Рекомендации по построению прикладного программного обеспечения (ППО) для интеграции с механизмами идентификации, аутентификации, авторизации и разграничения доступа операционной системы специального назначения «Astra Linux Special Edition»

Оглавление

1. ОБЩИЕ СВЕДЕНИЯ

Разработка и внедрение информационных систем в настоящее время происходит в условиях нарастающего информационного противоборства и возрастания роли информационной безопасности и импортозамещения, как способа повышения технологической независимости от средств иностранного производства.

В соответствии с требованиями регуляторов в области обеспечения информационной безопасности, в частности — ФСТЭК и ФСБ России, проектирование информационных систем необходимо проводить с учётом применения средств защиты информации (СрЗИ). Эти средства должны входить в состав средств вычислительной техники и автоматизированных систем в виде совокупности программного и технического обеспечения.

Данный документ описывает особенности проектирования прикладного ПО при построении автоматизированных систем (АС) в защищённом исполнении, обрабатывающих информацию ограниченного доступа, на базе платформы операционной системы специального назначения «Astra Linux Special Edition» (ОС СН).

Разработчикам прикладного ПО при построении подобных АС следует обращать внимание на особенности функционирования общесистемного программного обеспечения и встроенных средств защиты информации ОС СН. Взаимодействие компонентов АС, обрабатывающей информацию ограниченного доступа, построенной на платформе ОС СН, в соответствии с требованиями по защите информации (ЗИ), как правило, происходит с учётом работы подсистем идентификации/аутентификации, управления доступом, регистрации и учёта, обеспечения целостности информации.

Прикладное ПО АС в приоритетном порядке должно разрабатываться с применением информационных технологий, реализованных в ОС СН. С точки зрения построения и функционирования прикладного ПО, среди имеющихся встроенных в ОС механизмов ЗИ особое внимание уделяется механизмам идентификации и проверки подлинности субъектов доступа, а

также системе разграничения доступом, в частности мандатному и дискреционному разграничению.

2. ВСТРОЕННЫЕ СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ ОС СН

2.1. Идентификация и аутентификация пользователей

2.1.1. Первоначальная идентификация и аутентификация пользователей в ОС СН

Первоначальная идентификация и аутентификация пользователей в ОС СН основывается на использовании механизма PAM.

Процесс загрузки ОС СН сопровождается инициализацией модуля ядра и запуском сервисов системы безопасности информации PARSEC. По завершению загрузки пользователю предоставляется возможность работы с ОС СН в графическом режиме. Для перехода на пользовательский рабочий стол Fly, пользователю необходимо пройти процедуру идентификации и аутентификации, которая основывается на использовании механизма PAM.

PAM представляет собой набор библиотек (модулей), которые подразделяются на четыре основные категории: модули аутентификации, модули управления учётными записями, модули управления сеансами и модули управления паролями. С помощью этих библиотек системный администратор может организовывать процедуру аутентификации (подтверждение) пользователей прикладными программами.

Общее описание первоначальной аутентификации по PAM представлено в документе «Руководство по КСЗ. Часть 1. РУСБ.10015-16 97 01-1», раздел 2 - «Идентификация и аутентификация».

2.1.2. Идентификация и аутентификация пользователей в условиях работы единого пространства пользователей с использованием протокола Kerberos

Единое пространство пользователей (ЕПП) представляет собой средства организации работы пользователя в сети компьютеров, работающих под управлением ОС. В основу положен доменный принцип

построения сети, подразумевающий объединение в одну сеть логически связанных компьютеров, например, принадлежащих одной организации. При этом пользователь получает возможность работы с сетевыми ресурсами сети и взаимодействия с другими пользователями. Сетевая аутентификация и централизация хранения информации об окружении пользователя подразумевает использование двух основных механизмов: поддержки кросс-платформенных серверных приложений для обеспечения безопасности (NSS) и подгружаемых аутентификационных модулей (PAM). Сквозная аутентификация в сети (Single-Sign-On, SSO) реализуется на основе протокола Kerberos с использованием службы каталогов LDAP в качестве источника данных для базовых системных сервисов на базе механизмов NSS и PAM.

Полное описание архитектуры ЕПП и средств его организации представлено в документе «Руководство администратора. Часть 1. РУСБ.10015-01 95 01-1», раздел 7 - «Средства организации ЕПП».

Общий алгоритм процесса первоначальной аутентификации пользователя по протоколу Kerberos в системе, где организовано ЕПП, заключается в следующем:

1. Рабочая станция (клиент Kerberos) передаёт идентификационные данные клиента Центру распространения ключей KDC (key distribution center) и запрашивает TGT (ticket-granting ticket — билет на получение билета). Этот запрос обрабатывается специальным компонентом Kerberos, который называется TGS (ticket-granting service — служба получения билета). KDC ищет имя пользователя, предоставленное в идентификационных данных, в базе данных. Если имя присутствует в ней, KDC возвращает в этом билете имя пользователя, которому он предназначен, время выдачи билета и время, в течение которого он остаётся действительным, кодирует, используя для этого пароль, содержащийся в базе данных, и передаёт его клиенту.

2. Клиент получает TGT и расшифровывает его с помощью пароля, введённого пользователем. Если попытка расшифровки оказывается

успешной, клиент сохраняет билет для дальнейшей работы. Все действия с билетом остаются прозрачными для пользователя.

Пройдя процедуру аутентификации в системе, где организовано ЕПП, пользователь избавляется от необходимости многократного ввода данных своей учётной записи для получения доступа ко всем доступным приложениям, настроенным на взаимодействие с Kerberos.

