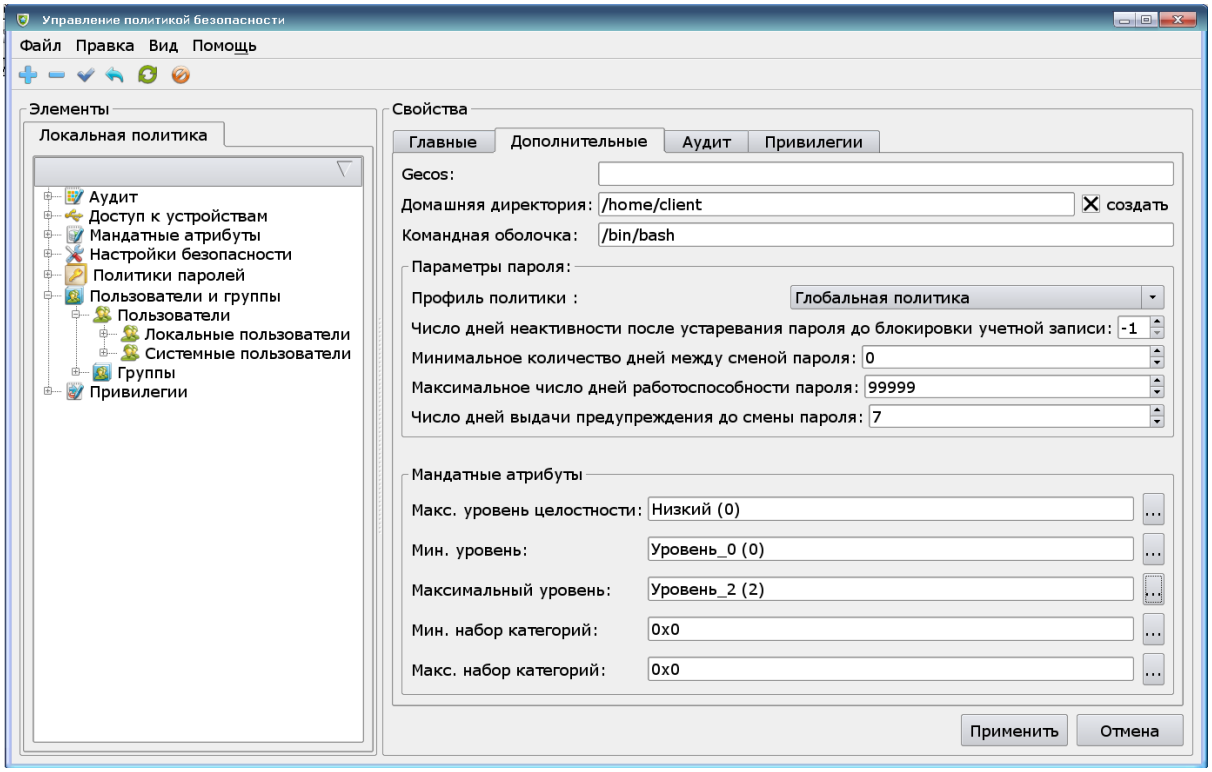

Рисунок 17 – Присвоение пользователю ОС диапазона мандатных меток

По нажатию кнопки «Применить» пользователь сохраняется в системе. Действия по созданию пользователя повторяются со всеми оставшимися пользователями.

Пользователь БД

Создание пользователя БД осуществляется в самой СУБД (pgAdmin III) путем добавление новой роли входа. Роли присваивается Имя. (Рисунок 18)

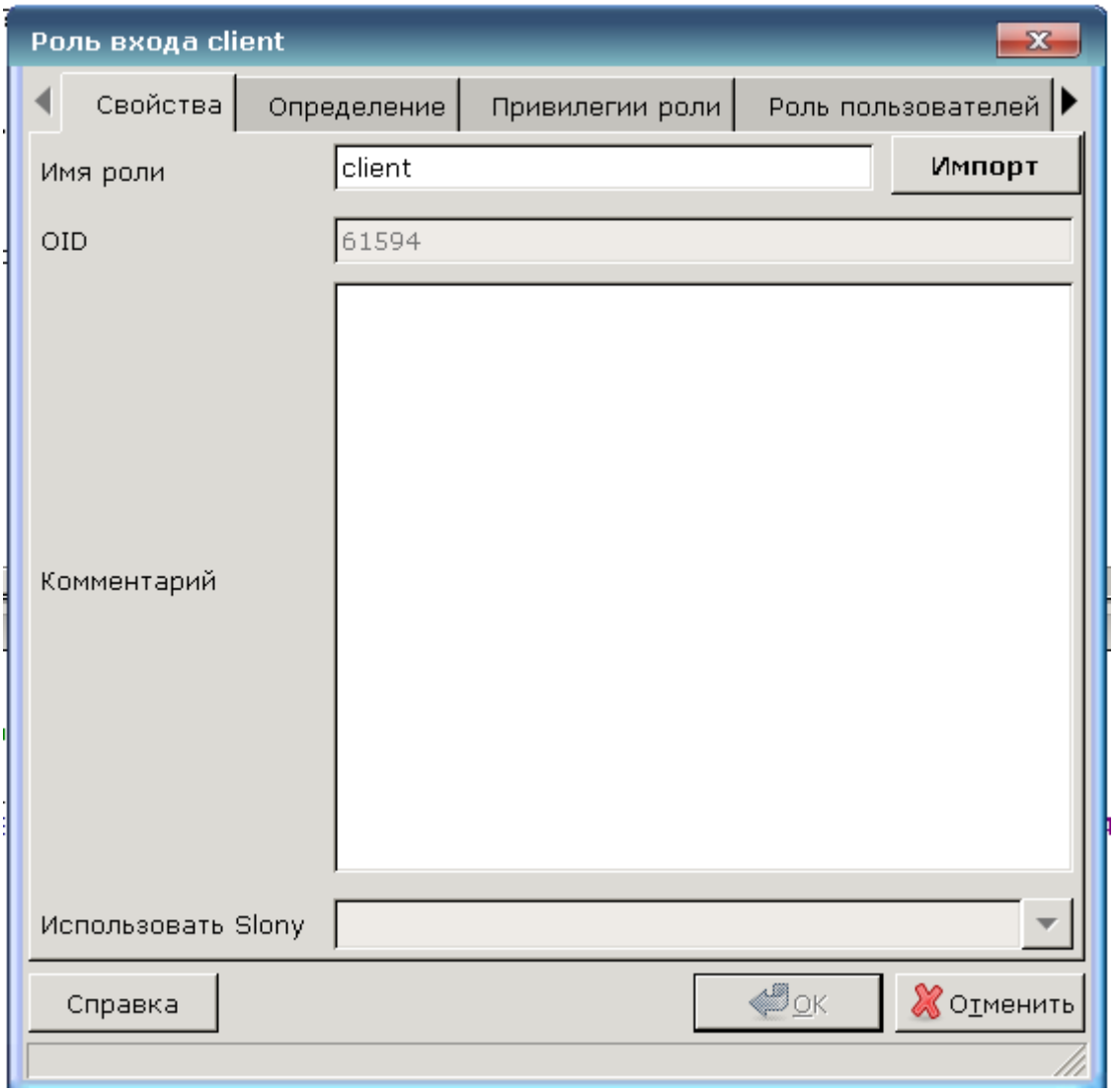

Рисунок 18 – Создание пользователя в БД

После чего происходит присвоение Пароля и Даты, до которой роль будет оставаться активной, иначе СУБД задает параметр даты по умолчанию – следующий день.

По нажатию кнопки «OK» пользователь сохраняется в системе. Действия по созданию пользователя повторяются со всеми оставшимися пользователями.

3.4. Назначение прав доступа (привилегий) пользователям на таблицы – дискреционное разграничение доступа

Так как мандатный контроль определяется только для видов доступа на чтение и запись, все операции с данными в защищаемых объектах сводятся к ним следующим образом:

- SELECT – доступ на чтение (возможен, если метка допуска пользователя больше или равна метке конфиденциальности таблицы);
- UPDATE, DELETE – последовательное выполнение допуска на чтение и запись (возможен, если метка доступа пользователя равна метке конфиденциальности таблицы);
- INSERT – доступ на запись (возможен, если метка допуска пользователя меньше или равна метки конфиденциальности таблицы).

Для присвоения данных привилегий необходимо в свойствах таблицы назначить всем пользователям права или отсутствие прав на таблицу в соответствии с таблицей 6. (Рисунок 19)

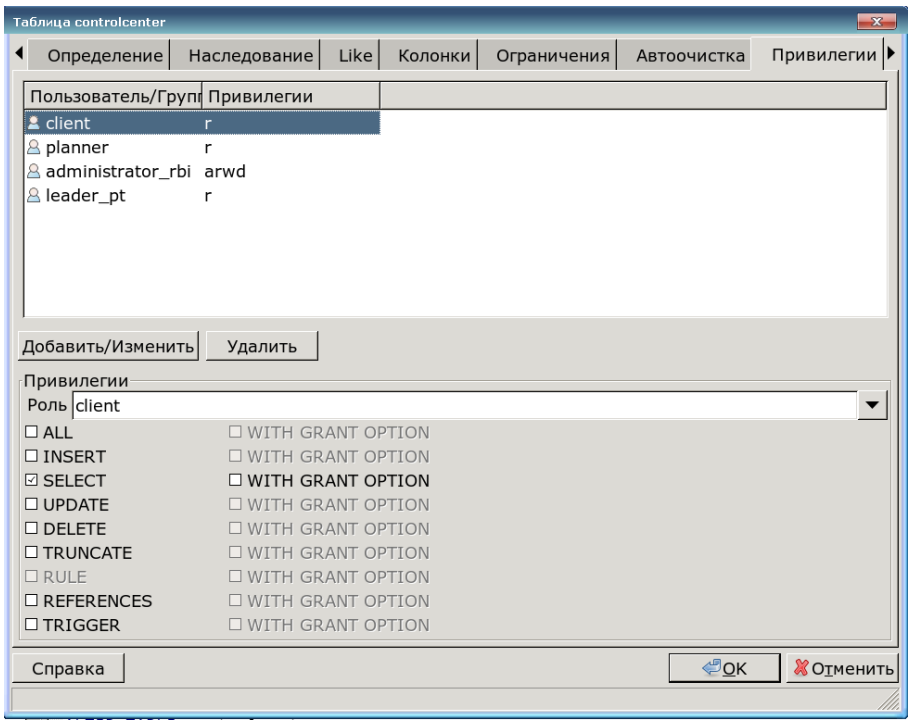

Рисунок 19 – Присвоение привилегий пользователям

По нажатию кнопки «OK» выбранные привилегии сохраняются для выбранных пользователей.

Права также можно присвоить при помощи SQL–запроса:

GRANT *<перечисленный список прав через запятую>* ON TABLE *<наименование таблицы>* TO *«<наименование пользователя>«;*

Представленные действия повторяются для всех таблиц БД.

3.5. Назначение таблицам меток конфиденциальности – мандатное разграничение доступа

Для присвоения мандатных меток таблицам необходимо в свойствах назначить таблице метку

конфиденциальности в соответствии с таблицей 8. (Рисунок 20)

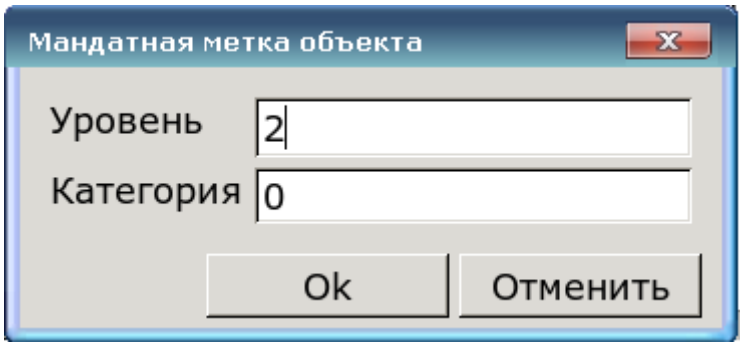

Рисунок 20 – Присвоение мандатных меток таблицам

По нажатию кнопки «OK» выбранная метка таблицы сохраняется.

Права также можно присвоить при помощи SQL-запроса:

ALTER TABLE <*наименование таблицы*> SET MAC TO ‘{<*номер метки*>,0};

Представленные действия повторяются для всех таблиц БД.

На данном этапе система соответствует требованиям, которые необходимы для обработки сведений, составляющих государственную тайну вплоть до грифа «совершенно секретно», в части осуществления контроля доступа субъектов в соответствие с матрицей доступа к защищенным ресурсам и управление потоками информации с помощью меток конфиденциальности.

4. ТЕСТИРОВАНИЕ

Для сравнения полученного результата с заданными требованиями (задачи дипломной работы) были применены два метода верификации – проверка на доступность и проверка на целостность.

Согласно ГОСТ Р ИСО/МЭК 12207–2010 «Информационная технология. Системная и программная инженерия. Процессы жизненного цикла программных средств» верификация (verification) – это подтверждение того, что заданные требования полностью выполнены[37].

Проверка на доступность – проверка на доступ к информации и связанным с ней активам авторизованных пользователей по мере необходимости [38]. В данном случае необходима проверка доступа разноуровневых пользователей к разноуровневым таблицам.

Проверка на целостность – проверка на достоверность и полноту информации [38]. В данном случае осуществляется проверка отображения или неотображения разноуровневых таблиц в одном запросе разноуровневыми пользователями.

Для осуществления проверок необходимо для каждого примера создать новую сессию, авторизоваться в системе путем ввода логина и пароля пользователя и присвоить возможную для данного пользователя метку сессии. (Рисунок 21).

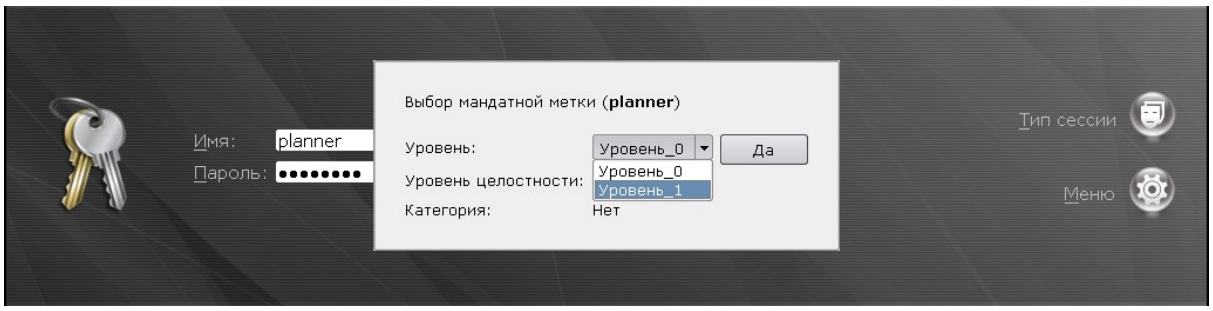

Рисунок 21 – Авторизация в системе

4.1. Проверка доступности

Данный способ проверки осуществляется при помощи SQL-запросов на чтение и запись к таблицам разного уровня конфиденциальности, исходящих от разноуровневых пользователей.

Проверка продемонстрирована на следующих примерах:

1. Планировщик с меткой сессии 0 осуществляет запрос на чтение и запись в таблицу «План» (1) ;
2. Планировщик с меткой сессии 1 осуществляет запрос на чтение и запись таблицы «План» (1);
3. Заказчик с меткой сессии 2 осуществляет запрос на чтение и запись
   «Задача БК» (1);
4. Начальник ГП с меткой сессии 2 осуществляет запрос на чтение и запись к таблице «Состояние БК» (2);
5. Заказчик с меткой сессии 2 осуществляет запрос на чтение и запись к таблице «Состояние БК» (2);
   Примеры подробно рассмотрены в приложение Ж.

Пример 1 – Планировщик с меткой сессии 0 осуществляет запрос на чтение и запись в таблицу «План» (1) ;

Ожидаемый результат: доступ на чтение – запрещен, доступ на запись – разрешен.

Полученный результат полностью соответствует ожидаемому результату: доступ на чтение – запрещен, доступ на запись – разрешен. В данном случае наблюдается в части мандатного разграничения доступа действие правила NRU – «нет чтения вверх», так как уровень конфиденциальности таблицы выше уровня допуска пользователя.

Пример 2 – Планировщик с меткой сессии 1 осуществляет запрос на чтение и запись таблицы «План» (1) ;

Ожидаемый результат: доступ на чтение – разрешен, доступ на запись – разрешен.

Полученный результат полностью соответствует ожидаемому результату: доступ на чтение – разрешен, доступ на запись – разрешен. В данном случае наблюдается в части дискреционного и мандатного разграничения доступа разрешение доступа пользователя на чтение и запись в таблицу. Уровень конфиденциальности таблицы и уровень допуска к ней пользователя совпадают.

Пример 3 – Заказчик с меткой сессии 2 осуществляет запрос на чтение и запись «Задача БК» (1);

Ожидаемый результат: доступ на чтение – разрешен, доступ на запись – запрещен.

Полученный результат полностью соответствует ожидаемому результату: доступ на чтение – разрешен, доступ на запись – запрещен. В данном случае наблюдается в части мандатного разграничения доступа действие правила NWD – «нет записи вниз», так как уровень конфиденциальности таблицы ниже уровня допуска пользователя.

Пример 4 – Начальник ГП с меткой сессии 2 осуществляет запрос на чтение и запись к таблице «Состояние БК» (2);

Ожидаемый результат: доступ на чтение – разрешен, доступ на запись – запрещен.

