ЗАЩИТА ЭКСПЛУАТАЦИОННЫХ ДАННЫХ В ИНФОРМАЦИОННО-АНАЛИТИЧЕСКОЙ СИСТЕМЕ «СИРЕНА»

Шутенко О.В., Баклай Д.Н., Сапожников А.С.
Национальный технический университет
"Харьковский политехнический институт",
г. Харьков

В настоящее время в энергетике широкое применение получили информационно-аналитические системы, что осуществляют достоверную, многоаспектную оценку технического состояния оборудования с использованием методов и критериев оценки, которые повышают оперативность и качество организации технического обслуживания оборудования. Однако, как показал анализ литературных источников, разработчики данных систем не уделяют должного внимания резервированию и защите накопленных эксплуатационных данных, при потере которых предприятия теряют дорогостоящую диагностическую информацию, что на наш взгляд является недопустимым. В связи с этим в разрабатываемой на кафедре «Передача электрической энергии» НТУ «ХПІ» ИАС «СИРЕНА» были заложены дополнительные модули, которые расширяют стандартную схему по которой реализуется система.

Для хранения данных в приложении используется свободная реляционная СУБД MySQL, одной из особенностей которой является наличие версий как для ОС Windows, так и для Linux-based операционных систем, что позволяет использовать одну и ту же СУБД как в случае клиент-серверной архитектуры, так и при установки приложения в приделах одной машины.

Защита данных от частичной либо полной потери осуществляется хранением резервной копии БД на внешнем запоминающем устройстве, которым может являться как дополнительный жесткий диск, другой компьютер либо облачный сервис. В случае наличия повышенных требований к надежности системы возможно создание кластера серверов с репликацией данных на уровне базы данных, что позволит продолжать системе нормально функционировать даже в случае выхода из строя одного из компьютеров кластера.

Соединение между клиентом и сервером происходит по протоколу HTTPS с шифрованием передаваемой информации по локальной сети либо через сеть Internet. Для этого могут использоваться как защищенные проводные линии для передачи данных, так и защищенные Wi-Fi, GPRS, 3G.

Управление доступом к данным осуществляется сервером индивидуально для каждого подключения на основании выданных администратором системы правах. Для авторизации у каждого пользователя имеется личный уникальный идентификатор и пароль.