Получение доступа клиента к приложениям, настроенным на взаимодействие с Kerberos, происходит благодаря сквозной авторизации (Single-Sign-On, SSO) по протоколу Kerberos и заключается в следующем:

1) Используя данные, содержащиеся в полученном при аутентификации билете Kerberos, клиент отправляет KDC запрос на получение такого билета, который давал бы возможность взаимодействовать с требуемым целевым сервером (приложением, настроенным на взаимодействие с Kerberos). Поскольку данные, содержащиеся в полученном при аутентификации билете Kerberos, были успешно расшифрованы, а затем снова зашифрованы, KDC принимает их как корректные и передаёт клиенту новый билет. Этот билет зашифрован паролем целевого сервера (его знают только сервер и KDC) и содержит имя пользователя, инициировавшего запрос, имя службы, доступ к которой должен быть предоставлен, время выдачи билета, время его действия, код сеанса и другую информацию. Код сеанса выполняет роль нового пароля; этот пароль создан KDC и предназначен для совместного использования клиентом и сервером. Для того чтобы уменьшить риск перехвата и незаконного использования информации, устанавливается малое время действия билета.

2) Клиент принимает билет на получение услуг, но не предпринимает попытки расшифровать его (действия с этим билетом также прозрачны для пользователя).

3) Клиент передаёт билет на получение услуг целевому серверу. Этот билет рассматривается как запрос на инициализацию сеанса передачи данных.

4) Сервер расшифровывает билет, пользуясь для этого своим паролем (паролем целевого сервера).

5) Клиент получает ответ от сервера. Если данные корректны, клиент предполагает, что сервер аутентифицирован, завершает процедуру установления соединения и начинает передачу информации. Информация передаётся только в том случае, если от сервера получен допустимый ответ.

6) С этого момента процесс обмена данными происходит так, как будто система Kerberos не используется, за исключением того, что в составе взаимодействующих приложений действуют средства кодирования и декодирования данных (в обычных приложениях такие средства отсутствуют). Со временем срок действия TGT и билета на получение услуг истекает. Срок действия билетов обычно устанавливается равным нескольким часам. Если же такая ситуация возникла в течение сеанса, билеты должны быть обновлены.

2.2. Дискреционный принцип контроля доступа

В ОС СН реализован механизм дискреционных правил разграничения доступа (ПРД) именованных субъектов (пользователей) к именованных объектам. Реализация механизма дискретных ПРД обеспечивает наличие для каждой пары (субъект-объект) явное и недвусмысленное перечисление разрешённых типов доступа.

Объектами доступа являются:

- файлы;
- устройства;
- соединения (сокеты);
- механизмы IPC (разделяемая память, очереди сообщение и др.).

В ОС СН механизм дискреционного управления доступом обеспечивает проверку дискреционных ПРД, формируемых в виде базовых

ПРД ОС семейства Linux - идентификаторов субъектов (идентификатор пользователя (UID) и идентификатор группы (GID), имеющих определённый доступ к объекту (чтение, запись, исполнение). Кроме того, для формирования дискреционных ПРД в ОС СН используются списки контроля доступа (ACL) и механизм системных привилегий ОС семейства Linux. Права доступа включают список (битовую маску) из девяти пунктов: по три вида доступа для трёх классов — пользователя-владельца, группы-владельца и всех остальных.

Механизмы контроля дискреционного разграничения доступа реализованы в ядре ОС. При обращении процесса к объекту (с запросом доступа определённого вида, т.е. на чтение, запись или исполнение) система проверяет совпадение идентификаторов владельцев процесса и владельцев файла в определённом порядке, и в зависимости от результата, применяет ту или иную группу прав.

Механизм дискреционного контроля доступа в ОС СН подробнее описан в документе «Руководство по КСЗ. Часть 1, РУСБ.10015-16 97 01-1», раздел 3 - «Дискреционное управление доступом».

2.3. Мандатный принцип контроля доступа

С каждым субъектом и объектом ОС СН связаны мандатный контекст безопасности и метка безопасности (мандатная метка) соответственно. При создании субъектом любого из выше приведённых объектов, объект наследует метку на основе мандатного контекста безопасности процесса.

Механизмы контроля мандатного разграничения доступа реализованы в ядре ОС и затрагивают такие подсистемы, как ФС, сетевую защищённую ФС, стек TCP/IP (IPv4). Метка безопасности состоит из классификационной метки, определяемой уровнем и категориями, и уровня целостности (категории целостности). При создании субъектом объекта, относящегося к любой из вышеперечисленных подсистем, объект наследует метку на основе мандатного контекста безопасности процесса.

В ОС СН сетевые соединения рассматриваются как средство межпроцессного взаимодействия и подвергаются мандатному контролю доступа. Для этого в сетевые пакеты протокола IPv4 в соответствии со стандартом ГОСТ Р 58256-2018 внедряются метки безопасности, заданные для объекта – сетевого соединения (сокета). При этом метка объекта (сокета) наследуется от субъекта (процесса). Приём сетевых пакетов подчиняется мандатным правилам разграничения доступа. Метка объекта может иметь тип, позволяющий создавать сетевые сервисы, принимающие соединения с любыми метками безопасности.

Отсутствие метки на объекте доступа является синонимом нулевой метки безопасности. Таким образом, ядро ОС, в которой все объекты и субъекты доступа имеют уровень секретности «несекретно», функционирует аналогично стандартному ядру ОС Linux.

Механизмы мандатного управления доступом и мандатного контроля целостности описаны в документе «Руководстве по КСЗ. Часть 1 РУСБ.10015-16 97 01-1», раздел 4 - «Мандатные управление доступом и контроль целостности».