Полученный результат полностью соответствует ожидаемому результату: доступ на чтение – разрешен, доступ на запись – запрещен. В данном случае наблюдается в части дискреционного разграничения доступа запрет доступа пользователя на запись в таблицу, несмотря на то, что уровень конфиденциальности таблицы и уровень допуска к ней пользователя совпадают.

Пример 5 – Заказчик с меткой сессии 2 осуществляет запрос на чтение и запись к таблице «Состояние БК» (2);

Ожидаемый результат: доступ на чтение – разрешен, доступ на запись – разрешен.

Полученный результат полностью соответствует ожидаемому результату: доступ на чтение – разрешен, доступ на запись – разрешен. В данном случае наблюдается в части дискреционного и мандатного разграничения доступа разрешение доступа пользователя на чтение и запись в таблицу. Уровень

конфиденциальности таблицы и уровень допуска к ней пользователя совпадают.

По результатам тестирования можно сделать вывод о том, что дискреционная и мандатная модели разграничения доступа работают корректно.

В пунктах 1–3 продемонстрирована работа мандатной модели разграничения доступа – правила NRU и NWD (пункт 1.4.2). Данная модель работает корректно.

В пунктах 4–5 продемонстрирована работа дискреционной модели разграничения доступа в случае, если мандатные метки пользователей совпадают. Данная модель работает корректно.

4.2. Проверка целостности

Данный способ проверки осуществляется при помощи Представлений. Представление – это SQL-запрос, лишенный физической материализации, который имеет возможность отображения выбранных полей нескольких таблиц, сопоставленных друг другу, в одной сводной таблице.

Для проверки на целостность было создано представление «station_coordination» (Приложение Ж), которое отображает идентификатор и наименование ПЭ и соответствующие ему координаты. (Рисунок 22)

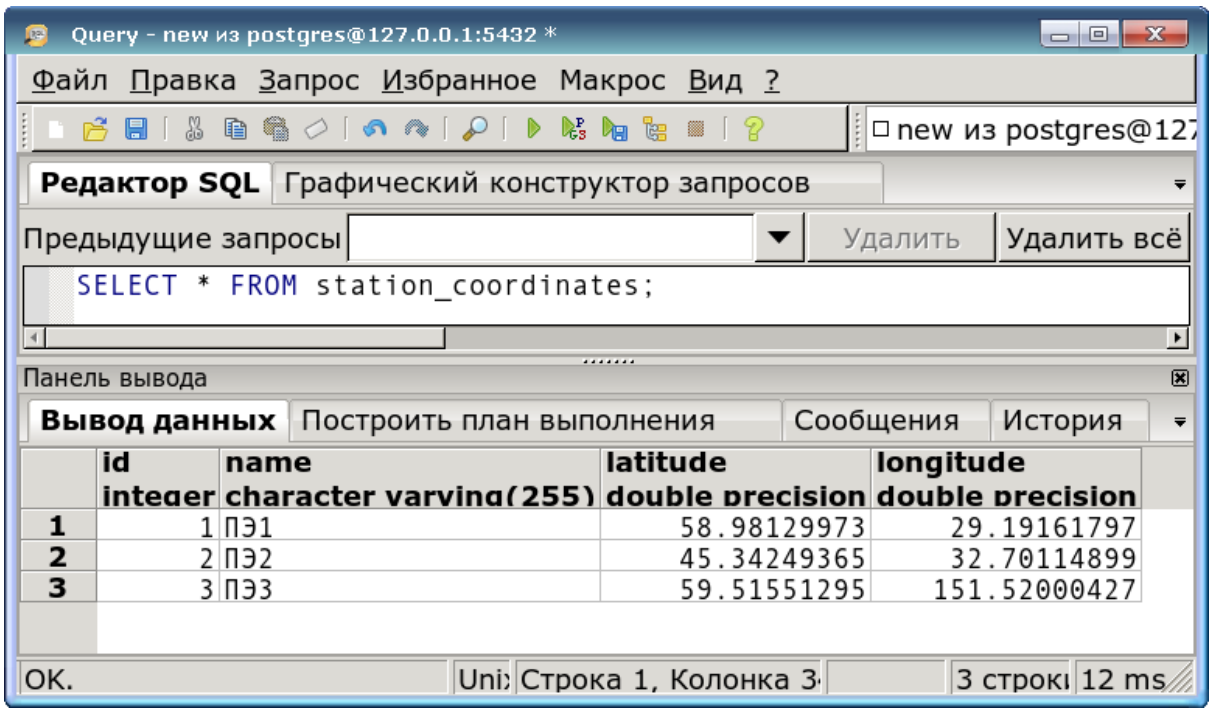

Рисунок 22 – Отображение представления «station_coordination»

Проверка продемонстрирована на следующих примерах:

1. Начальник ГП с меткой сессии 0 осуществляет запрос на чтение к представлению, в состав которого входят таблицы с меткой 0 и 1;
2. Начальник ГП с меткой сессии 1 осуществляет запрос на чтение к представлению, в состав которого входят таблицы с меткой 0 и 1;

Примеры рассмотрены подробно в приложение Ж.

Пример 1 – Начальник ГП с меткой сессии 0 осуществляет запрос на чтение к представлению, в состав которого входят таблицы с меткой 0 и 1;

Ожидаемый результат: доступ на чтение – запрещен.

Полученный результат полностью соответствует ожидаемому результату: доступ на чтение запрещен. В

данном случае наблюдается в части мандатного разграничения доступа действие правила NRU – «нет чтения вверх»: так как в состав сводной таблицы, к которой осуществляется запрос на чтение, входит таблица, уровень конфиденциальности которой превышает уровень допуска пользователя, то пользователю запрещен доступ к представлению.

Пример 2 – Начальник ГП с меткой сессии 1 осуществляет запрос на чтение к представлению, в состав которого входят таблицы с меткой 0 и 1;

Ожидаемый результат: доступ на чтение – разрешен.

Полученный результат полностью соответствует ожидаемому результату: доступ на чтение разрешен. В данном случае наблюдается в части мандатного разграничения доступа действие правила NRU – «нет чтения вверх»: так как в состав сводной таблицы, к которой осуществляется запрос на чтение, входят таблицы, уровень конфиденциальности которых не превышает уровень допуска пользователя, то пользователю разрешен доступ к представлению.

ЗАКЛЮЧЕНИЕ

В заключение выполненной работы можно сделать вывод о том, что разграничение доступа является одним из наиболее важных методов контроля доступа, определяющих возможность и способы работы субъектов с объектами, в защищенной АС. Мандатный механизм разграничения доступа, который необходим для обработки сведений, составляющих государственную тайну, позволяет контролировать потоки информации между разноуровневыми субъектами и объектами.

Для выполнения практической работы была выявлена ОС Astra Linux SE путем проведения анализа на предмет соответствия требованиям СВТ и АС для работы с информацией, содержащей государственную тайну до грифа «совершенно секретно» включительно, так как она наилучшим образом отвечает данным требованиям в сравнение с другими ОС. СУБД PostgreSQL, входящая в состав Astra Linux SE и доработанная в части мандатного разграничения доступа, позволила создать на ее основе мандатно–разграниченную БД.

Что касается самой БД, предметная область, на основе которой БД была спроектирована, позволила наиболее ярко отобразить работу мандатной модели разграничения доступа в совокупности с дискреционной. Принцип эксплуатации беспилотных кораблей (БК) представляет собой систему с разноуровневыми данными и разными

требованиями разноуровневых пользователей к этим данным.

Таким образом, в ходе выполнения работы были решены следующие задачи:

- выбрана платформа для реализации на ее основе мандатно-разграниченной БД;
- спроектирована модель БД и мандатная модель разграничения доступа к данной БД;
- реализованы спроектированные модель БД и мандатная модель разграничения доступа к данной БД;
- осуществлена проверка корректности работы разграничения доступа в реализованной БД.

Представленная работа была выполнена в АО «НИЦ СПб ЭТУ» в рамках проектов, направленных на автоматизацию и информатизацию бизнес-процессов выбранных управлений Министерства Обороны Российской Федерации, что подтверждает ее значимость, актуальность и новизну.

СПИСОК ЛИТЕРАТУРЫ

1. Цирлов В.Л. Основы информационной безопасности автоматизированных систем [Текст]. – Феникс, 2008;

2. Руководящий документ «Концепция защиты средств вычислительной техники и автоматизированных систем от несанкционированного доступа к информации» [Текст], утвержденный решением Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г.;

3. Руководящий документ «Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации.» [Текст], утвержденный решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г.;

4. Закон РФ «О государственной тайне»[Текст], от 21 июля 1993 г. № 5485–I (с изменениями и дополнениями);

5. СТР «Специальные требования и рекомендации по защите информации, составляющей государственную тайну, от утечки по техническим каналам» [Текст], утвержденный Государственной Технической Комиссией при Президенте РФ от 23 мая 1997 года № 55;

6. Постановление Правительства РФ «Об утверждении Правил отнесения сведений, составляющих государственную тайну, к различным степеням секретности» [Текст] от 4 сентября 1995 г. № 870 г. Москва;

7. Постановление Правительства РФ «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти, уполномоченном органе управления использованием атомной энергии и уполномоченном органе по космической деятельности» [Текст] от 3 ноября 1994 г. № 1233 г. Москва;

8. ГОСТ Р ИСО/МЭК 15408–1–2008 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель» [Текст] от 01.10.2009 г. ;

9. Шаньгин В.Ф. «Информационная безопасность компьютерных систем и сетей» [Текст]. – М.: ИД «ФОРУМ» – Инфра–М 2011 г.;

10. ГОСТ Р ИСО/МЭК 15408–1–2012 «Информационная технология (ИТ). Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий. Часть 1. Введение и общая модель» [Текст] от 01.12.2013;

11. Руководящий документ «Безопасность информационных технологий. Положение по разработке профилей защиты и заданий по безопасности» [Текст], утвержденный решением председателя Государственной технической комиссии при Президенте Российской Федерации от 2003 г.;

12. Качур Е.Д., Попов Н.Н., Абрамов Е.П., Шнеерсон Е.З., Козлов М. И., Богданов П.Ю., Голосовская В.А., Ткаченко Г.Н. Использование мандатной модели

управления доступом при защите конфиденциальной информации / Межвузовый сборник научных трудов «Информационные технологии и системы. Управление, экономика, транспорт, право» 1(32) [Текст]. – СПб.: ООО «Андреевский издательский дом» 2018 г.;

13. Качур Е.Д., Козлов М.И., Попов Н.Н., Абрамов Е.П. Методика обеспечения безопасности автоматизированной системы на основе мандатной модели разграничения доступа / Межвузовый сборник научных трудов «Информационные технологии и системы. Управление, экономика, транспорт, право» 1(33) [Текст]. – СПб.: ООО «Андреевский издательский дом» 2018 г.;

14. Блинов А.М. «Информационная безопасность. Учебное пособие. Часть 1» [Текст]. – СПб.: Государственный университет экономики и финансов 2010 г.;

15. Постановление Правительства РФ «Об установлении запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд» [Текст] от 16 ноября 2015 года № 1236 г. Москва;

16. Зима В.М. Многоуровневая защита информационно–программного обеспечения вычислительных систем [Текст]. – СПб.: Военная инженерно–космическая краснознаменная академия имени А.Ф. Можайского 1997 г.;

17. ГОСТ 15971–90 «Системы обработки информации. Термины и определения» [Текст] от 01.01.1992 г.;

18. Вопросы по МСВС / официальный сайт ВНИИНС [Электронный ресурс]. URL: http://www.vniins.ru/index.php?lang=%D0%A0%D1%83%D1%81 (дата обращения 15.11.2018);

19. Государственный реестр сертифицированных средств защиты информации N РОСС RU.0001.01БИ00 / сайт ФСТЭК [Электронный ресурс]. URL: https://fstec.ru/tekhnicheskaya–zashchita–informatsii/dokumenty–po–sertifikatsii/153–sistema–sertifikatsii/591–gosudarstvennyj–reestr–sertifitsirovannykh–sredstv–zashchity–informatsii–n–ross–ru–0001–01bi00 (дата обращения 18.11.2018);

20. Русский бронированный Debian. Как устроена новая модель управления доступом в Astra Linux SE / блог журнала «Хакер» [Электронный ресурс]. URL: https://xakep.ru/2015/09/15/astra–linux–se/ (дата обращения 19.11.2018);

21. ОПЕРАЦИОННАЯ СИСТЕМА СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ «ASTRA LINUX SPECIAL EDITION» Описание применения РУСБ.10015–01 31 01 [Текст] – 2014 г.;

22. Новая версия «Astra Linux Special Edition» успешно сертифицирована министерством обороны РФ» / Новости на официальном сайте НПО РусБИТех [Электронный ресурс]. URL: https://astralinux.ru/news/category–news/2018/novaya–versiya–%C2%ABastra–linux–special–edition%C2%BB–uspeshno–

sertificzirovana–ministerstvom–oboronyi–rf/ (дата обращения 19.11.2018);

23. Операционная система специального назначения «Astra Linux Special Edition» / описание продуктов на официальном сайте НПО РусБИТех [Электронный ресурс]. URL: https://astralinux.ru/products/astra–linux–special–edition/ (дата обращения 21.11.2018);

24. ОС и СУБД: мандатное разграничение доступа / Новости сайта PostgreSQL [Электронный ресурс]. URL: https://postgrespro.ru/blog/media/229432 (дата обращения 21.11.2018);

25. Базовые информационные технологии. Средства защиты информации в среде ОС «МСВС» 3.0. Учебное пособие – 2009 г.;

26. 188–ФЗ и перспективы российского ПО для систем безопасности / статья главного конструктора ГК СИГМА Левина С.Н. [Электронный ресурс]. URL: https://elibrary.ru/item.asp?id=27654562 (дата обращения 25.11.2018);

27. Лазунов П., Рогов Е., Лёвшин И. «PostgreSQL для начинающих» [Текст] – официальный сайт PostgreSQL;

28. Выбор СУБД для информационных систем специального назначения / Архив докладов конференции PgConf.Russia 2015 [Электронный ресурс]. URL: https://pgconf.ru/2015/89318 (дата обращения 29.11.2018);

29. Объектно–реляционная СУБД / Свободная энциклопедия Википедия [Электронный ресурс]. URL: https://ru.wikipedia.org/wiki/%D0%9E%D0%B1%D1%8A%D0%B5%D0%BA%D1%82%D0%BD%D0%BE–

%D1%80%D0%B5%D0%BB%D1%8F
%D1%86%D0%B8%D0%BE%D0%BD%D0%BD
%D0%B0%D1%8F_%D0%A1%D0%A3%D0%91%D0%94 (дата обращения 02.12.2018);

30. Реляционные БД vs объектно–ориентированные БД / блог пользователя @CrazyViper на сайте Хабр [Электронный ресурс]. URL: https://habr.com/ru/post/93356/ (дата обращения 02.12.2018);

31. Закончилась ли эпоха Реляционных СУБД? / блог CNews|аналитика [Электронный ресурс]. URL: http://www.cnews.ru/reviews/free/marketBD/articles/articles2.shtml (дата обращения 02.12.2018);

32. Ребекка М. Райордан «Основы реляционных баз данных» [Текст]. – М.: Русская редакция 2001 г.;

33. Безопасность и быстродействие PostgreSQL для государственной тайны / Архив докладов конференции PgConf.Russia 2015 [Электронный ресурс]. URL: https://pgconf.ru/2015/89379 (дата обращения 03.12.2018);

34. Фуфаев Э.В., Фуфаев Д.Э. «Базы данных. 7–е издание» [Текст]. – М.: Издательский центр «Академия» 2012 г.;

35. ОПЕРАЦИОННАЯ СИСТЕМА СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ «ASTRA LINUX SPECIAL EDITION» Руководство по КСЗ. Часть 1 РУСБ.10015–01 97 01–1 [Текст] – 2014 г.;

36. ОПЕРАЦИОННАЯ СИСТЕМА СПЕЦИАЛЬНОГО НАЗНАЧЕНИЯ «ASTRA LINUX SPECIAL EDITION» Руководство администратора. Часть 1 РУСБ.10015–01 95 01–1 [Текст] – 2014 г.;

37. ГОСТ Р ИСО/МЭК 12207–2010 «Информационная технология. Системная и программная инженерия. Процессы жизненного цикла программных средств» [Текст] от 01.03.2012 г.;

38. ГОСТ Р ИСО/МЭК 17799–2005 «Информационная технология. Практические правила управления информационной безопасностью» [Текст] от 01.01.2007 г.

ПРИЛОЖЕНИЕ А

Требования к АС и СВТ, необходимые для обработки сведений, составляющих государственную тайну до грифа «совершенно секретно» включительно

А.1 Требования АС для класса защищенности 1Б

Требования по защите информации от НСД реализуются в рамках системы защиты информации от НСД АС и состоят из четырех подсистем:

- управления доступом;
- регистрации и учета;
- криптографической;
- обеспечения целостности.

Подсистема управления доступом

В подсистеме происходит проверка и идентификация субъектов доступа, идентификация ЭВМ, ее узлов, терминалов, каналов связи и внешних устройств ЭВМ. Также идентифицируются тома, каталоги, программы, файлы, записи, поля записей по именам. Осуществляется контроль доступа субъектов в соответствие с матрицей доступа к защищенным ресурсам и управление потоками информации с помощью меток конфиденциальности.

