ПРОГРАММНЫЙ СЕРВИС АДМИНИСТРИРОВАНИЯ РОЛЕВОГО ДОСТУПА И УПРАВЛЕНИЯ ПРИЛОЖЕНИЯМИ

Бордович Т. Д.

Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

Шведова О. А. – маг. техн. наук, старший преподаватель

В работе рассматривается разработка программного сервиса, предназначенного для централизации процессов управления доступом и автоматизации запуска приложений в корпоративной сети. Описана архитектура системы, включающая серверную часть, модуль администрирования и пользовательский лаунчер. Особое внимание уделено реализации ролевой модели доступа (RBAC) и механизмам динамического формирования рабочего окружения пользователя.

Процессы цифровизации современных предприятий приводят к значительному усложнению их ИТ-инфраструктур. Увеличение количества используемого прикладного ПО и расширение штата сотрудников создают проблему «информационного хаоса», повышая риски несанкционированного доступа и снижая общую эффективность администрирования. Целью данного дипломного проекта является разработка программного сервиса, обеспечивающего централизованное управление жизненным циклом доступа к корпоративным приложениям [1].

Разработанная система построена по модульному принципу, что обеспечивает масштабируемость и независимость компонентов. Функциональность сервиса разделена на три ключевых блока:

1 Модуль администратора (Admin Tool): реализован как мощный инструмент управления нормативно-справочной информацией. Он позволяет выстраивать сложную иерархическую структуру организации, регистрировать исполняемые файлы прикладных программ и гибко распределять права доступа. Критически важной особенностью является развитая подсистема аудита: администратор имеет возможность детально просматривать логи всех действий в системе, применяя фильтрацию по времени, типу события или конкретному пользователю. Это гарантирует полную прозрачность процессов управления.

2 Клиентское приложение (Launcher): представляет собой персонализированную графическую оболочку для конечного пользователя. Главная задача модуля — полностью избавить сотрудника от необходимости самостоятельного поиска исполняемых файлов в файловой системе. Управление доступным функционалом осуществляется через интуитивно понятный параметрический интерфейс. После прохождения авторизации лаунчер автоматически запрашивает у сервера список разрешенного для данной роли ПО и формирует его в виде удобного меню. В приложении реализован алгоритм контроля уникальности запущенных процессов, что исключает дублирование рабочих сессий и предотвращает нерациональное использование вычислительных ресурсов рабочей станции.

3 Серверная часть и база данных: сервер выполняет роль связующего звена, обрабатывая входящие запросы от клиентских лаунчеров и административной панели. Для обеспечения надежного хранения структурированных данных о пользователях, их ролях и путях к программным ресурсам используется СУБД PostgreSQL. Взаимодействие между всеми модулями системы организовано по защищенному REST-like протоколу, что позволяет сохранять целостность и конфиденциальность информации при её передаче по локальной или глобальной сети [2].

Теоретическим фундаментом системы выступает ролевая модель управления доступом (RBAC). В отличие от классического избирательного управления, подход RBAC базируется на назначении прав доступа не конкретным персоналиям, а определенным ролям (например, «Бухгалтер» или «Менеджер»). Это коренным образом упрощает и ускоряет процесс администрирования при массовом приеме или увольнении сотрудников [3]. Весь программный комплекс разработан в среде Embarcadero Delphi с применением библиотек VCL и FMX. Это позволило достичь высокой скорости отрисовки интерфейса и обеспечить стабильное взаимодействие с низкоуровневыми системными вызовами операционной системы Windows.

Практическая значимость работы заключается в создании готового к внедрению программного инструмента, который сводит к минимуму влияние человеческого фактора на общую безопасность корпоративной сети и автоматизирует большинство рутинных задач системного администрирования, повышая отказоустойчивость.

Список использованных источников:

1 Таненбаум, Э. Компьютерные сети / Э. Таненбаум, Д. Уэзеролл. – СПб. : Питер, 2021. – 960 с.

2 Борботько, Т. В. Основы информационной безопасности : учеб. пособие / Т. В. Борботько, О. В. Бойправ, А. М. Тимофеев. – Минск : БГУИР, 2025. – 128 с.

3 Щеглов, А. Ю. Модели, методы и средства контроля доступа к ресурсам вычислительных систем : учеб. пособие / А. Ю. Щеглов. – СПб. : Университет ИТМО, 2022. – 95 с.