2.4. Встроенные средства защиты информации общего программного обеспечения

В состав общего программного обеспечения (ОПО) ОС СН входят программы, чаще всего востребованные при построении различных АС: системы управления базами данных (СУБД) реляционного типа, средства работы в сетях, набор офисных программ, система вёрстки текстов, средства работы с мультимедиа-данными и графикой.

Для разработчиков АС можно выделить следующие важные компоненты:

1) для разработки ПО с использованием СУБД:

- защищенная СУБД PostgreSQL версии 9.6.

2) для разработки web-ориентированного ПО:

- HTTP-сервер Apache2;

- браузер Firefox.

2.4.1. Встроенные средства защиты СУБД PostgreSQL

В качестве защищённой СУБД в составе ОС СН используется PostgreSQL, доработанная для обеспечения соответствия требованиям по защите информации от несанкционированного доступа. СУБД PostgreSQL предназначена для создания и управления реляционными БД и предоставляет многопользовательский доступ к расположенным в них данным. Единицей хранения и доступа к данным является строка, состоящая из полей, идентифицируемых именами столбцов.

Идентификация и аутентификация в СУБД PostgreSQL

СУБД PostgreSQL предлагает несколько различных методов аутентификации клиента.

Метод, используемый для аутентификации конкретного клиентского соединения, может быть выбран на основе адреса узла сети клиента, БД и пользователя. В соответствии с требованиями по защите информации от НСД требуется сопоставление пользователей СУБД пользователям ОС. Таким образом, при настройке аутентификации в СУБД следует использовать только методы аутентификации, в которых осуществляется подобное сопоставление. В ОС СН таким требованиям отвечает PAM-аутентификация и сквозная аутентификация на основе протокола Kerberos, используемая в ЕПП.

Описание и необходимые настройки аутентификации в СУБД по данным протоколам представлены в документе «Руководство администратора. Часть 2. РУСБ.10015-01 95 01-2», подраздел 1.4 - «Настройка аутентификации».

Средства дискреционного и мандатного разграничения доступа в СУБД PostgreSQL

Данные в реляционной БД хранятся в отношениях (таблицах), состоящих из строк и столбцов. Кроме таблиц, существуют другие типы объектов БД (виды, представления, процедуры, функции, триггеры и др.),

которые предоставляют доступ к данным, хранящимся в таблицах. Таким образом, в защищённом комплексе программ СУБД определены типы объектов, с каждым из которых ассоциируется определённый набор типов доступа (возможных операций).

Для каждого объекта явно задаётся список ACL, содержащий список поименованных субъектов БД (пользователей, групп или ролей) и разрешённых им операций. В дальнейшем при разборе запроса к БД осуществляется проверка возможности предоставления доступа субъекта к объекту на основании типа запроса.

В общем случае отдельная строка таблицы не является однозначно идентифицируемым объектом (каждая строка идентифицируется только набором содержимого своих полей, но без специальных действий, например, создания первичного ключа или физического уникального идентификатора строки в БД, такая идентификация не является уникальной), и соответственно дискреционные ПРД к ней применены быть не могут. Столбцы могут являться объектами дискреционного управления доступом, поскольку могут быть однозначно идентифицированы по составному имени объекта и столбца (имя столбца внутри объекта является уникальным).

При выполнении любого запроса пользователя (субъекта БД) к защищаемому ресурсу (объекту БД) выполняется дискреционное управление доступом на основе установленных пользователю прав. Для каждой выполняемой операции производится проверка наличия права у пользователя на выполнение данной конкретной операции. Дискреционные ПРД применяются после разбора запроса пользователя и построения плана его выполнения.

Принципы дискреционного управления доступом СУБД PostgreSQL описаны в документе «Руководство по КСЗ. Часть 1. РУСБ.10015-01 97 01-1», подраздел 3.4 - «Дискреционное управление доступом в СУБД PostgreSQL».

В основе мандатного механизма разграничения доступа лежит управление доступом к защищаемым ресурсам БД на основе иерархических и неиерархических меток доступа. Это позволяет реализовать многоуровневую защиту с обеспечением разграничения доступа пользователей к защищаемым ресурсам БД и управление потоками информации. В качестве иерархических и неиерархических меток доступа при использовании СУБД в ОС СН используются метки конфиденциальности ОС.

При обращении пользователя к БД определяются его допустимый диапазон меток и набор специальных мандатных атрибутов. Если пользователю не присвоена метка, то он получает по умолчанию нулевую метку, соответствующую минимальному уровню доступа. Максимальная метка определяется по метке, заданной при регистрации пользователя в ОС. Сервер БД также может работать на разных уровнях доступа. В случае если метка пользователя выше метки сервера, то пользователю будут разрешены только операции чтения. Текущая метка пользователя определяется по установленному соединению и может быть задана в пределах его допустимого диапазона мандатных атрибутов при наличии соответствующей привилегии.

СУБД PostgreSQL не имеет собственного механизма назначения, хранения и модификации меток пользователей и использует для этого механизмы ОС.

Для хранения метки объекта БД введено служебное поле maclabel. При создании объекта БД (таблицы), он маркируется меткой безопасности пользователя текущей сессии БД. В дальнейшем по этой метке производится разграничение доступа к созданному объекту.

Применение мандатных ПРД осуществляется на уровне доступа к объектам БД и на уровне доступа непосредственно к данным (на уровне записей). Проверка мандатных прав доступа к таблицам осуществляется одновременно с проверкой дискреционных прав доступа к ним, после

разбора и построения плана запроса, непосредственно перед его выполнением, когда определены все необходимые для проверки данные и проверяемые объекты. Проверка мандатных прав доступа к записям таблиц осуществляется в процессе выполнения запроса при последовательном или индексном сканировании данных.