Подсистема регистрации и учета

В подсистеме осуществляется регистрация следующих событий:

- вход/выход субъектов доступа в систему/из системы;
- выдачи печатных документов на "твердую" копию;

- запуска/завершения всех программ и процессов (заданий, задач) в АС;
- регистрации попыток доступа программных средств (ПС) к защищаемым файлам;
- изменений статуса объектов доступа и полномочий субъектов доступа.

Осуществляется учет создаваемых инициируемых элементов ЭВМ, оперативной памяти, собственно ЭВМ, ее узлов и внешних устройств, фрагментов сети. Также учитываются защищаемые носители информации с помощью маркировки регистрации в журнале. Ведется очистка освобождаемых областей оперативной памяти и внешних накопителей и сигнализация при попытках нарушения защиты.

Криптографическая подсистема

В данной подсистеме осуществляется шифрование всей конфиденциальной информации, дополнительное контролирование доступа субъектов к операциям шифрования и к соответствующим криптографическим ключам и использование сертифицированных средств криптографической защиты.

Подсистема обеспечения целостности

Обеспечивается целостность программных средств СЗИ НСД и неизменность программной среды и физическая охраны СВТ. Предоставляется администратор (служба) защиты информации. Проводится периодическое тестирование всех функций СЗИ НСД. Также необходимо наличие средств восстановления СЗИ НСД и использование сертифицированных средства защиты.

А.2 Требования СВТ для 3 класса защищенности

Дискреционный принцип контроля доступа

Осуществляется контролирование комплексов средств защиты (КСЗ) информации доступа субъектов к объектам. Для каждой такой пары (субъект–объект) должно быть задано перечисление допустимых типов доступа. Необходимо наличие механизма дискреционного разграничения доступа и контролирование доступа, применяемое ко всем объектам и субъектам. Также предусмотрена возможности санкционированного изменения правил разграничения доступа (ПРД), предоставление средств управления и прав на изменение ПРД выделенным субъектам. Содержится механизм, претворяющий в жизнь дискреционные ПРД, которые в свою очередь являются дополнением мандатных ПРД.

Мандатный принцип контроля доступа

Сопоставляются классификационные метки субъектов и объектов. Посредством этих меток субъектам и объектам назначаются классификационные уровни. При вводе новых данных в систему должен происходить запрос классификационных меток. Реализация средства, осуществляющего перехват всех обращений субъектов к объектам и разграничение доступа в соответствии с заданным принципом разграничения доступа.

Очистка памяти

КСЗ осуществляет очистку оперативной и внешней памяти. Очистка производится путем записи маскирующей

информации в память при ее освобождении (перераспределении).

Изоляция модулей

При наличии в СВТ мультипрограммирования в КСЗ должен существовать программно–технический механизм, который изолирует программные модули одного процесса (одного субъекта), от программных модулей других процессов (других субъектов).

Маркировка документов

При выводе защищаемой информации на документ в начале и конце проставляют штамп N 1 и заполняют его реквизиты в соответствии с Инструкцией N 0126–87.

Защита ввода и вывода на отчуждаемый физический носитель информации

КСЗ должен различать каждое устройство ввода–вывода и каждый канал связи как произвольно используемые или идентифицированные.

Сопоставление пользователя с устройством

КСЗ должен обеспечивать вывод информации на запрошенное пользователем устройство как для произвольно используемых устройств, так и для идентифицированных (при совпадении маркировки).

Идентификация и аутентификация

КСЗ должен требовать от пользователей идентифицировать себя при запросах на доступ, должен проверять подлинность идентификатора субъекта – осуществлять аутентификацию.

Гарантии проектирования

На начальном этапе проектирования КСЗ должна строиться модель защиты, задающая принцип разграничения доступа и механизм управления доступом.

Регистрация

КСЗ должен быть в состоянии осуществлять регистрацию следующих событий:

- использование идентификационного и аутентификационного механизма;
- запрос на доступ к защищаемому ресурсу;
- создание и уничтожение объекта;
- действия по изменению ПРД.

Дополнительно должна быть предусмотрена регистрация всех попыток доступа, всех действий оператора и выделенных пользователей.

Взаимодействие пользователя с КСЗ

Для обеспечения возможности изучения, анализа, верификации и модификации КСЗ должен быть хорошо структурирован, его структура должна быть модульной и четко определенной. Интерфейс пользователя и КСЗ должен быть определен (вход в систему, запросы пользователей и КСЗ и т.п.). Должна быть обеспечена надежность такого интерфейса. Каждый интерфейс пользователя и КСЗ должен быть логически изолирован от других таких же интерфейсов.

Надежное восстановление

Процедуры восстановления после сбоев и отказов оборудования должны обеспечивать полное восстановление свойств КСЗ.

Целостность КСЗ

Необходимо осуществлять периодический контроль над целостностью КСЗ.

Программы должны выполняться в отдельной части оперативной памяти. Это требование должно подвергаться верификации.

Тестирование

Необходимо производить тестирование реализации ПРД, невозможности присвоения субъектом себе новых прав, работы механизма изоляции процессов в оперативной памяти, маркировки документов, защиты ввода и вывода информации на отчуждаемый физический носитель и сопоставление пользователя с устройством. Тестированию также подлежат идентификация и аутентификация, запрет на доступ несанкционированного пользователя, работа механизма по контролю за целостность. СВТ, регистрация событий средства защиты регистрационной информации и возможность санкционированного ознакомления с этой информацией, очистка памяти, работа механизма надежного восстановления.

Руководство для пользователя

Документация на СВТ должна включать в себя краткое руководство для пользователя с описанием способов использования КСЗ и его интерфейса с пользователем.

Тестовая документация

В документации должно быть представлено описание тестов и испытаний, которым подвергалось СВТ, а также результатов тестирования.

Конструкторская (проектная) документация

Должна содержать общее описание принципов работы СВТ, общую схему КСЗ, ее внешних интерфейсов отчуждаемый физический носитель и сопоставление пользователя с устройством и интерфейсом модулей. Также необходимо содержание механизмов контроля целостности КСЗ, очистки памяти, изоляции программ в оперативной памяти, идентификации и аутентификации. Должны быть описаны модель защиты, диспетчер устройств и средства регистрации.

ПРИЛОЖЕНИЕ Б

Запросы на чтение и запись к таблицам БД в теории

Б.1 Запросы на чтение

Запросы на чтение разноуровневыми пользователями разноуровневых таблиц представлены на рисунке 23.

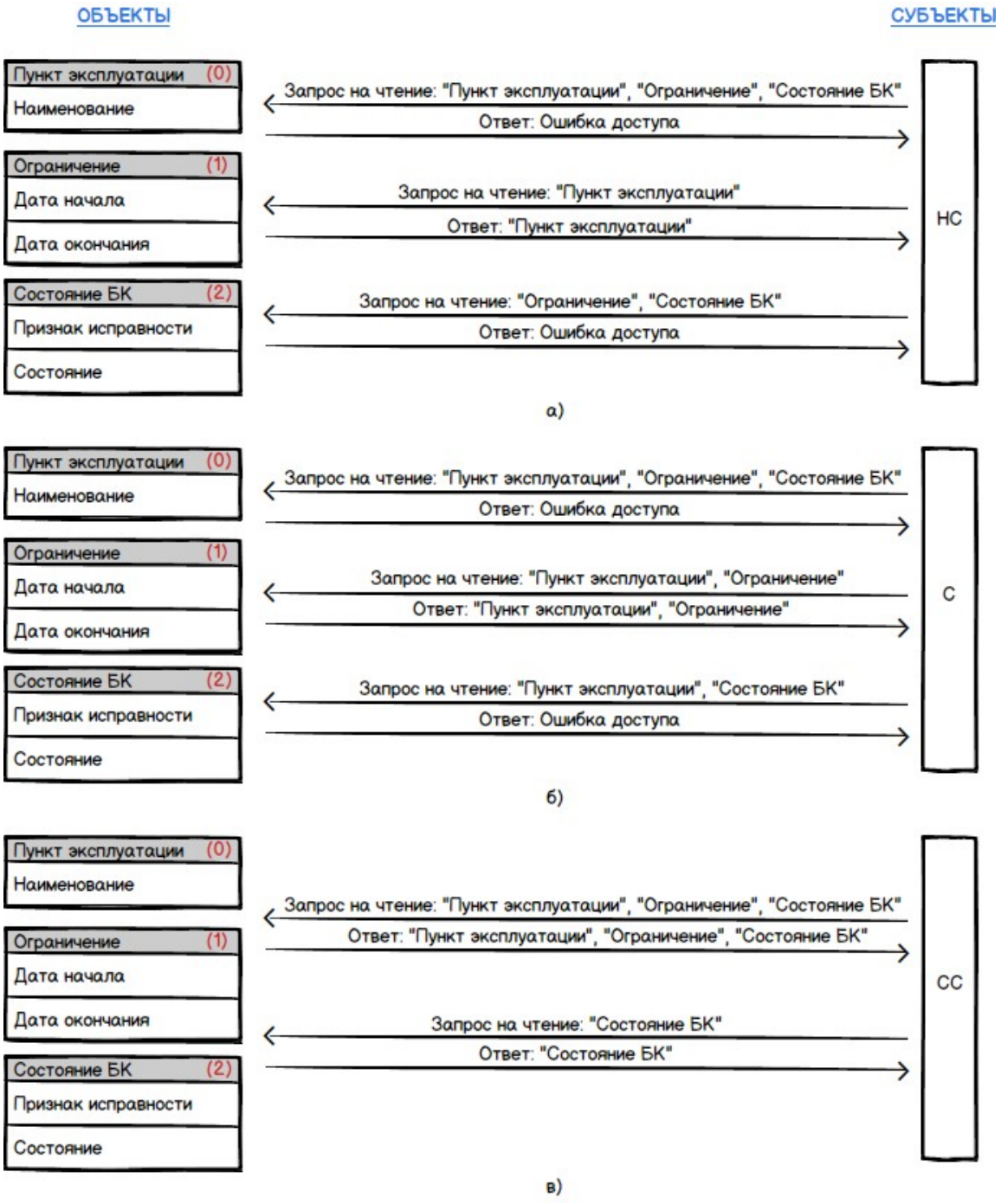

Рисунок 23 – Запрос на чтение

Б.2 Запросы на запись

Запросы на запись разноуровневыми пользователями разноуровневых таблиц представлены на рисунке 24.

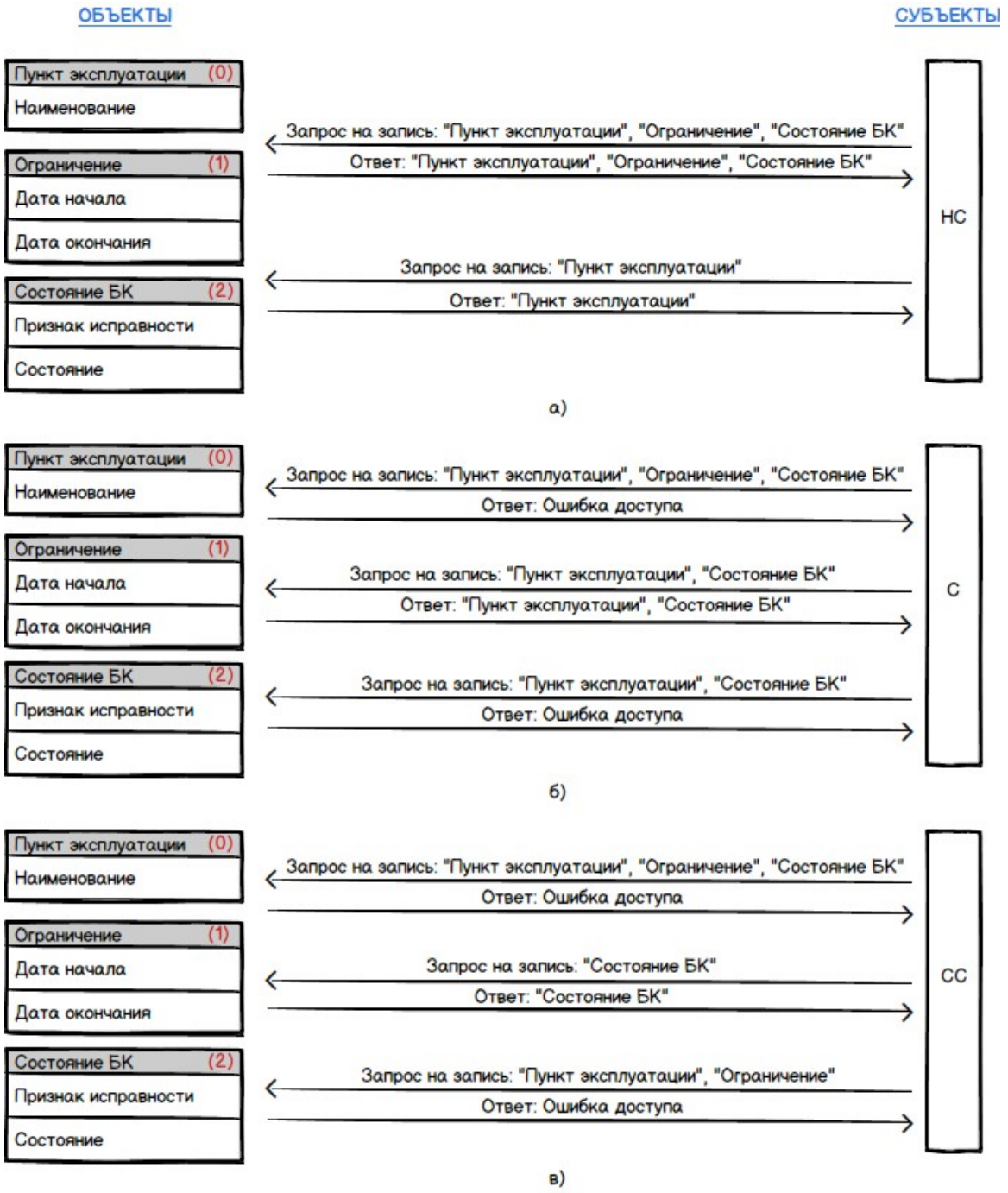

Рисунок 24 – Запрос на запись

Условные обозначения к рисунку 23 и 24:

- объект 0 – объект, обладающий меткой конфиденциальности «не секретно»;

- объект 1 – объект, обладающий меткой конфиденциальности «секретно»;
- объект 2 – объект, обладающий меткой конфиденциальности «совершенно секретно»;
- субъект НС – субъект обладающий уровнем допуска «не секретно»;
- субъект С – субъект обладающий уровнем допуска «секретно»;
- субъект СС – субъект обладающий уровнем допуска «совершенно секретно»[13].

ПРИЛОЖЕНИЕ В

Логическая и физическая схемы БД в среде Visual Paradigm

В.1 Логическая схема БД

Логическая схема БД представлена на рисунке 25.

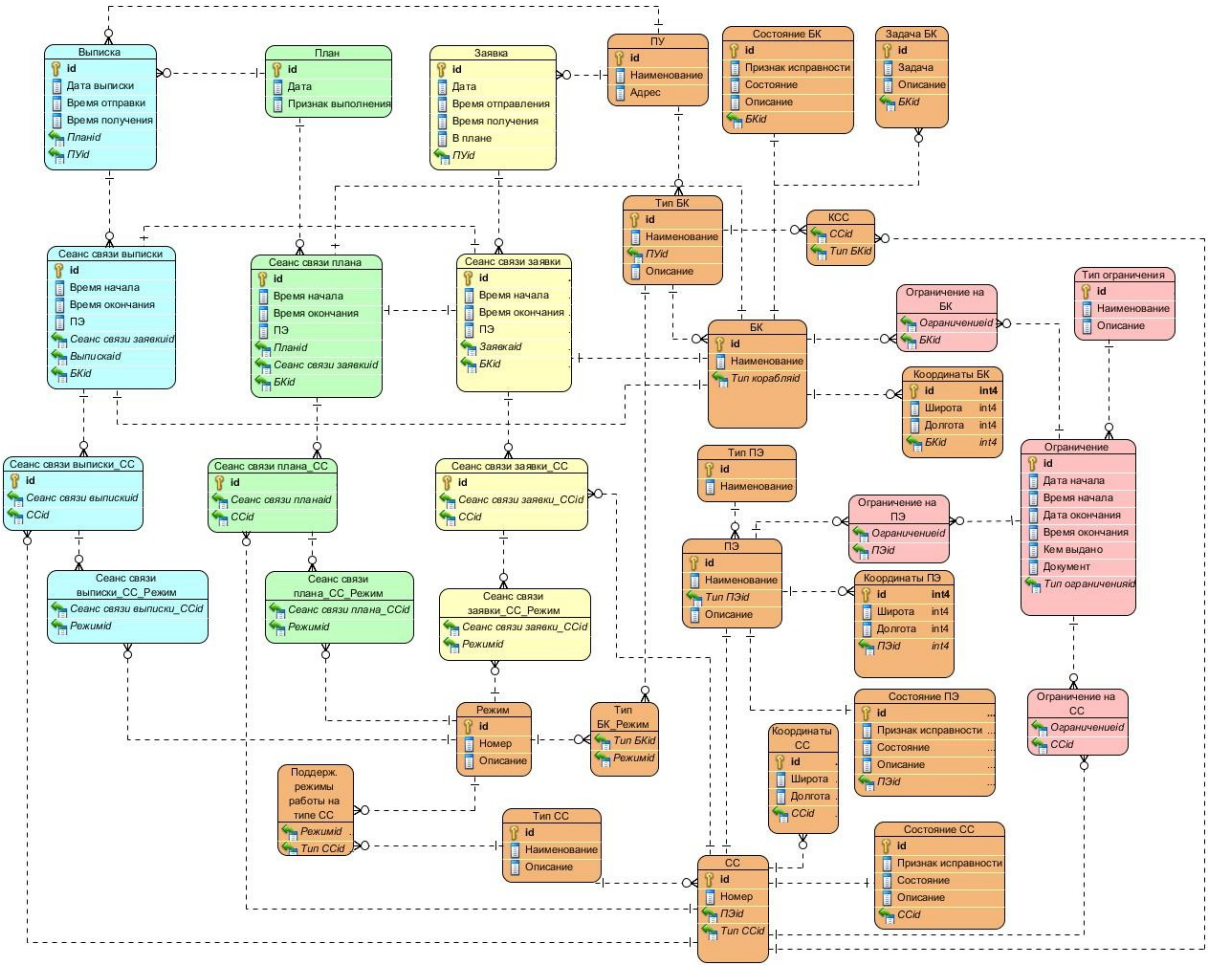

Рисунок 25 – Логическая схема БД

В.2 Физическая схема БД

Физическая схема БД представлена на рисунке 26.

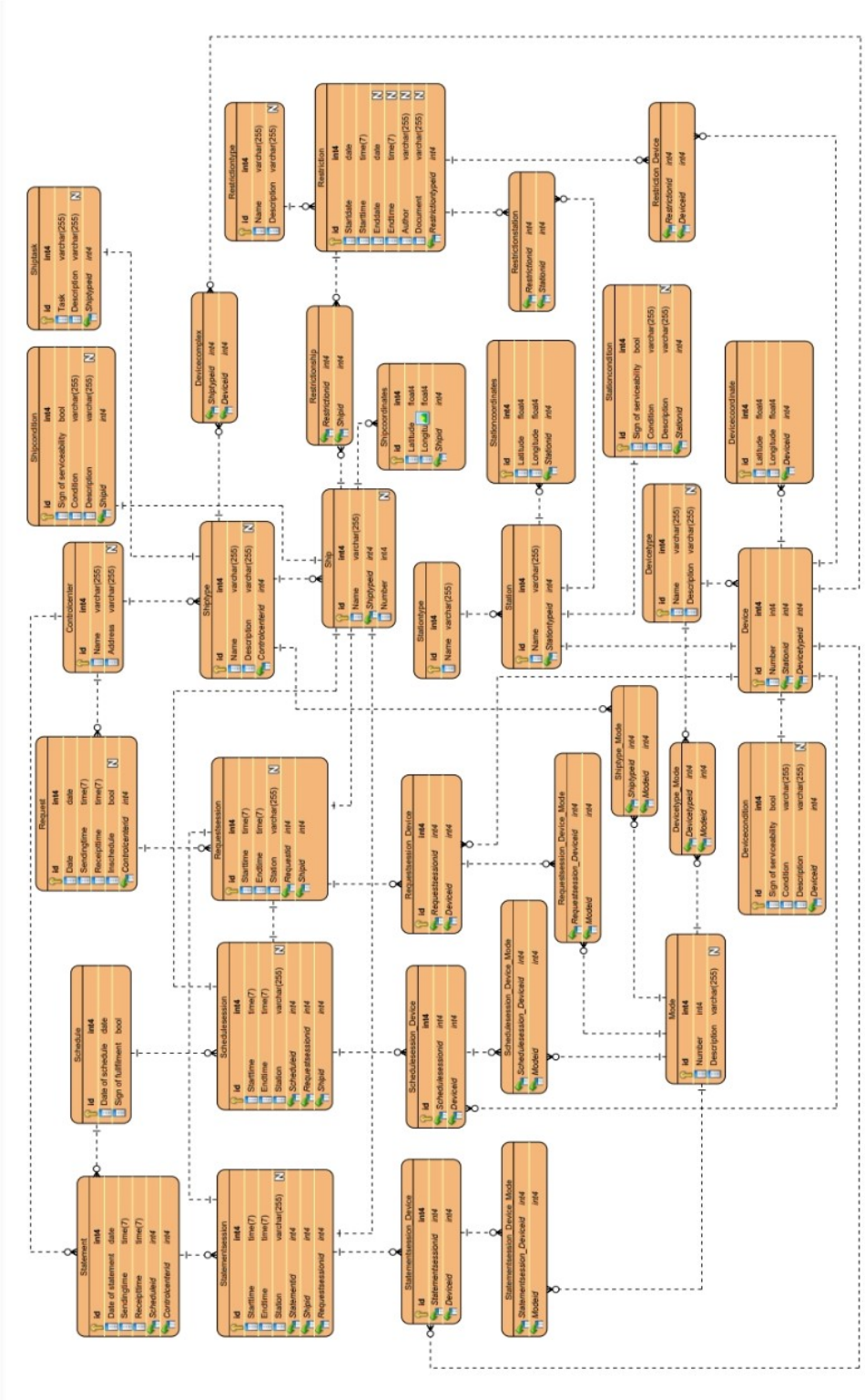

Рисунок 26 – Физическая схема БД

ПРИЛОЖЕНИЕ Г

Описание атрибутов логической модели БД

Г.1 Описание атрибутов

1) Заявка – сообщение о желании заказчика осуществить сеанс связи с кораблем с определенного средства. Атрибуты:
   - id – уникальный идентификатор заявки;
   - Дата – дата отправления заявки;
   - Время отправления – время отправления заявки;
   - Время получения – время получения заявки;
   - Планid – идентификатор плана;
   - В плане – признак включения в план;
   - ПУid – идентификатор ПУ.
2) Выписка – часть плана, содержащая сведения о сеансе связи с кораблем по заявке заказчика. Атрибуты:
   - id – уникальный идентификатор выписки;
   - Дата выписки – дата создания выписки;
   - Время отправления – время отправления выписки;
   - Время получения – время получения выписки;
   - Планid – уникальный идентификатор плана;
   - ПУid – уникальный идентификатор ПУ.
3) План – заранее составленный перечень сеансов связи, где указано какое СС на каком ПЭ с каким БК в какое время осуществляет сеанс связи. Атрибуты:
   - id – уникальный идентификатор плана;

- Дата – дата утверждения плана;
- Признак выполнения – факт выполнения плана (выполнен/не выполнен).

4) Сеанс связи заявки – желаемый заказчиком сеанс связи СС с БК в определенный промежуток времени, указанный в заявке. Атрибуты:
   - id – уникальный идентификатор сеанса связи заявки;
   - Время начала – время начала сеанса связи;
   - Время окончания – время окончания сеанса связи;
   - ПЭ – ПЭ, включенный в заявку;
   - БКid – уникальный идентификатор БК;
   - Заявкаid – уникальный идентификатор заявки.
5) Сеанс связи выписки – реально осуществимый сеанс связи СС с БК в определенный промежуток времени, указанный в выписке. Атрибуты:
   - id – уникальный идентификатор сеанса связи выписки;
   - Время начала – время начала сеанса связи;
   - Время окончания – время окончания сеанса связи;
   - ПЭ – ПЭ, включенный в выписку;
   - Сеанс связи заявкиid – уникальный идентификатор сеанса связи заявки;
   - Выпискаid – уникальный идентификатор выписки;
   - БКid – уникальный идентификатор БК.

6) Сеанс связи плана – план сеансов связи СС с БК на сутки. Атрибуты:
    - id – уникальный идентификатор сеанса связи плана;
    - Время начала – время начала сеанса связи;
    - Время окончания – время окончания сеанса связи;
    - ПЭ – ПЭ, включенный в план;
    - Сеанс связи заявкиid – уникальный идентификатор сеанса связи заявки;
    - Планid – уникальный идентификатор выписки;
    - БКid – уникальный идентификатор БК.
7) ПУ (пункт управления) – специальное подготовленное и оснащенное место, откуда органы управления осуществляют управление БК. Атрибуты:
    - id – уникальный идентификатор ПУ;
    - Наименование – наименование ПУ;
    - Адрес – физический адрес ПУ.
8) БК (беспилотный корабль) – морское или речное судно, оборудованное системой автоматического управления, которое может осуществлять передвижение и выполнение поставленных для него задач без участия человека. Атрибуты:
    - id – уникальный идентификатор БК;
    - Наименование – наименование БК
    - Тип БКid – уникальный идентификатор типа БК.
9) Тип БК – форма, вид БК, обладающие определенными признаками. Атрибуты:
    - id – уникальный идентификатор типа БК;

- Наименование – наименование типа БК;
- Описание – описание типа БК;
- ПУid – уникальный идентификатор ПУ.

10) Координаты БК – местоположение БК. Атрибуты:
    - id – уникальный идентификатор набора координат БК;
    - Широта x – координата широты БК;
    - Долгота – координата долготы БК;
    - БКid – уникальный идентификатор БК.
11) Состояние БК – отображение возможности использования БК. Атрибуты:
    - id – уникальный идентификатор состояния БК;
    - Признак исправности – наличие исправности БК;
    - Состояние – возможность использования БК;
    - Описание – описание БК.
12) Задача БК – обладание БК определенного набора функционала, необходимого для выполнения какого–либо действия. Атрибуты:
    - id – уникальный идентификатор задачи БК;
    - Задача – возможные действия БК;
    - Описание – подробное описание задачи;
    - БКid – уникальный идентификатор БК.
13) ПЭ (пункт эксплуатации) – специально подготовленное и оснащенное место, содержащее в себе набор СС, с помощью которых осуществляется сеанс связи с кораблем. Атрибуты:
    - id – уникальный идентификатор ПЭ;
    - Наименование – наименование ПЭ;
    - Тип ПЭid – уникальный идентификатор типа ПЭ.

14) Тип ПЭ – форма, вид ПЭ, обладающий определенными признаками. Атрибуты:
    - id – уникальный идентификатор типа ПЭ;
    - Описание – описание ПЭ;
    - Наименование – наименование типа ПЭ.
15) Координаты ПЭ – местоположение ПЭ. Атрибуты:
    - id – уникальный идентификатор набора координат ПЭ;
    - Широта – координата широты ПЭ;
    - Долгота – координата высоты ПЭ;
    - ПЭid – уникальный идентификатор ПЭ.
16) Состояние ПЭ – отображение возможности использования ПЭ. Атрибуты:
    - id – уникальный идентификатор состояния ПЭ;
    - Признак исправности – наличие исправности ПЭ;
    - Состояние – возможность использования ПЭ;
    - Описание – описание ПЭ.
17) СС (средство связи) – средство, предназначенное для поддержки связи и обмена информацией заказчика с БК. Атрибуты:
    - id – уникальный идентификатор СС;
    - Номер – номер СС;
    - ПЭid – ссылка на ПЭ;
    - Тип ССid – уникальный идентификатор типа средств связи.

18) Тип СС – форма, вид СС, обладающие определенными признаками. Атрибуты:
    - id – уникальный идентификатор типа СС;

- Наименование – наименование типа СС;
- Описание – описание типа СС.

19) Координаты СС – местоположение СС. Атрибуты:
- id – уникальный идентификатор набора координат СС;
- Широта – координата широты СС;
- Долгота – координата долготы СС;
- CCid – уникальный идентификатор СС.

20) Состояние СС – отображение возможности использования СС. Атрибуты:
- id – уникальный идентификатор состояния СС;
- Признак исправности – наличие исправности СС;
- Состояние – возможность использования СС;
- Описание – описание СС.

21) КСС (комплекс средств связи) – связочная таблица, представляющая собой сопоставление типов БК и взаимодействующих с ними СС. Атрибуты:
- CCid – идентификатор СС;
- Тип БКid – уникальный идентификатор типа БК.

22) Режим – описание характера работы средства. Атрибуты:
- id – уникальный идентификатор режима;
- Номер – номер режима;
- Описание – описание режима.

23) Поддерживаемые режимы на типе СС – связочная таблица, представляющая собой сопоставление режимов и поддерживающих их типов СС. Атрибуты:
- Тип CCid – уникальный идентификатор СС;
- Режимid – уникальный идентификатор режима.

24) Тип БК_Режим – связочная таблица, представляющая собой сопоставление типов БК и поддерживающих ими режимов. Атрибуты:
    - Тип БКid – уникальный идентификатор БК;
    - Режимid – уникальный идентификатор режима.
25) Сеанс связи заявки_СС – связочная таблица, представляющая собой сопоставление сеанс связи заявки, и задействованное в нем СС. Атрибуты:
    - id – уникальный идентификатор пары «Сеанс связи заявки» – «СС»;
    - Сеанс связи заявкиid – уникальный идентификатор сеанса связи заявки;
    - CCid – уникальный идентификатор СС.
26) Сеанс связи выписки_СС – связочная таблица, представляющая собой сопоставление сеанс связи выписки, и задействованное в нем СС. Атрибуты:
    - id – уникальный идентификатор пары «Сеанс связи выписки» – «СС»;
    - Сеанс связи выпискиid – уникальный идентификатор сеанса связи выписки;
    - CCid – уникальный идентификатор СС.
27) Сеанс связи плана_СС – связочная таблица, представляющая собой сопоставление сеанс связи плана, и задействованное в нем СС. Атрибуты:
    - id – уникальный идентификатор пары «Сеанс связи плана» – «СС»;
    - Сеанс связи планаid – уникальный идентификатор сеанса связи плана;
    - CCid – уникальный идентификатор СС.

28) Сеанс связи заявки_СС_режим – связочная таблица, представляющая собой сопоставление сеанса связи заявки на СС и работающего в этом сеансе режима. Атрибуты:
    - Сеанс связи заявки_CCid – уникальный идентификатор сеанса связи заявки на СС;
    - Режимid – уникальный идентификатор режима.
29) Сеанс связи выписки_СС_режим – связочная таблица, представляющая собой сопоставление сеанса связи выписки на СС и работающего в этом сеансе режима. Атрибуты:
    - Сеанс связи выписки_CCid – уникальный идентификатор сеанса связи выписки на СС;
    - Режимid – уникальный идентификатор режима.
30) Сеанс связи плана_СС_режим – связочная таблица, представляющая собой сопоставление сеанса связи плана на СС и работающего в этом сеансе режима. Атрибуты:
    - Сеанс связи плана_CCid – уникальный идентификатор сеанса связи плана на СС;
    - Режимid – уникальный идентификатор режима.
31) Ограничение – правило, ограничивающие какие–либо действия с ПЭ, БК или СС. Атрибуты:
    - id – уникальный идентификатор ограничения;
    - Дата начала – дата начала действия ограничения;
    - Время начала – время начала действия ограничения;
    - Дата окончания – дата окончания действия ограничения;

- Время окончания – время окончания действия ограничения;
- Кем выдано – лицо, выдавшее ограничение;
- Документ – документ, на основание которого было составлено ограничение;
- Тип ограниченияid – уникальный идентификатор типа ограничения.

32) Тип ограничения – форма, вид ограничения, обладающие определенными признаками. Атрибуты:
- id – уникальный идентификатор типа ограничения;
- Наименование – наименование типа ограничения;
- Описание – описание типа ограничения.

33) Ограничение на БК – связочная таблица, представляющая собой ограничение, наложенное на использование БК. Атрибуты:
- Ограничениеid – уникальный идентификатор ограничения;
- БКid – уникальный идентификатор БК.

34) Ограничение на ПЭ – связочная таблица, представляющая собой ограничение, наложенное на использование ПЭ. Атрибуты:
- Ограничениеid – уникальный идентификатор ограничения;
- ПЭid – уникальный идентификатор ПЭ.

35) Ограничение на СС – связочная таблица, представляющая собой ограничение, наложенное на использование СС. Атрибуты:

- Ограничениеid – уникальный идентификатор ограничения;
- CCid – уникальный идентификатор СС.

ПРИЛОЖЕНИЕ Д

Модели разграничения доступа субъектов к объектам БД

Д.1 Дискреционная модель разграничения доступа

Дискреционные права доступа субъектов к объектам представлены в таблице 6.

Таблица 6 - Дискреционная модель разграничения доступа

Субъекты → *Объекты ↓*	Заказчик	Планировщик	Начальник ГП	Администратор НСИ
Выписка (statement)	r	rw	–	–
Сеанс связи выписки (statementsession)	r	rw	–	–
Сеанс связи выписки_СС (statementsession_device)	r	rw	–	–
Сеанс связи выписки_СС_Режим (statementsession_device_mode)	r	rw	–	–
План (schedule)	–	rw	r	–
Сеанс связи плана	–	rw	r	–

(schedulesession)				
Сеанс связи плана_СС (schedulesession_device)	–	rw	r	–

Продолжение таблицы 6

Субъекты → *Объекты ↓*	Заказчик	Планировщик	Начальник ГП	Администратор НСИ
Сеанс связи плана_СС_Режим (schedulesession_device_mode)	–	rw	r	–
Заявка (request)	rw	r	–	–
Сеанс связи заявки (requestsession)	rw	r	–	–
Сеанс связи заявки_СС (requestsession_device)	rw	r	–	–
Сеанс связи заявки_СС_Режим (requestsession_device_mode)	rw	r	–	–
ПУ (controlcenter)	r	r	r	rw
БК (ship)	r	r	r	rw
Тип БК (shiptype)	r	r	r	rw

Координаты БК (shipcoordinates)	rw	r	–	–
Состояние БК (shipcondition)	rw	–	r	–

Продолжение таблицы 6

Субъекты → *Объекты ↓*	Заказчик	Планировщик	Начальник ГП	Администратор НСИ
Задача БК (shiptask)	rw	–	–	–
ПЭ (station)	r	r	r	rw
Тип ПЭ (stationtype)	r	r	r	rw
Координаты ПЭ (stationcoordinates)	–	r	rw	–
Состояние ПЭ (stationcondition)	–	rw	rw	–
Режим (mode)	r	r	–	rw
Тип БК_Режим (shiptype_mode)	r	r	–	rw
СС (device)	r	r	r	rw
Тип СС (devicetype)	r	r	r	rw
Координаты СС (devicecoordinates)	–	r	rw	–
Состояние СС (devicecondition)	–	rw	rw	–
Поддерж. режимы работы на типе СС	r	r	–	rw

(devicetype_mode)				

Продолжение таблицы 6

Субъекты → *Объекты ↓*	Заказчик	Планировщик	Начальник ГП	Администратор НСИ
КСС (devicecomplex)	r	r	–	rw
Ограничения (restriction)	–	r	rw	–
Тип ограничения (restrictiontype)	–	r	r	rw
Ограничение на БК (restrictionship)	–	r	rw	–
Ограничение на ПЭ (restrictionstation)	–	r	rw	–
Ограничение на СС (restriction_device)	–	r	rw	–
П р и м е ч а н и е: ГП – группа планирования; НСИ – нормативно–справочная информация.				