Варианты использования мандатных ПРД для объектов, его столбцов и непосредственно строки приведены в документе «Описание применения. РУСБ.10265-01 31 01», подпункт 4.1.14.2 - «Мандатное управление доступом в защищённой СУБД».

Принципы мандатного управления доступом в СУБД PostgreSQL описаны в документе «Руководство по КСЗ. Часть 1. РУСБ.10015-01 97 01-1», подраздел 4.10 - «Мандатное управление доступом в СУБД PostgreSQL».

2.4.2. Встроенные средства защиты информации комплекса гипертекстовой обработки данных

Защищённый комплекс программ гипертекстовой обработки данных представлен web-сервером Apache и браузером Mozilla Firefox.

Web-сервер Apache2 из состава ОС СН доработан для интеграции с ядром ОС СН и базовыми библиотеками с целью обеспечения мандатного управления доступом при организации удалённого доступа к информационным ресурсам в информационных системах, обрабатывающих защищаемую информацию. Обеспечение мандатного управления доступом реализовано на основе программного интерфейса библиотек подсистемы безопасности PARSEC.

Web-сервер запускается как сервис ОС СН. Обслуживание запросов пользователей осуществляется в дочернем процессе, созданном в контексте безопасности пользователя. Информационные ресурсы, к которым осуществляется доступ, хранятся как объекты ФС, БД. Доступ к защищаемой информации разграничивается средствами расширенной подсистемы безопасности PARSEC.

На серверах комплексов программ гипертекстовой обработки данных при обработке запросов на соединение выполняется получение мандатного контекста соединения, унаследованного от субъекта — процесса, инициировавшего запрос к серверу. Сокет сервера, ожидающий входящих запросов на соединение, работает в контексте процесса, имеющего привилегию для приёма соединений с любыми уровнями секретности. После установки соединения и успешного прохождения процедуры идентификации и аутентификации пользователя процесс сервера, обрабатывающий запросы пользователя, переключается в контекст безопасности пользователя, сбрасывает привилегии, и обрабатывает запросы пользователя. При этом обращение к ресурсам сервера происходит в контексте пользователя, инициировавшего начальный запрос.

Описание управления мандатным разграничением доступа в комплексе гипертекстовой обработки данных представлено в документе «Руководство по КСЗ. Часть 1. РУСБ.10015-01 97 01-1», подраздел 4.11 - «Мандатное управление доступом в комплексах программ гипертекстовой обработки данных и электронной почты».

Настройка веб-сервера заключается в создании для каждого файлового ресурса своего конфигурационного файла виртуального хоста с учётом выбранного типа аутентификации и авторизации:

- по умолчанию используется модуль PAM из пакета libapache2-mod-authnz-pam. При этом будет использоваться пользовательская БД, прописанная в настройках ОС. Логин и пароль пользователя будут передаваться от пользователя к серверу в открытом виде с использованием метода аутентификации Basic.

- при организации ЕПП с доменным принципом построения сети, в системе должен быть установлен модуль web-сервера Apache 2.2 auth_kerb. Активация модуля web-сервера Apache 2.2 auth_kerb предоставляет возможность организации совместной работы с доменом с использованием для аутентификации пользователей посредством Kerberos метода GSSAPI.

Использование PAM-аутентификации и сквозной аутентификации в случае ЕПП для защищённого комплекса программ гипертекстовой обработки данных описаны в документе «Руководство администратора. Часть 1. РУСБ.10015-01 95 01-1», раздел 6 — «Защищённый комплекс программ гипертекстовой обработки данных».

3. ПРИНЦИПЫ ПОСТРОЕНИЯ ППО

3.1. Особенности функционирования ППО в условиях работы локальной информационной системы (автономного компьютера) на базе ОС СН

Принципы построения прикладного ПО в условиях работы встроенных механизмов ЗИ ОС СН легче всего рассмотреть на примере локальной информационной системы (ИС), исключающей сетевое взаимодействие.

В данной архитектуре ИС будут задействованы следующие механизмы ЗИ ОС СН:

1. Механизмы идентификации и аутентификации.

Первоначальная идентификация и аутентификация пользователя в системе обеспечивается средствами ОС СН и основывается на использовании механизма PAM (см. пункт 2.1.1 настоящего документа).

2. Механизмы контроля мандатного и дискреционного разграничения доступа.

Поскольку в графическую подсистему ОС СН встроена мандатная защита, после прохождения аутентификации пользователю предоставляется возможность выбора мандатного контекста (мандатного уровня и категории) из разрешённого ему диапазона. После выбора пользователя, в системе сохраняется контекст его работы (учётная запись, группы, мандатный уровень и категория), и все запущенные субъектом процессы, в том числе прикладное ПО, наследуют этот контекст.

В зависимости от поставленных целевых задач, прикладное ПО может обращаться к защищаемым объектам АС:

1) Обращение субъекта к защищаемым объектам файловой системы.

При обращении субъекта (в данном случае — процесса прикладного ПО, запущенного в контексте пользователя) к защищаемым объектам файловой системы проверка доступа осуществляется на основе контекста текущего процесса и разрешённых для данного контекста операций. Проверка мандатных прав доступа к файлам осуществляется одновременно с проверкой дискреционных прав доступа к ним.

2) Обращение субъекта к объектам БД.

При попытке соединения с сервером СУБД клиентское приложение указывает пользователя СУБД PostgreSQL, от имени которого осуществляется подключение. В пределах окружения SQL активное имя пользователя СУБД определяет права на объекты БД. Использование защищённого сервера СУБД из состава ОС СН в режиме мандатного управления доступом не допускает отключения аутентификации субъектов доступа путём установки в конфигурационных файлах режима «trust» (без аутентификации). Доступ субъекта к объектам БД в обязательном порядке должен ограничивается средствами аутентификации. При этом, в соответствии с требованиями по защите информации от НСД, необходимо обязательное сопоставление пользователей СУБД и пользователей ОС. При настройке аутентификации в СУБД следует использовать только методы аутентификации, в которых осуществляется подобное сопоставление.

При организации локальной модели ИС, в которой все компоненты (БД, СУБД, клиентские приложения) находятся на одном компьютере, в качестве метода аутентификации в СУБД рекомендуется использовать механизм PAM. Данный метод аутентификации работает подобно методу password, только с учётом использования подключаемых моделей аутентификации PAM в качестве механизма аутентификации. PAM используется только для подтверждения соответствия имени пользователя и

пароля. Таким образом, для аутентификации пользователя с применением PAM необходимо наличие его учётной записи в БД.

Описание необходимых настроек аутентификации по PAM для СУБД PostgreSQL представлено в документе «Руководство администратора, Часть 2, РУСБ.10015-01 95 01-2», пункт 1.4.1 - «Использование PAM аутентификации».

3) Обращение к устройствам.

Доступ к съёмным машинным носителям информации, будь то блочные, символьные устройства ввода-вывода или блочные устройства, которые можно смонтировать, подчиняется мандатным и дискреционным ПРД обычным образом и, следовательно, ввод-вывод информации остаётся в рамках контроля этих правил.

Для ОС СН возможность санкционированного монтирования конкретным пользователем конкретных носителей с конкретными ФС определяется администратором системы. В ОС СН реализованы средства разграничения доступа к подключаемым устройствам на основе правил для менеджера устройств udev (см. документ «Руководство по КСЗ. Часть 1. РУСБ.10015-01 97 01-1», раздел 13 - «Контроль подключения съёмных машинных носителей информации»).

3.2. Особенности функционирования ППО в условиях работы трехзвенной территориально-распределённой ИС на базе ОС СН

3.2.1. Общее описание трехзвенной территориально-распределённой ИС

Многие территориально распределенные ИС, построенные на основе ЛВС, имеют трехзвенную клиент-серверную архитектуру.

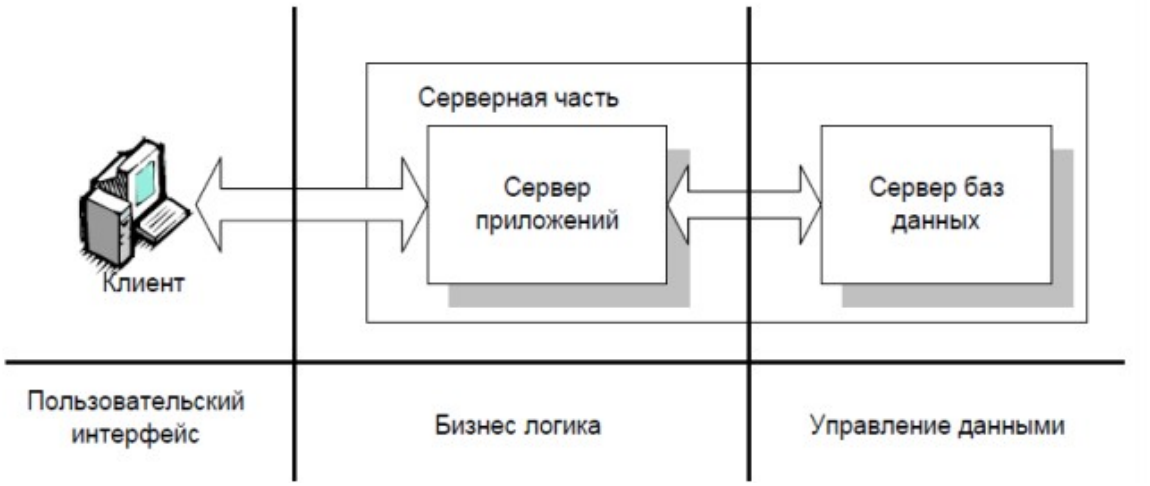

Рисунок 3.1 Трехзвенная клиент-серверная архитектура ИС

Физическое разделение программных компонент позволяет оптимизировать нагрузку как на сетевое, так и на вычислительное оборудование системы.

Выделяются следующие компоненты трехзвенной клиент-серверной архитектуры ИС:

- компонент представления данных (пользовательский интерфейс, клиент);

- прикладной компонент, реализующий бизнес-логику АС (сервер приложений);

- компонент управления ресурсами (ресурсный сервер);

Цель сервера приложений заключается в одновременном обслуживании большого количества клиентов, максимально эффективно используя при этом аппаратные ресурсы. Сервер приложений, получивший от клиента запросы на обработку динамических данных, обращается к ресурсному серверу, клиентом которого он является, со своим собственным запросом. Получив от ресурсного сервера результат выполнения собственного запроса, сервер приложений передаёт данные клиенту.

На ряду с преимуществами трехзвенной архитектуры ИС остро встаёт вопрос обеспечения безопасности информации в условиях взаимодействия компонентов системы по сети — каждый компонент представляет собой потенциальный источник угроз. В общем случае между сторонами идентификации/аутентификации не существует доверенного маршрута. Это

значит, что в общем случае данные, переданные субъектом, могут не совпадать с данными, полученными и использованными для проверки подлинности. У злоумышленника появляется возможность перехвата трафика по сети как до, так и после сервера-приложений, возможность получения информации через уязвимости компонентов системы или получения информации напрямую из ресурсного сервера. Также, с учётом распределения компонентов по разным узлам сети, возникает проблема затруднения управления безопасностью ИС.