Д.2 Мандатная модель разграничения доступа

Мандатные метки субъектов и объектов представлены в таблицах 7 и 8.

Таблица 7 – Мандатные метки субъектов

Субъекты	*Минимальная метка*	*Максимальная метка*
Заказчик (client)	0	2
Планировщик (planner)	0	1
Начальник ГП (leader_pt)	0	2
Администратор НСИ (administrator_rbi)	0	0

Примечание:

- pt – Planning Team;
- rbi – Regulatory Background Information.

Таблица 8 – Мандатные метки объектов

Объекты	*Мандатная метка*
Выписка (statement)	0
Сеанс связи выписки (statementsession)	0
Сеанс связи выписки_СС (statementsession_device)	0
Сеанс связи выписки_СС_Режим (statementsession_device_mode)	0
План (schedule)	1
Сеанс связи плана (schedulesession)	1
Сеанс связи плана_СС	1

(schedulesession_device)	

Продолжение таблицы 8

Объекты	*Мандатная метка*
Заявка (request)	0
Сеанс связи заявки (requestsession)	0
Сеанс связи заявки_СС (requestsession_device)	0
Сеанс связи заявки_СС_Режим (requestsession_device_mode)	0
ПУ (controlcenter)	0
БК (ship)	0
Тип БК (shiptype)	0
Координаты БК (shipcoordinates)	1
Состояние БК (shipcondition)	2
Задача БК (shiptask)	1
ПЭ (station)	0
Тип ПЭ (stationtype)	0
Координаты ПЭ (stationcoordinates)	1
Состояние ПЭ (stationcondition)	2
Режим (mode)	0
Тип БК_Режим (shiptype_mode)	1
СС (device)	0
Тип СС (devicetype)	0

Продолжение таблицы 8

Объекты	*Мандатная метка*
Состояние СС (devicecondition)	2

Поддерж. режимы работы на типе СС (devicetype_mode)	1
КСС (devicecomplex)	0
Ограничения (restriction)	1
Тип ограничения (restrictiontype)	0
Ограничение на БК (restrictionship)	1
Ограничение на ПЭ (restrictionstation)	1
Ограничение на СС (restriction_device)	1

ПРИЛОЖЕНИЕ Е

SQL-код для создания БД

Е.1 SQL-код для создания БД

SQL-код, при помощи которого осуществляется создание БД, следующий:

```
CREATE TABLE Statementsession (
  id                SERIAL NOT NULL,
  Starttime         time(7) NOT NULL,
  Endtime           time(7) NOT NULL,
  Station           varchar(255),
  Statementid       int4 NOT NULL,
  Shipid            int4 NOT NULL,
  Requestsessionid int4 NOT NULL,
  PRIMARY KEY (id));
CREATE TABLE Statement (
  id                    SERIAL NOT NULL,
  "Date of statement" date NOT NULL,
  Sendingtime           time(7) NOT NULL,
  Receipttime           time(7) NOT NULL,
  Scheduleid            int4 NOT NULL,
  Controlcenterid       int4 NOT NULL,
  PRIMARY KEY (id));
CREATE TABLE Schedule (
  id                      SERIAL NOT NULL,
  "Date of schedule"    date NOT NULL,
  "Sign of fullfilment" bool NOT NULL,
```

```
  PRIMARY KEY (id));
CREATE TABLE Controlcenter (
  id       SERIAL NOT NULL,
  Name    varchar(255) NOT NULL,
  Address varchar(255),
  PRIMARY KEY (id));
CREATE TABLE Ship (
  id          SERIAL NOT NULL,
  Name       varchar(255) NOT NULL,
  Shiptypeid int4 NOT NULL,
  Number     int4,
  PRIMARY KEY (id));
CREATE TABLE Shiptype (
  id              SERIAL NOT NULL,
  Name           varchar(255) NOT NULL,
  Description     varchar(255),
  Controlcenterid int4 NOT NULL,
  PRIMARY KEY (id));
CREATE TABLE Requestsession (
  id         SERIAL NOT NULL,
  Starttime time(7) NOT NULL,
  Endtime   time(7) NOT NULL,
  Station   varchar(255),
  Requestid int4 NOT NULL,
  Shipid    int4 NOT NULL,
  PRIMARY KEY (id));
CREATE TABLE Request (
  id              SERIAL NOT NULL,
  "Date"          date NOT NULL,
```

```
  Sendingtime     time(7) NOT NULL,
  Receipttime     time(7) NOT NULL,
  Inschedule      bool,
  Controlcenterid int4 NOT NULL,
  PRIMARY KEY (id));
CREATE TABLE Statementsession_Device (
  id                  SERIAL NOT NULL,
  Statementsessionid int4 NOT NULL,
  Deviceid            int4 NOT NULL,
  PRIMARY KEY (id));
CREATE TABLE Device (
  id            SERIAL NOT NULL,
  Number        int4 NOT NULL,
  Stationid     int4 NOT NULL,
  Devicetypeid int4 NOT NULL,
  PRIMARY KEY (id));
CREATE TABLE Station (
  id             SERIAL NOT NULL,
  Name           varchar(255) NOT NULL,
  Stationtypeid int4 NOT NULL,
  PRIMARY KEY (id));
CREATE TABLE Stationtype (
  id    SERIAL NOT NULL,
  Name varchar(255) NOT NULL,
  PRIMARY KEY (id));
CREATE TABLE Devicetype (
  id           SERIAL NOT NULL,
  Name         varchar(255) NOT NULL,
  Description varchar(255),
```

```
  PRIMARY KEY (id));
CREATE TABLE Schedulesession (
  id                SERIAL NOT NULL,
  Starttime         time(7) NOT NULL,
  Endtime           time(7) NOT NULL,
  Station           varchar(255),
  Scheduleid        int4 NOT NULL,
  Requestsessionid int4 NOT NULL,
  Shipid            int4 NOT NULL,
  PRIMARY KEY (id));
CREATE TABLE Schedulesession_Device (
  id                 SERIAL NOT NULL,
  Schedulesessionid int4 NOT NULL,
  Deviceid           int4 NOT NULL,
  PRIMARY KEY (id));
CREATE TABLE Requestsession_Device (
  id                SERIAL NOT NULL,
  Requestsessionid int4 NOT NULL,
  Deviceid          int4 NOT NULL,
  PRIMARY KEY (id));
CREATE TABLE Shiptype_Mode (
  Shiptypeid int4 NOT NULL,
  Modeid     int4 NOT NULL);
CREATE TABLE Mode (
  id            SERIAL NOT NULL,
  Number        int4 NOT NULL,
  Description varchar(255),
  PRIMARY KEY (id));
CREATE TABLE Statementsession_Device_Mode (
```

```
  Statementsession_Deviceid int4 NOT NULL,
  Modeid                    int4 NOT NULL);
CREATE TABLE Schedulesession_Device_Mode (
  Schedulesession_Deviceid int4 NOT NULL,
  Modeid                   int4 NOT NULL);
CREATE TABLE Requestsession_Device_Mode (
  Requestsession_Deviceid int4 NOT NULL,
  Modeid                  int4 NOT NULL);
CREATE TABLE Devicecondition (
  id                      SERIAL NOT NULL,
  "Sign of serviceability" bool NOT NULL,
  "Condition"              varchar(255) NOT NULL,
  Description              varchar(255),
  Deviceid                 int4 NOT NULL,
  PRIMARY KEY (id));
CREATE TABLE Stationcondition (
  id                      SERIAL NOT NULL,
  "Sign of serviceability" bool NOT NULL,
  "Condition"              varchar(255) NOT NULL,
  Description              varchar(255),
  Stationid                int4 NOT NULL,
  PRIMARY KEY (id));
CREATE TABLE Shipcondition (
  id                      SERIAL NOT NULL,
  "Sign of serviceability" bool NOT NULL,
  "Condition"              varchar(255) NOT NULL,
  Description              varchar(255),
  Shipid                   int4 NOT NULL,
  PRIMARY KEY (id));
```

```
CREATE TABLE Shiptask (
  id           SERIAL NOT NULL,
  Task         varchar(255) NOT NULL,
  Description varchar(255),
  Shiptypeid  int4 NOT NULL,
  PRIMARY KEY (id));
CREATE TABLE Devicecomplex (
  Shiptypeid int4 NOT NULL,
  Deviceid   int4 NOT NULL);
CREATE TABLE Restriction_Device (
  Restrictionid int4 NOT NULL,
  Deviceid      int4 NOT NULL);
CREATE TABLE Restriction (
  id                SERIAL NOT NULL,
  Startdate         date NOT NULL,
  Starttime         time(7) NOT NULL,
  Enddate           date,
  Endtime           time(7),
  Author            varchar(255),
  Document          varchar(255),
  Restrictiontypeid int4 NOT NULL,
  PRIMARY KEY (id));
CREATE TABLE Restrictiontype (
  id           SERIAL NOT NULL,
  Name         varchar(255) NOT NULL,
  Description varchar(255),
  PRIMARY KEY (id));
CREATE TABLE Devicecoordinate (
  id         SERIAL NOT NULL,
```

```
  Latitude  float4 NOT NULL,
  Longitude float4 NOT NULL,
  Deviceid  int4 NOT NULL,
  PRIMARY KEY (id));
CREATE TABLE Restrictionstation (
  Restrictionid int4 NOT NULL,
  Stationid     int4 NOT NULL);
CREATE TABLE Restrictionship (
  Restrictionid int4 NOT NULL,
  Shipid        int4 NOT NULL);
CREATE TABLE Stationcoordinates (
  id         SERIAL NOT NULL,
  Latitude  float4 NOT NULL,
  Longitude float4 NOT NULL,
  Stationid int4 NOT NULL,
  PRIMARY KEY (id));
CREATE TABLE Shipcoordinates (
  id         SERIAL NOT NULL,
  Latitude  float4 NOT NULL,
  Longitude float4 NOT NULL,
  Shipid    int4 NOT NULL,
  PRIMARY KEY (id));
CREATE TABLE Devicetype_Mode (
  Devicetypeid int4 NOT NULL,
  Modeid       int4 NOT NULL);
ALTER TABLE Statementsession_Device ADD
CONSTRAINT FKStatements225326 FOREIGN KEY
(Statementsessionid) REFERENCES Statementsession (id);
```

ALTER TABLE Statementsession ADD CONSTRAINT FKStatements316749 FOREIGN KEY (Statementid) REFERENCES Statement (id);

ALTER TABLE Statement ADD CONSTRAINT FKStatement954306 FOREIGN KEY (Scheduleid) REFERENCES Schedule (id);

ALTER TABLE Statement ADD CONSTRAINT FKStatement462505 FOREIGN KEY (Controlcenterid) REFERENCES Controlcenter (id);

ALTER TABLE Statementsession ADD CONSTRAINT FKStatements498656 FOREIGN KEY (Shipid) REFERENCES Ship (id);

ALTER TABLE Ship ADD CONSTRAINT FKShip479997 FOREIGN KEY (Shiptypeid) REFERENCES Shiptype (id);

ALTER TABLE Shiptype ADD CONSTRAINT FKShiptype185342 FOREIGN KEY (Controlcenterid) REFERENCES Controlcenter (id);

ALTER TABLE Statementsession ADD CONSTRAINT FKStatements909676 FOREIGN KEY (Requestsessionid) REFERENCES Requestsession (id);

ALTER TABLE Requestsession ADD CONSTRAINT FKRequestses521539 FOREIGN KEY (Requestid) REFERENCES Request (id);

ALTER TABLE Request ADD CONSTRAINT FKRequest20316 FOREIGN KEY (Controlcenterid) REFERENCES Controlcenter (id);

ALTER TABLE Requestsession ADD CONSTRAINT FKRequestses720454 FOREIGN KEY (Shipid) REFERENCES Ship (id);

ALTER TABLE Statementsession_Device ADD CONSTRAINT FKStatements107025 FOREIGN KEY (Deviceid) REFERENCES Device (id);

ALTER TABLE Device ADD CONSTRAINT FKDevice781657 FOREIGN KEY (Stationid) REFERENCES Station (id);

ALTER TABLE Station ADD CONSTRAINT FKStation256887 FOREIGN KEY (Stationtypeid) REFERENCES Stationtype (id);

ALTER TABLE Device ADD CONSTRAINT FKDevice892305 FOREIGN KEY (Devicetypeid) REFERENCES Devicetype (id);

ALTER TABLE Schedulesession_Device ADD CONSTRAINT FKSchedulese704692 FOREIGN KEY (Schedulesessionid) REFERENCES Schedulesession (id);

ALTER TABLE Schedulesession ADD CONSTRAINT FKSchedulese364705 FOREIGN KEY (Scheduleid) REFERENCES Schedule (id);

ALTER TABLE Schedulesession ADD CONSTRAINT FKSchedulese244034 FOREIGN KEY (Requestsessionid) REFERENCES Requestsession (id);

ALTER TABLE Schedulesession ADD CONSTRAINT FKSchedulese655054 FOREIGN KEY (Shipid) REFERENCES Ship (id);

ALTER TABLE Schedulesession_Device ADD CONSTRAINT FKSchedulese875078 FOREIGN KEY (Deviceid) REFERENCES Device (id);

ALTER TABLE Requestsession_Device ADD CONSTRAINT FKRequestses982065 FOREIGN KEY (Requestsessionid) REFERENCES Requestsession (id);

ALTER TABLE Requestsession_Device ADD CONSTRAINT FKRequestses959462 FOREIGN KEY (Deviceid) REFERENCES Device (id);

ALTER TABLE Shiptype_Mode ADD CONSTRAINT FKShiptype_M206127 FOREIGN KEY (Shiptypeid) REFERENCES Shiptype (id);

ALTER TABLE Shiptype_Mode ADD CONSTRAINT FKShiptype_M734920 FOREIGN KEY (Modeid) REFERENCES Mode (id);

ALTER TABLE Statementsession_Device_Mode ADD CONSTRAINT FKStatements660401 FOREIGN KEY (Statementsession_Deviceid) REFERENCES Statementsession_Device (id);

ALTER TABLE Statementsession_Device_Mode ADD CONSTRAINT FKStatements997322 FOREIGN KEY (Modeid) REFERENCES Mode (id);

ALTER TABLE Schedulesession_Device_Mode ADD CONSTRAINT FKSchedulese490523 FOREIGN KEY (Schedulesession_Deviceid) REFERENCES Schedulesession_Device (id);

ALTER TABLE Schedulesession_Device_Mode ADD CONSTRAINT FKSchedulese865425 FOREIGN KEY (Modeid) REFERENCES Mode (id);

ALTER TABLE Requestsession_Device_Mode ADD CONSTRAINT FKRequestses815078 FOREIGN KEY (Requestsession_Deviceid) REFERENCES Requestsession_Device (id);

ALTER TABLE Requestsession_Device_Mode ADD CONSTRAINT FKRequestses824996 FOREIGN KEY (Modeid) REFERENCES Mode (id);

ALTER TABLE Devicecondition ADD CONSTRAINT FKDevicecond855293 FOREIGN KEY (Deviceid) REFERENCES Device (id);

ALTER TABLE Stationcondition ADD CONSTRAINT FKStationcon82685 FOREIGN KEY (Stationid) REFERENCES Station (id);

ALTER TABLE Shipcondition ADD CONSTRAINT FKShipcondit148560 FOREIGN KEY (Shipid) REFERENCES Ship (id);

ALTER TABLE Shiptask ADD CONSTRAINT FKShiptask536510 FOREIGN KEY (Shiptypeid) REFERENCES Shiptype (id);

ALTER TABLE Devicecomplex ADD CONSTRAINT FKDevicecomp770283 FOREIGN KEY (Shiptypeid) REFERENCES Shiptype (id);

ALTER TABLE Devicecomplex ADD CONSTRAINT FKDevicecomp165731 FOREIGN KEY (Deviceid) REFERENCES Device (id);

ALTER TABLE Restriction_Device ADD CONSTRAINT FKRestrictio22481 FOREIGN KEY (Restrictionid) REFERENCES Restriction (id);

ALTER TABLE Restriction ADD CONSTRAINT FKRestrictio330838 FOREIGN KEY (Restrictiontypeid) REFERENCES Restrictiontype (id);

ALTER TABLE Restriction_Device ADD CONSTRAINT FKRestrictio818022 FOREIGN KEY (Deviceid) REFERENCES Device (id);

ALTER TABLE Devicecoordinate ADD CONSTRAINT FKDevicecoor321398 FOREIGN KEY (Deviceid) REFERENCES Device (id);

ALTER TABLE Restrictionstation ADD CONSTRAINT FKRestrictio629858 FOREIGN KEY (Restrictionid) REFERENCES Restriction (id);

ALTER TABLE Restrictionstation ADD CONSTRAINT FKRestrictio388040 FOREIGN KEY (Stationid) REFERENCES Station (id);

ALTER TABLE Restrictionship ADD CONSTRAINT FKRestrictio499039 FOREIGN KEY (Restrictionid) REFERENCES Restriction (id);

ALTER TABLE Restrictionship ADD CONSTRAINT FKRestrictio243386 FOREIGN KEY (Shipid) REFERENCES Ship (id);

ALTER TABLE Stationcoordinates ADD CONSTRAINT FKStationcoo828110 FOREIGN KEY (Stationid) REFERENCES Station (id);

ALTER TABLE Shipcoordinates ADD CONSTRAINT FKShipcoordi113904 FOREIGN KEY (Shipid) REFERENCES Ship (id);

ALTER TABLE Devicetype_Mode ADD CONSTRAINT FKDevicetype665305 FOREIGN KEY (Devicetypeid) REFERENCES Devicetype (id);

ALTER TABLE Devicetype_Mode ADD CONSTRAINT FKDevicetype405436 FOREIGN KEY (Modeid) REFERENCES Mode (id);

ПРИЛОЖЕНИЕ Ж

Запросы на чтение и запись к таблицам БД на практике

Ж.1 Проверка БД на доступность

Пример 1 – Планировщик с меткой сессии 0 осуществляет запрос на чтение и запись в таблицу «План» (1) ;

Ожидаемый результат: доступ на чтение – запрещен, доступ на запись – разрешен.