3.2.2. Типичные ошибки построения ППО при организации многопользовательской трехзвенной клиент-серверной ИС

Рассмотрим схему организации многопользовательской трехзвенной клиент-серверной ИС, в которой не предполагается использование встроенных средств защиты ОС СН.

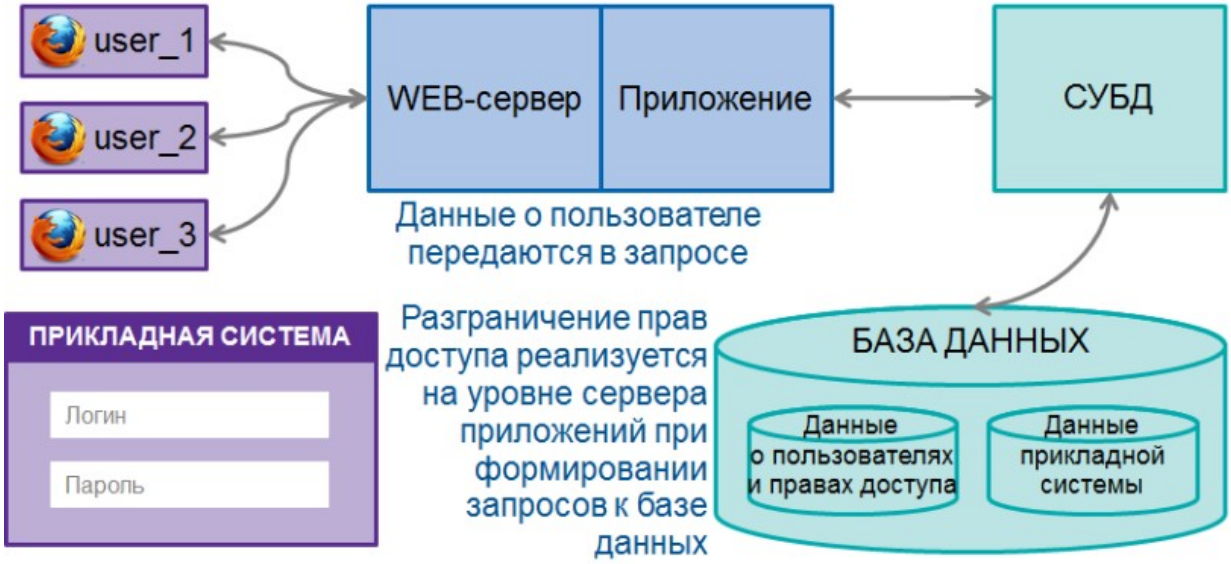

Рисунок 3.2. Пример многопользовательского ППО в трезвенной клиент-серверной архитектуре ИС, не использующей механизмы ЗИ ОС СН.

В качестве клиента в рассматриваемом примере выступает Web-браузер, в качестве сервера приложений — Web-сервер, в качестве ресурсного сервера выступает СУБД. Функции идентификации и аутентификации пользователей возложены на стандартные средства Web-сервера и СУБД, а средства разграничения доступа реализованы на уровне сервера приложений в прикладном ПО (рисунок 3.2). При этом данные о пользователях (включая аутентификационные данные) и их правах доступа

хранятся непосредственно в БД и передаются прикладному ПО при запросе клиента на работу с системой.

Алгоритм взаимодействия компонентов в данном случае будет соответствовать следующей схеме:

1) Аутентифицированный в системе пользователь производит запуск Web-браузера и устанавливает соединение с Web-сервером.

2) Web-сервер, при обращении неавторизованного клиента к защищённому ресурсу, отсылает HTTP статус и добавляет заголовок с указанием схемы и параметров аутентификации. По умолчанию, в Web-сервере используется аутентификация Basic — наиболее простая схема, при которой username и password пользователя передаются в заголовке пакета в незашифрованном виде. Даже при использовании HTTPS протокола, этот способ является лишь относительно безопасным.

3) Web-браузер, при получении такого ответа, автоматически показывает диалог ввода username и password. Пользователь вводит детали своей учетной записи.

4) Во всех последующих запросах к этому web-серверу браузер автоматически добавляет HTTP заголовок, в котором передаются данные пользователя для аутентификации сервером.

5) Сервер приложений инициирует проверку учётной записи пользователя. Для этого он осуществляет обращение к БД, в которой хранятся аутентификационные данные о пользователях и данные о правах их доступа. Обращение сервера приложений к БД осуществляется от лица специального пользователя, выделенного для работы сервера приложений с СУБД. Необходимые данные передаются серверу приложений в соответствии с его запросом.

6) Web-сервер производит аутентификацию пользователя, сравнивая данные из HTTP заголовка и полученные из запроса к БД данные о пользователях.

7) Решение о предоставлении доступа (авторизация) к защищаемым ресурсам БД производится сервером приложений на основании данных о правах пользователя, полученных по запросу сервера приложений. Для этого сервер приложений средствами языка манипулирования данными формирует запрос для получения данных, к которому пользователю разрешен доступ.

8) Обращение к СУБД для выполнения сформированного запроса осуществляется от лица специального пользователя, выделенного для работы с БД (и имеющего доступ ко всем данным БД).

Данная схема имеет ряд недостатков, среди которых можно отметить следующие:

- Существует необходимость многократного ввода пароля пользователя при обращении к различным сервисам ИС.

- Web-приложение не защищено от возможности перебора паролей. Также, как правило, система при регистрации пользователя не проводит проверку на сложность пароля, пароль не имеет срока действия. При аутентификации пароль от браузера может передаваться к серверу открытом виде. Устранение подобных проблем реализуются в виде встраиваемых в web-приложение дополнительных модулей.