Проверка осуществляется следующими командами:

а) чтение – *SELECT * FROM schedule;*

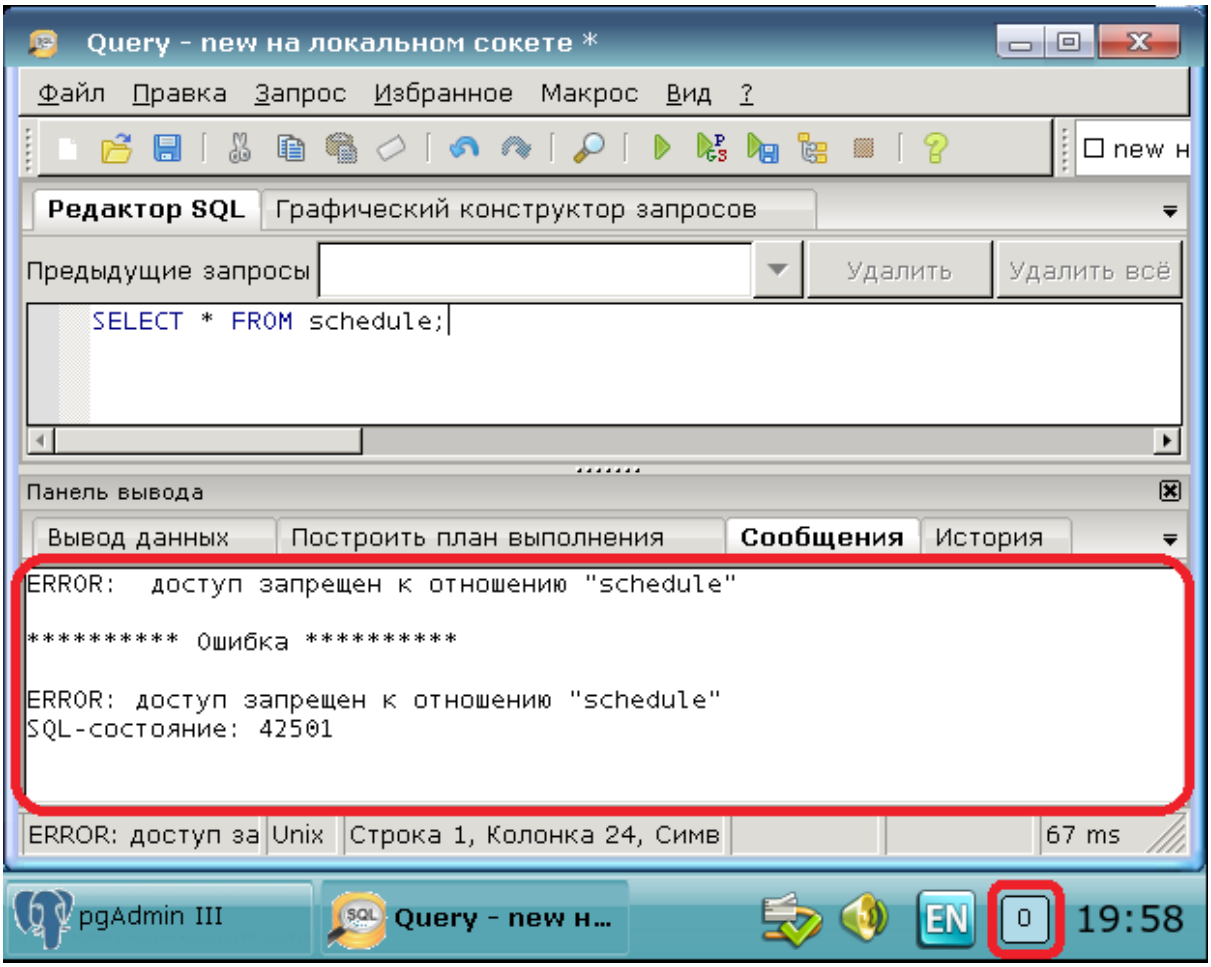

Рисунок 27 – Чтение Планировщиком с меткой сессии 0 таблицы «План»

б) запись – *INSERT INTO schedule VALUES (‘4’, ‘2019–01–28’, FALSE)*;

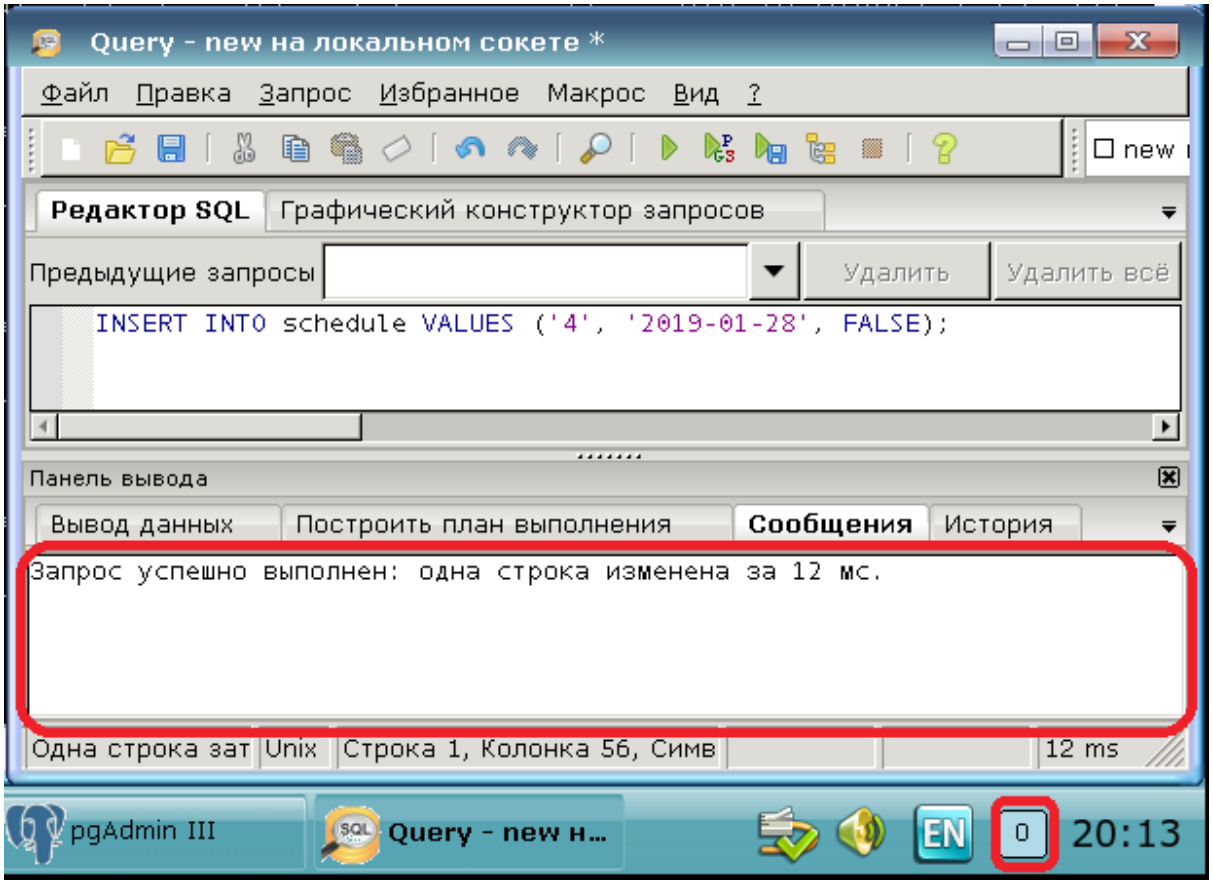

Рисунок 28 – Запись Планировщиком с меткой сессии 0 в таблицу «План»

Полученный результат полностью соответствует ожидаемому результату: доступ на чтение – запрещен, доступ на запись – разрешен. В данном случае наблюдается в части мандатного разграничения доступа действие правила NRU – «нет чтения вверх», так как уровень конфиденциальности таблицы выше уровня допуска пользователя.

Пример 2 – Планировщик с меткой сессии 1 осуществляет запрос на чтение и запись таблицы «План» (1) ;

Ожидаемый результат: доступ на чтение – разрешен, доступ на запись – разрешен.

Проверка осуществляется следующими командами:

а) чтение – *SELECT * FROM schedule;*

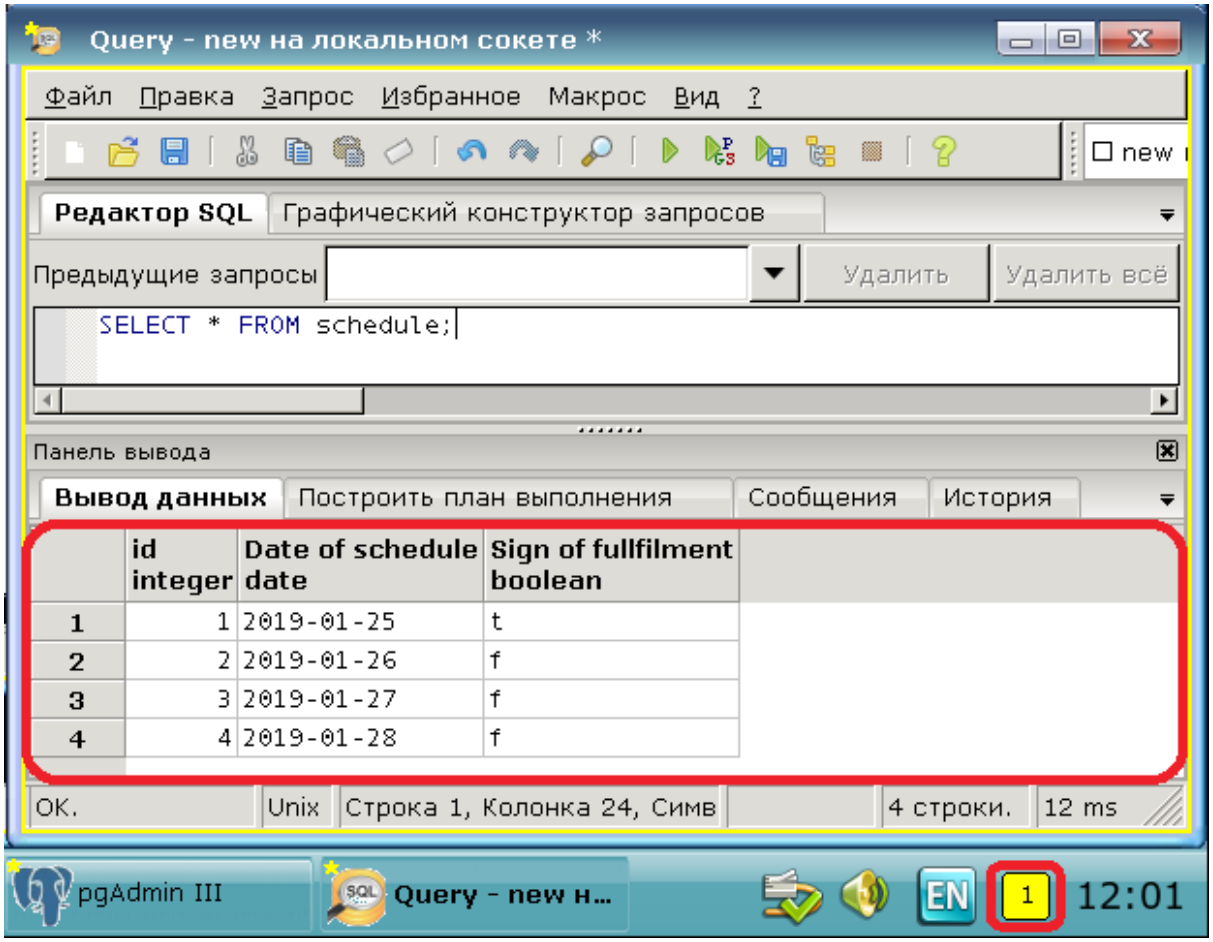

Рисунок 29 – Чтение Планировщиком с меткой сессии 1 таблицы «План»

б) запись – *INSERT INTO shipcondition VALUES (‘5’, ‘2019–01–29’, TRUE).*

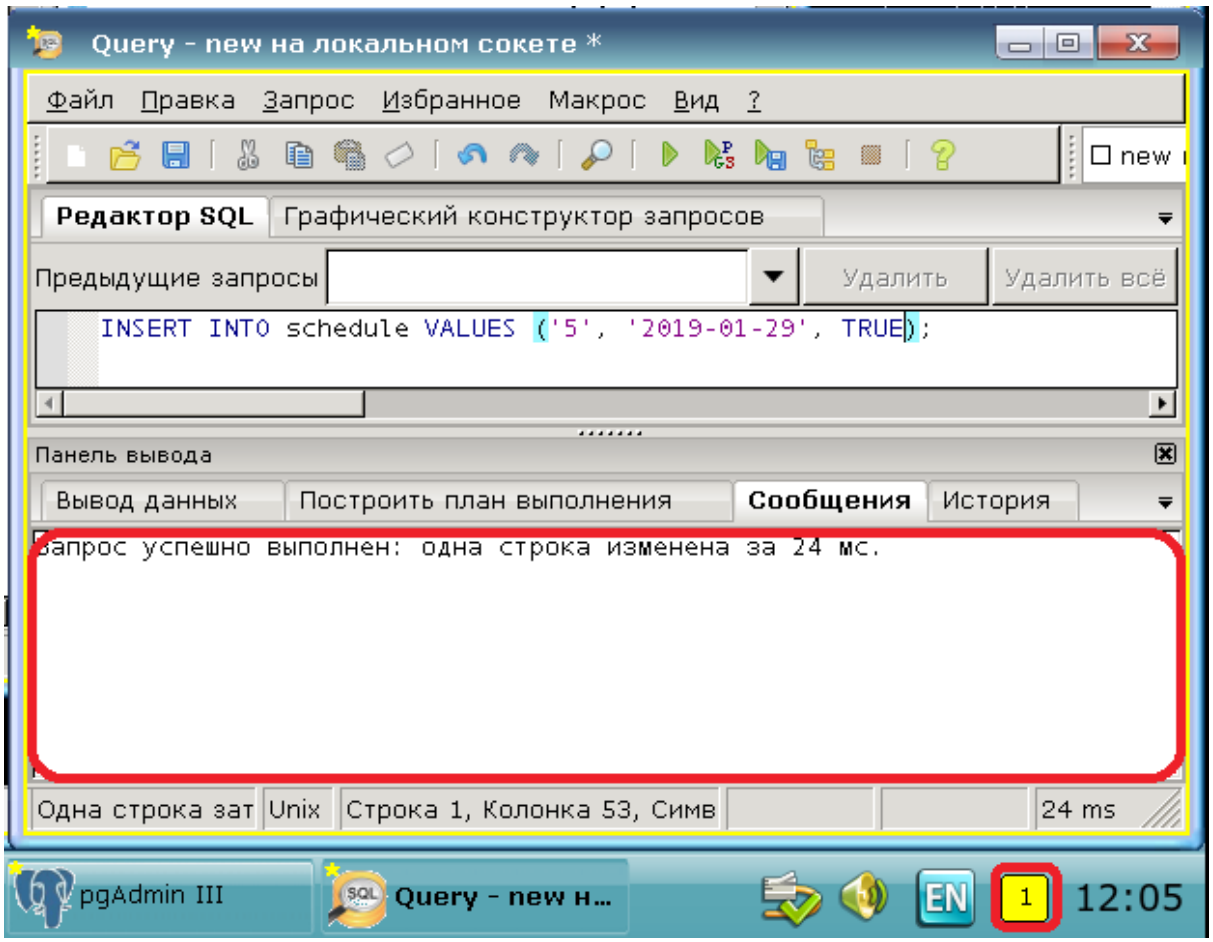

Рисунок 30 – Запись Планировщиком с меткой сессии 1 в таблицу «План»

Полученный результат полностью соответствует ожидаемому результату: доступ на чтение – разрешен, доступ на запись – разрешен. В данном случае наблюдается в части дискреционного и мандатного разграничения доступа разрешение доступа пользователя на чтение и запись в таблицу. Уровень конфиденциальности таблицы и уровень допуска к ней пользователя совпадают.

Пример 3 – Заказчик с меткой сессии 2 осуществляет запрос на чтение и запись «Задача БК» (1);

Ожидаемый результат: доступ на чтение – разрешен, доступ на запись – запрещен.

Проверка осуществляется следующими командами:

а) чтение – *SELECT * FROM shiptask;*

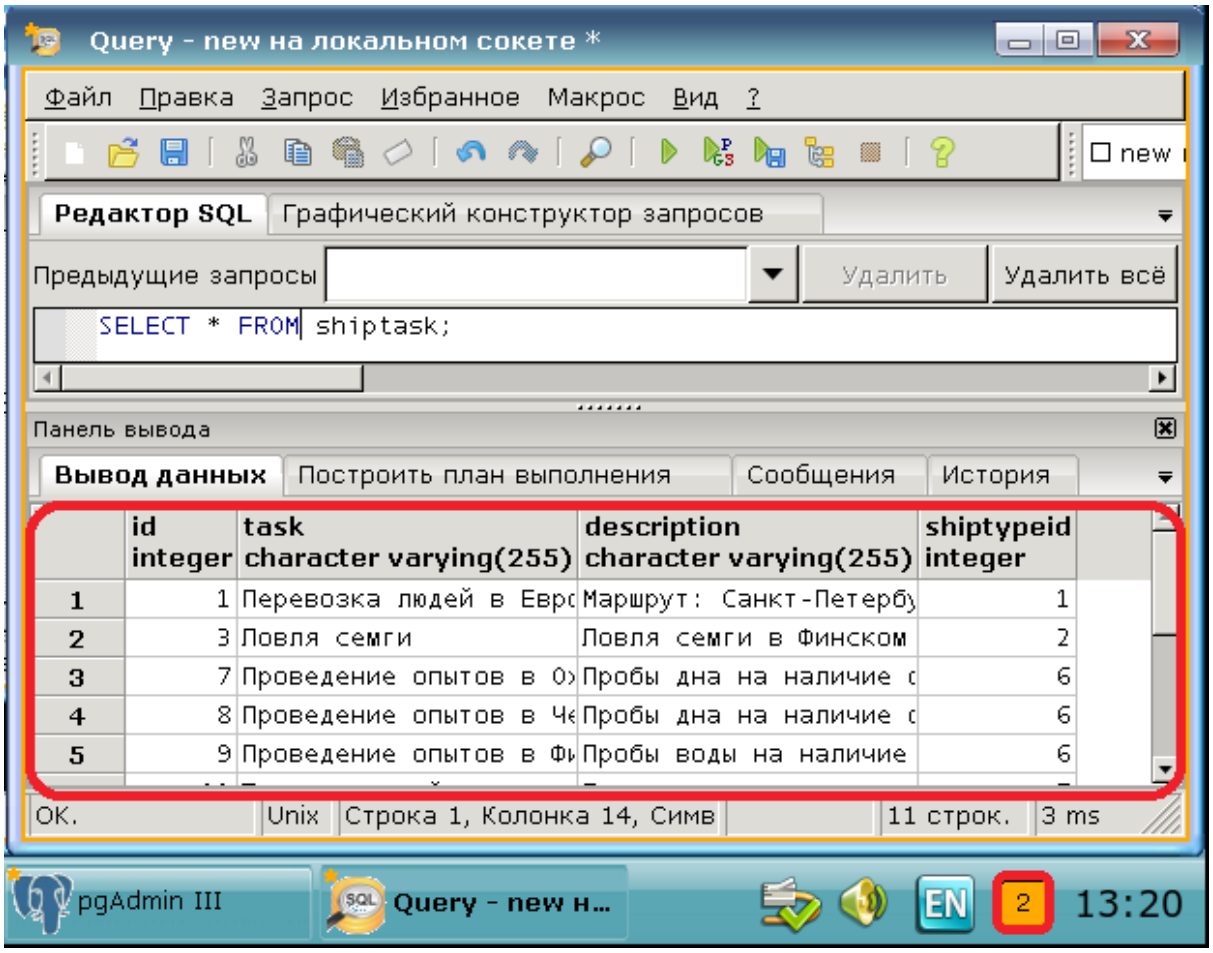

Рисунок 31 – Чтение Заказчиком с меткой сессии 2 таблицы «Задача БК»

б) запись – *INSERT INTO shiptask VALUES (‘11’, ‘Ловля форели’, ‘Ловля форели в Финском заливе’, ‘2’).*

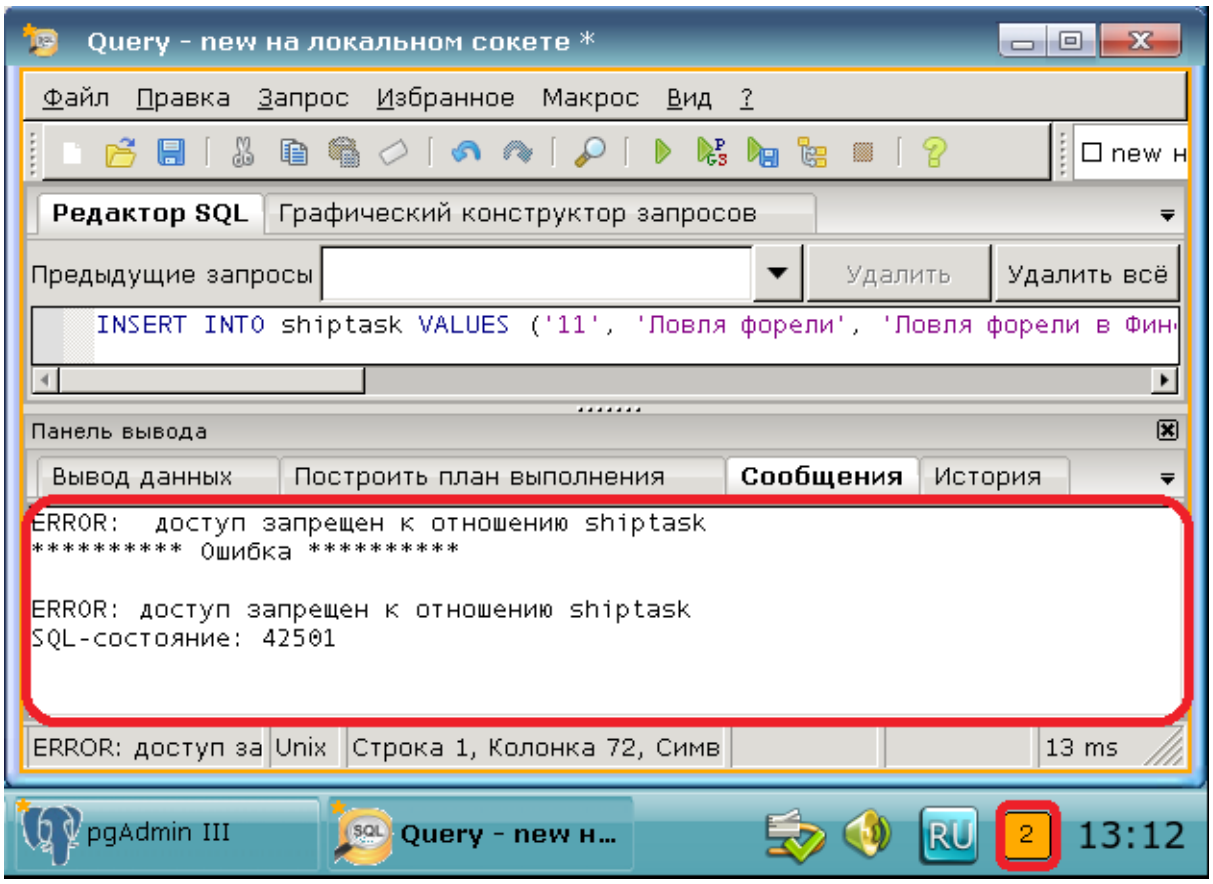

Рисунок 32 – Запись Заказчиком с меткой сессии 2 в таблицу «Задача БК»

Полученный результат полностью соответствует ожидаемому результату: доступ на чтение – разрешен, доступ на запись – запрещен. В данном случае наблюдается в части мандатного разграничения доступа действие правила NWD – «нет записи вниз», так как уровень конфиденциальности таблицы ниже уровня допуска пользователя.

Пример 4 – Начальник ГП с меткой сессии 2 осуществляет запрос на чтение и запись к таблице «Состояние БК» (2);

Ожидаемый результат: доступ на чтение – разрешен, доступ на запись – запрещен.

Проверка осуществляется следующими командами:

а) чтение – *SELECT * FROM shipcondition;*

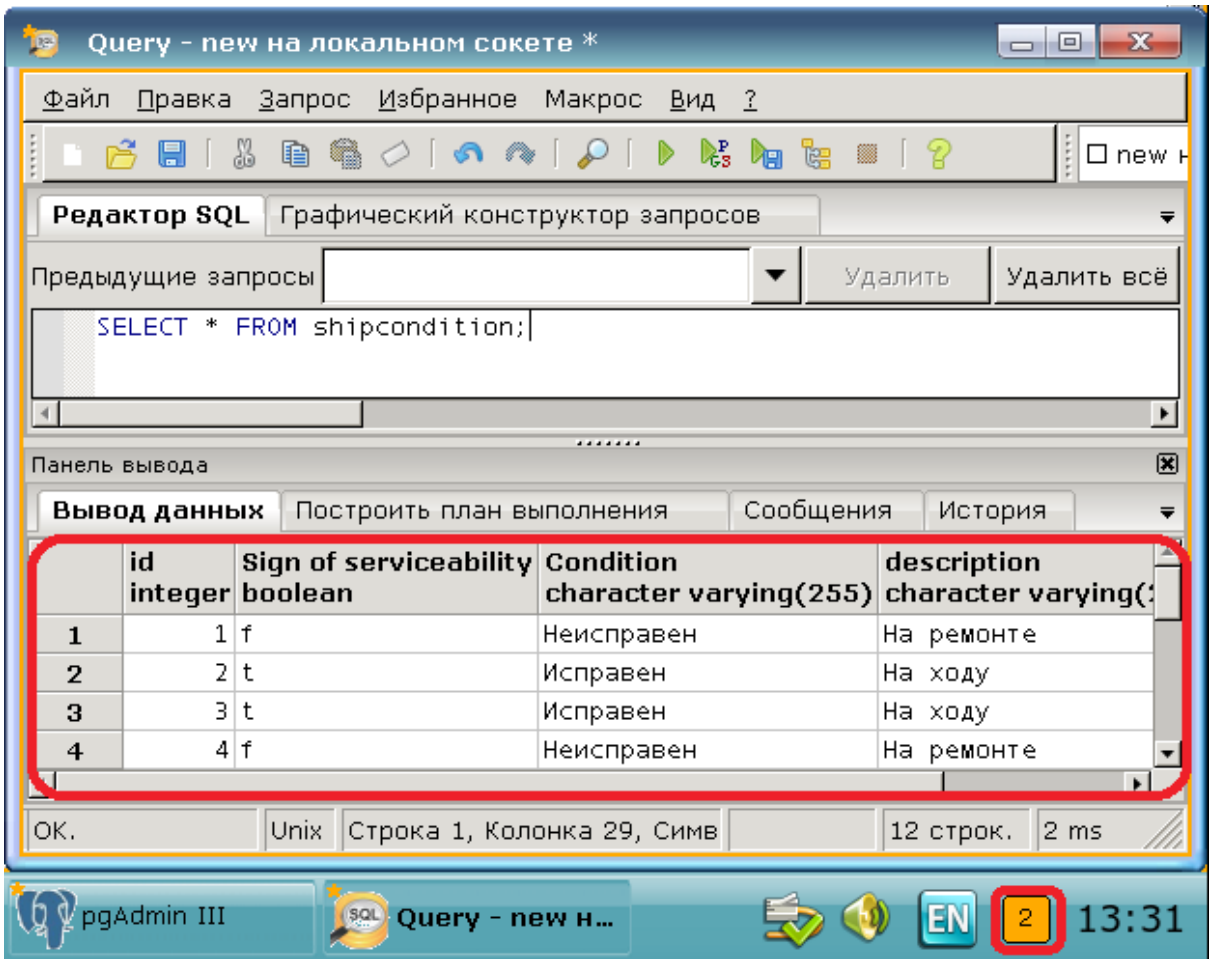

Рисунок 33 – Чтение Начальником ГП с меткой сессии 2 таблицы «Состояние БК»

б) запись – *INSERT INTO shipcondition VALUES (‘13’, FALSE, ‘Исправен’, ‘В порту’, ‘1’)*.

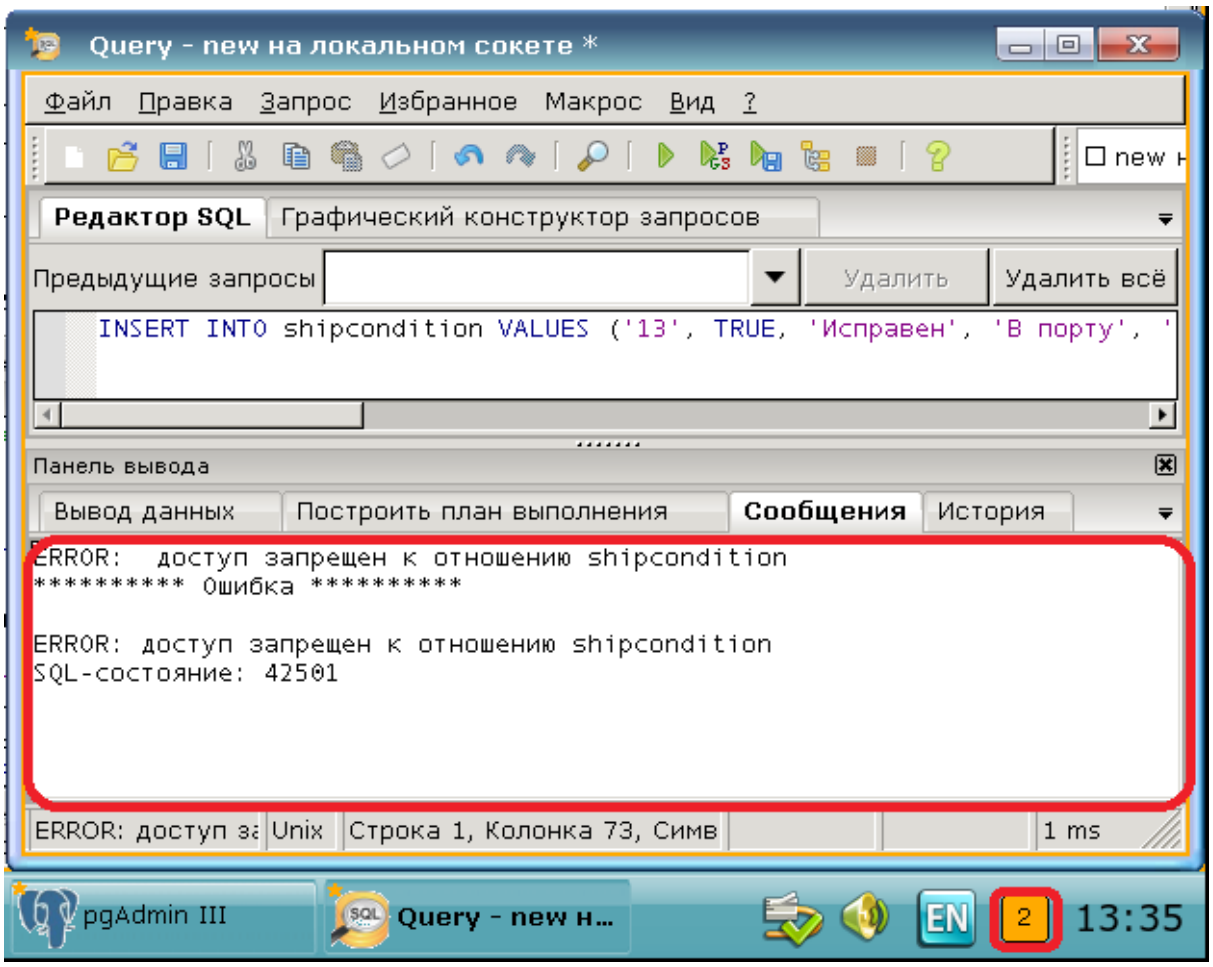

Рисунок 34 – Запись Начальником ГП с меткой сессии 2 в таблицу «Состояние БК»

Полученный результат полностью соответствует ожидаемому результату: доступ на чтение – разрешен, доступ на запись – запрещен. В данном случае наблюдается в части дискреционного разграничения доступа запрет доступа пользователя на запись в таблицу, несмотря на то, что уровень конфиденциальности таблицы и уровень допуска к ней пользователя совпадают.

Пример 5 – Заказчик с меткой сессии 2 осуществляет запрос на чтение и запись к таблице «Состояние БК» (2);

Ожидаемый результат: доступ на чтение – разрешен, доступ на запись – разрешен.