- Сервер приложений не переключается в контекст пользователя. Соответственно, при ошибке в реализации логики обработки запроса пользователя (или наличии уязвимости в коде сервера приложений), пользователю может быть предоставлена информация, к которой он не должен получить доступ.

- Разграничение прав доступа к ресурсам ИС происходит на уровне сервера приложений, соответственно прикладное ПО из состава сервера приложений, реализующее эти функции, подлежит обязательной сертификации по требованиям безопасности информации, предъявляемым к средствам разграничения доступа, что приведёт к существенным дополнительным временным и финансовым затратам.

Таким образом, реализация вышеизложенной схемы работы приводит к наличию многих рисков информационной безопасности, а реализация функций разграничения доступа к защищаемым ресурсам в прикладном ПО является серьезной ошибкой с точки зрения информационной безопасности при его построении.

3.2.3. Построение ИС с использованием Web-сервера и Web-браузера из состава ОС СН и использование интегрированных механизмов безопасности ОС СН

С точки зрения информационной безопасности, многоуровневые ИС необходимо конструировать с учётом использования ЕПП (создания домена), обеспечивающего сквозную аутентификацию пользователей по сети, централизованное хранение информации об окружении пользователей, централизованное хранение настроек СЗИ, интеграцию в домен защищённых серверов СУБД и серверов гипертекстовой обработки данных.

Ниже на рисунке 3.3 представлено взаимодействие компонентов трезвенной архитектуры клиент-серверного прикладного ПО с использованием встроенных механизмов ЗИ ОС СН.

Рисунок 3.3. Пример многопользовательского ППО в среде ОС СН

В данной схеме клиент представлен Web-браузером FireFox, в качестве сервера приложений выступает Web-сервер Apache (с работающем в нем прикладным ПО), в качестве ресурсного сервера может выступать

либо СУБД PostgreSQL, либо защищенные ресурсы ОС СН (объекты файловой системы, устройства).

В данном случае взаимодействие компонентов трехзвенной территориально-распределённой ИС происходит с учётом развёрнутой доменной сетевой инфраструктуры ЕПП и встроенных в ОС СН механизмов разграничения доступа. Web-сервер и СУБД настроены на сквозную аутентификацию и авторизацию пользователей с использованием протокола Kerberos.

Обобщенный алгоритм взаимодействия компонентов будет следующим:

1) Пользователь проходит аутентификацию в системе по протоколу Kerberos (см. пункт 2.1.2 настоящего документа) с загрузкой защищённого рабочего стола Fly. Сопровождается выбором мандатного контекста из разрешённого диапазона.

2) Пользователь производит запуск в сеансе пользователя Web-браузера Firefox. Web-браузер запускается в контексте пользователя. Обращение к Web-серверу из приложения Web-браузера Firefox инициирует установку защищённого сетевого соединения. ОС добавляет в каждый пакет на уровне IP классификационную метку, соответствующую мандатному уровню пользователя, выполнившего операцию.

Обращение Web-браузера к Web-серверу будет сопровождаться сквозной авторизацией (Single-Sign-On, SSO) по протоколу Kerberos (см. пункт 2.4.2 настоящего документа).

3) В случае успешного завершения аутентификации Web-сервер создаёт дочерний процесс, в котором будет осуществляться обработка информации в контексте пользователя. Данный процесс обладает тем же набором прав, привилегий и мандатных атрибутов, что и учётная запись пользователя, запросившего доступ. Информация о мандатном контексте получается Web-сервером из IP-пакетов с помощью функций сетевого стека ОС СН. Дальнейшая обработка информации при взаимодействии с

пользователем в рамках установленного соединения осуществляется в контексте дочернего процесса.

4) Если серверу приложений приходит запрос на доступ к объектам ФС или устройствам, то доступ к ним осуществляется на основании переданного контекста дочернего процесса, работающего в контексте пользователя, инициировавшего запрос. Таким образом, ядро системы принимает решение о доступе к запрошенному ресурсу, основываясь на полученной информации о контексте пользователя (такой как GID, UID, мандатный уровень и категория, привилегии) и с учётом действующей доменной политики безопасности.

5) Если серверу приложений приходит запрос на обработку данных, хранящихся в БД, то прикладное ПО, входящее в состав сервера приложений, определяет дальнейшее взаимодействие с защищаемыми ресурсами СУБД PostgreSQL — на программном уровне средствами языка манипулирования данными формулирует запрос, с которым обращается к СУБД. Цикл взаимодействия прикладного ПО и СУБД можно разделить на следующие основные этапы:

а) Обращение прикладного ПО к СУБД инициирует установку защищённого сетевого соединения. ОС добавляет метку безопасности в каждый пакет на уровне IP, соответствующую мандатному контексту дочернего процесса, работающего в контексте пользователя, инициировавшего запрос.

б) Происходит процесс аутентификации и авторизации пользователя, в контексте которого запущен дочерний процесс, с использованием протокола Kerberos (см. пункт 2.4.1, «Идентификация и аутентификация в СУБД PostgreSQL» настоящего документа). Учётные данные пользователя, от которого запущен процесс, пытающийся подключиться к базе данных PostgreSQL, будут направлены на сервер KDC для аутентификации на основе общих закрытых ключей. Те же учётные данные подвергаются проверке между сервером PostgreSQL и KDC на основе файла keytab,

сгенерированного Kerberos. Этот файл ключей должен существовать на сервере базы данных с соответствующими разрешениями для пользователя, владеющего процессом PostgreSQL.