Проверка осуществляется следующими командами:

а) чтение – *SELECT * FROM shipcondition;*

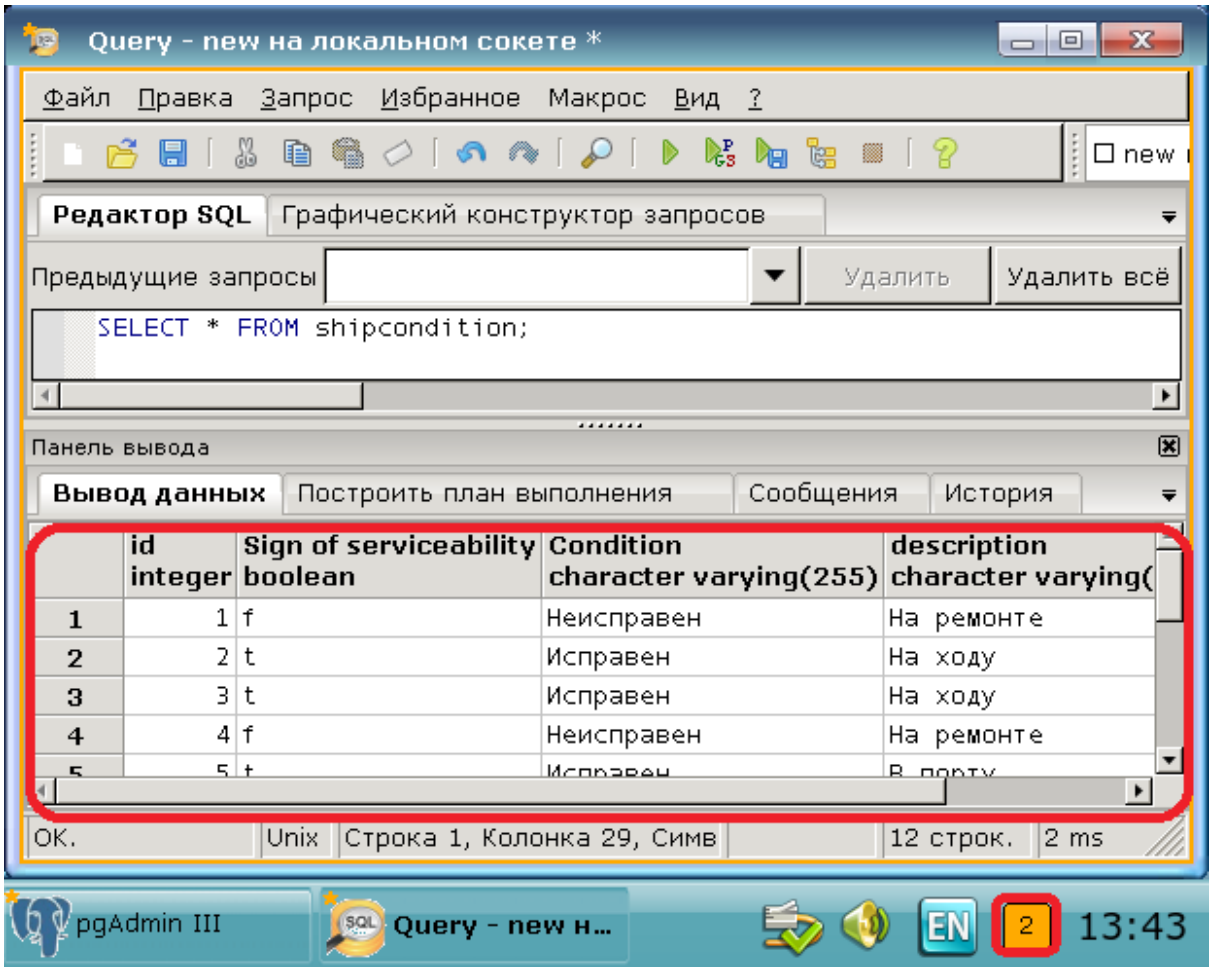

Рисунок 35 – Чтение Заказчиком с меткой сессии 2 таблицы «Состояние БК»

б) запись – *INSERT INTO shipcondition VALUES (‘13’, FALSE, ‘Исправен’, ‘В порту’, ‘1’).*

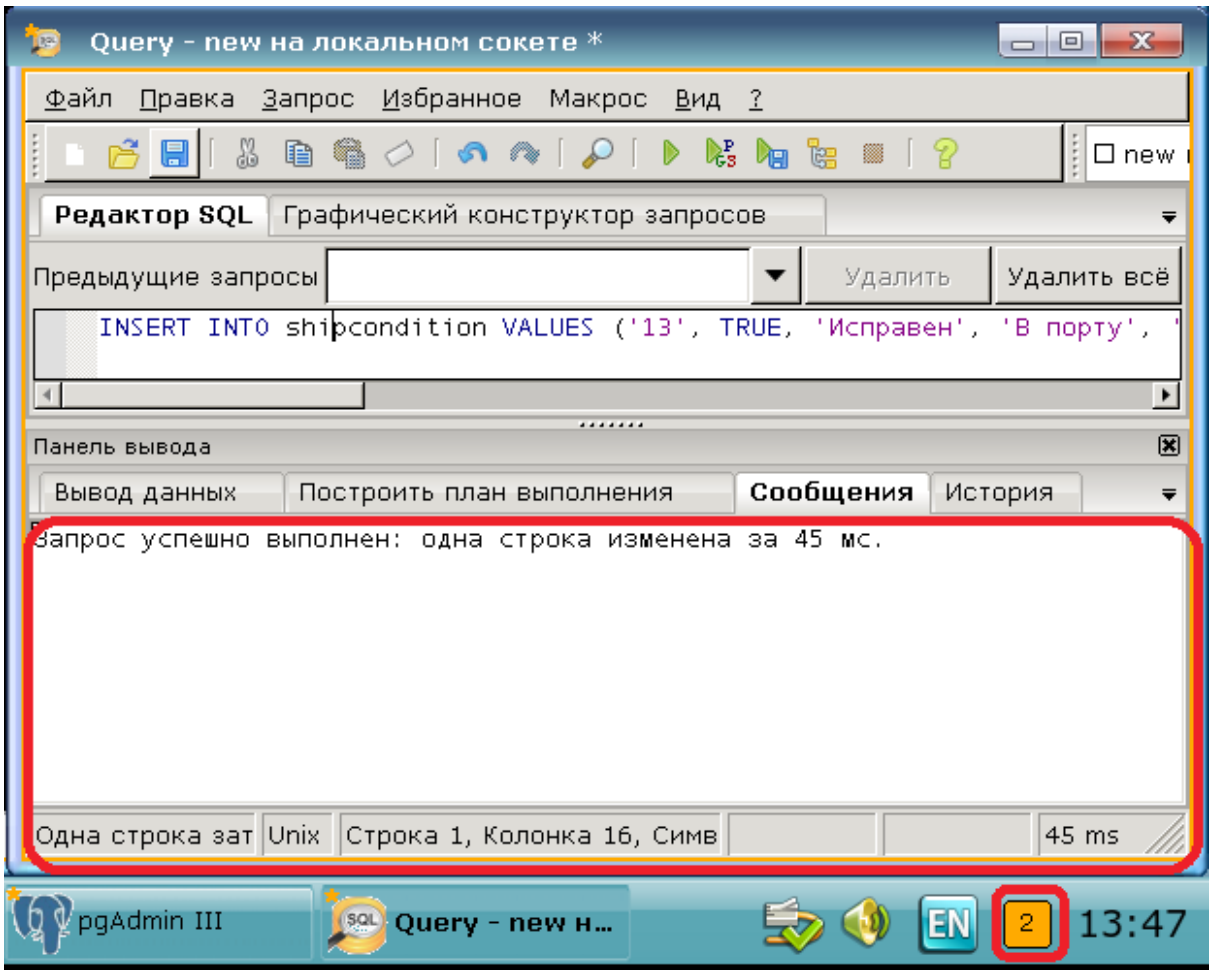

Рисунок 36 – Запись Заказчиком с меткой сессии 2 в таблицу «Состояние БК»

Полученный результат полностью соответствует ожидаемому результату: доступ на чтение – разрешен, доступ на запись – разрешен. В данном случае наблюдается в части дискреционного и мандатного разграничения доступа разрешение доступа пользователя на чтение и запись в таблицу. Уровень конфиденциальности таблицы и уровень допуска к ней пользователя совпадают.

Ж.2 Проверка БД на целостность

Пример 1 – Начальник ГП с меткой сессии 0 осуществляет запрос на чтение к представлению «*ship_coordinates*», в состав которого входят таблицы с меткой 0 и 1;

Ожидаемый результат: доступ на чтение – запрещен.

Проверка осуществляется командой: *SELECT * FROM ship_coordinates;*

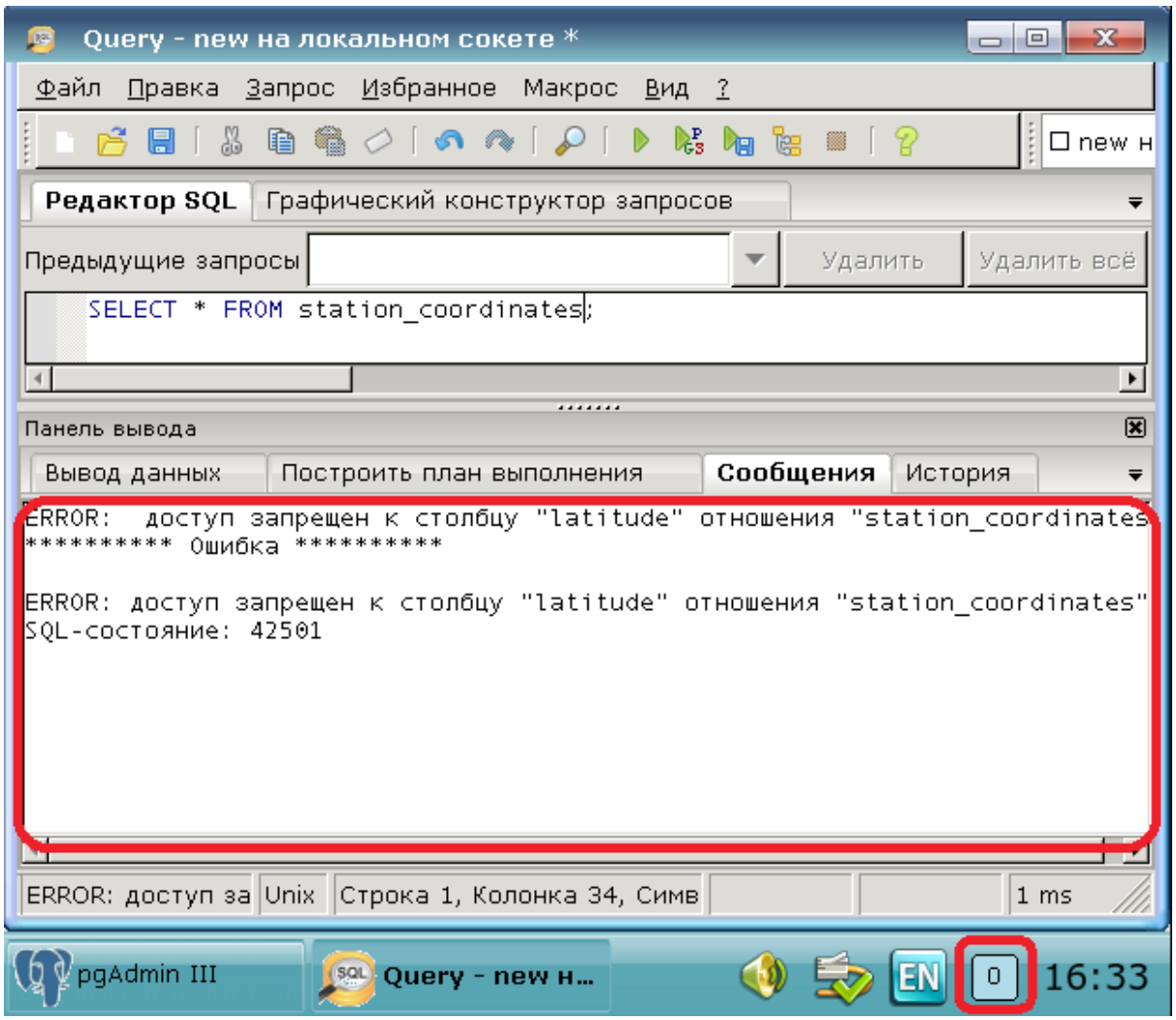

Рисунок 37 – Чтение Начальником ГП с меткой сессии 0 представления «*ship_coordinates*»

Полученный результат полностью соответствует ожидаемому результату: доступ на чтение запрещен. В данном случае наблюдается в части мандатного разграничения доступа действие правила NRU – “нет

чтения вверх”: так как в состав сводной таблицы, к которой осуществляется запрос на чтение, входит таблица, уровень конфиденциальности которой превышает уровень допуска пользователя, то пользователю запрещен доступ к представлению.

Пример 2 – Начальник ГП с меткой сессии 1 осуществляет запрос на чтение к представлению, в состав которого входят таблицы с меткой 0 и 1;

Ожидаемый результат: доступ на чтение – разрешен.

Проверка осуществляется командой: *SELECT * FROM ship_coordinates;*

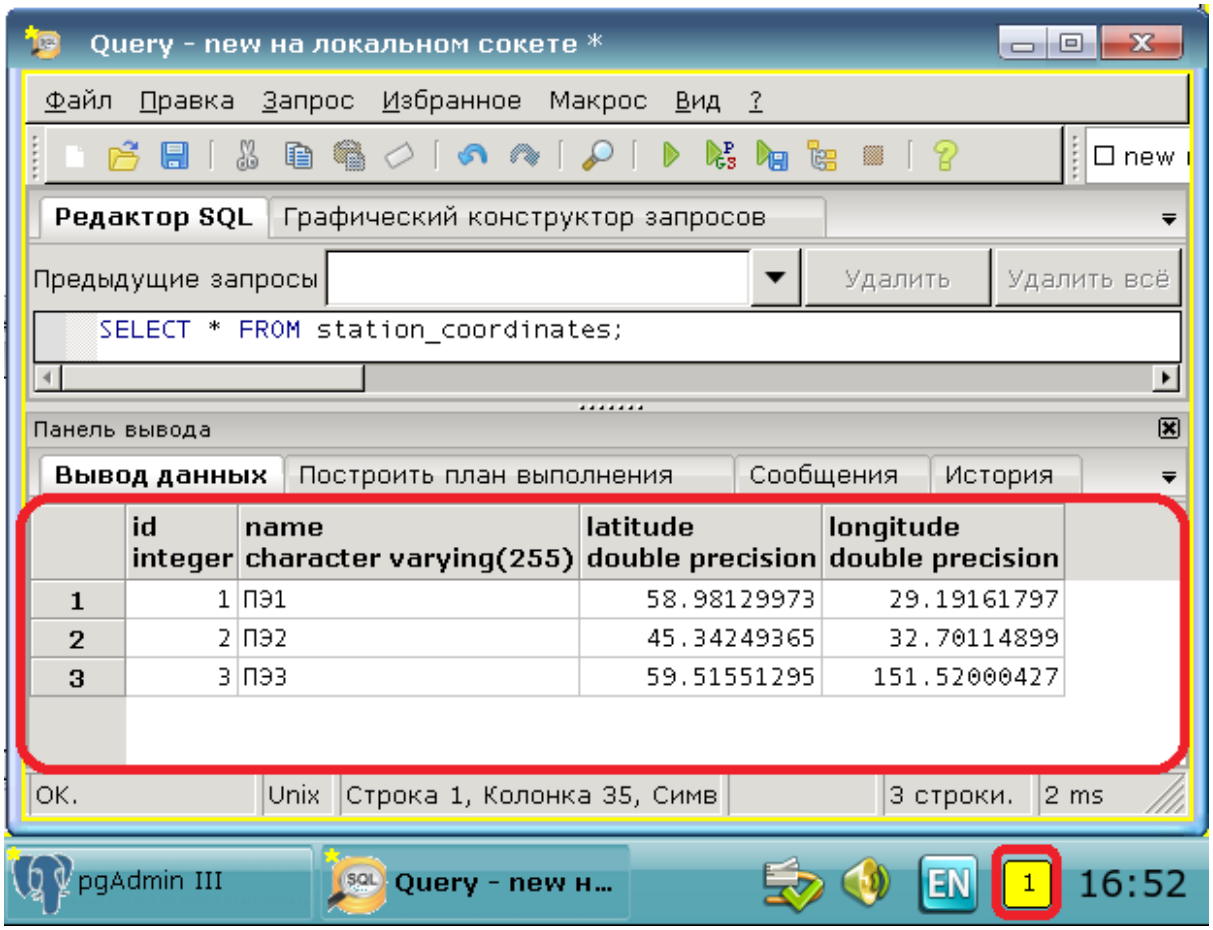

Рисунок 38 – Чтение Начальником ГП с меткой сессии 1 представления «*ship_coordinates*»

Полученный результат полностью соответствует ожидаемому результату: доступ на чтение разрешен. В

данном случае наблюдается в части мандатного разграничения доступа действие правила NRU – “нет чтения вверх”: так как в состав сводной таблицы, к которой осуществляется запрос на чтение, входят таблицы, уровень конфиденциальности которых не превышает уровень допуска пользователя, то пользователю разрешен доступ к представлению.