в) Далее осуществляется проверка доступа на основе контекста текущего процесса и разрешённых для данного контекста операций. Осуществляется проверка мандатных прав доступа к объектам БД, одновременно с проверкой дискреционных прав доступа к ним (см. пункт 2.4.1 «Средства дискреционного и мандатного разграничения доступа в СУБД PostgreSQL» настоящего документа).

Данный подход к построению взаимодействия в рамках информационных систем обеспечивает следующие преимущества:

- Наличие в системе единой базы учётных записей пользователей, которая используется всеми компонентами.

- Единую точку входа в информационную систему — локальный вход пользователя на компьютер, работающий под управлением ОС СН. В процессе входа определяется контекст работы пользователя (в том числе — мандатный), под которым он далее будет работать со всеми приложениями в рамках распределенной информационной системы.

- Безопасные механизмы идентификации и аутентификации пользователей в рамках информационной системы.

- Безопасное функционирование прикладной логики сервера приложений (Web-сервера). Т.к. операции выполняются в контексте пользователя, инициировавшего запрос, ошибки в прикладной логике не могут привести к неправомерному доступу пользователя к защищаемой информации — принятие решения о доступе вынесено за пределы алгоритма работы прикладного программного обеспечения.

- Операции идентификации/аутентификации и разграничения доступа выполняются механизмами ОС СН, сертифицированной по требованиям безопасности информации. Это существенно упрощает вопросы сертификации прикладного ПО (в системе сертификации ФСТЭК России

программное обеспечение, не реализующее функции безопасности, обязательной сертификации не подлежит).

3.2.4. Рекомендации по разработке собственного сервера приложений в многопользовательской трехзвенной клиент-серверной архитектуре на базе ОС СН

Если прикладное ПО разрабатывается не на основе Web-технологий и реализуется собственный сервер приложений, обрабатывающий сетевые запросы, для корректного взаимодействия прикладного ПО со встроенными механизмами безопасности ОС СН, в составе сервера приложений необходимо реализовать механизмы, обеспечивающие сохранение контекста работы пользователя до операций обращения к защищаемым ресурсам.

Как правило, при реализации собственного сервера приложений, в качестве клиента выступает также программа собственной разработки («толстый клиент», далее — клиентское приложение).

Далее приведены рекомендации, которые необходимо учитывать при разработке клиента и сервера приложений.

Рекомендации по разработке клиентского приложения.

В клиентском приложении должна быть реализована поддержка возможности последующей идентификации/аутентификации пользователя в сервере приложений.

Для этого необходимо использовать API SASL (Simple Authentication Security Layer - простой уровень аутентификации и безопасности). Краткое описание данного API и примеры его использования приведены в документе «API аутентификации приложений SASL в Astra Linux» (https://nas01.astralinux.ru/sharing/yX3tRc1sF).

В клиентском приложении необходимо реализовать действия, описанные в разделе «Клиентские приложения». Также в документе «API аутентификации приложений SASL в Astra Linux» приведен пример соответствующего программного кода.

Так как клиентское приложение запускается в контексте работы пользователя, вошедшего в систему, при сетевом взаимодействии такого приложения сетевой стек ОС СН обеспечивает автоматическое добавление информации о метке и категории конфиденциальности (из контекста пользователя) в исходящие IP-пакеты.

Рекомендации по разработке сервера приложений

В сервере приложений необходимо реализовать:

1. Идентификацию и аутентификацию пользователя для входящих сетевых запросов. Как уже описано выше в документе, при использовании в информационной системе ЕПП такая идентификация/аутентификация выполняется по протоколу Kerberos. Для реализации этого функционала в сервере приложений необходимо воспользоваться API SASL и реализовать действия, описанные в разделе «Серверные приложения» документа «API аутентификации приложений SASL в Astra Linux». Такая реализация позволит получить в сервере приложений параметры контекста работы пользователя, за исключением его мандатного контекста.

2. Получение мандатного контекста из сетевого сокета, по которому пришел запрос. После этого необходимо запустить обработку запроса пользователя в отдельном процессе и переключить данный процесс-обработчик в контекст работы пользователя (параметры которого получены на данном шаге и на шаге 1). Рекомендации по реализации данных механизмов представлены в документе «Руководящие указания по конструированию прикладного программного обеспечения для операционной системы специального назначения «Astra Linux Special Edition» РУСБ.10015-01», пункт 3.2.2 - «Разработка ПО для обработки информации с различными уровнями конфиденциальности»). Управление метками безопасности в сетевом трафике также описано в документе «Руководство по КСЗ. Часть 1. РУСБ.10015-01 97 01-1», подраздел 4.6 «Сетевое взаимодействие».

После этого процесс-обработчик функционирует в контексте работы пользователя (в том числе мандатном) и КСЗ системы корректно обрабатывает запросы этого процесса к ресурсам системы.

В случае, если из процесса-обработчика необходимо обратиться по сети к другому серверу приложений — то процесс-обработчик начинает выполнять роль клиента для этого (другого) сервера приложений, и в нем необходимо реализовать рекомендации, изложенные в пункте «Рекомендации по разработке клиентского приложения» данного подраздела.

В результате реализации рекомендаций подраздела 3.2.4 алгоритм взаимодействия клиентской и серверной части приложения будут соответствовать схеме, представленной в подразделе 3.2.3 настоящего документа, которая описывает работу Web-сервера (сервера приложений) и Web-браузера (клиентского приложения) из состава ОС СН. Таким образом, сервер приложений будет иметь возможность интеграции с ЕПП с использованием однократной авторизации пользователей и будет функционировать с учётом передачи мандатного контекста, обеспечивая корректную обработку механизмами разграничения доступа ОС СН запросов пользователей на доступ к защищаемым ресурсам.