УДК 004.91

ОБЕСПЕЧЕНИЕ СОХРАННОСТИ ДОКУМЕНТОВ В ЭЛЕКТРОННОЙ ФОРМЕ

Магистрант Ермолович П.А.
Канд. физ.-мат. наук, доцент Гурский Н.Н.
Белорусский национальный технический университет

Рассматриваемая проблема одна из основных вопросов, определяющих успешное использование компьютерных технологий в приборостроении - это надежность хранения документов в электронной форме. Решение проблемы сохранности электронных документов складывается из: устойчивого электропитания; резервного копирования; антивирусной защиты; профилактики и диагностики с использованием специальных утилит (вспомогательных программ).

В данной работе рассматривается система управления документами, которая позволяет организовать на внутреннем портале предприятия специальный раздел для коллективной работы над документами. Раздел может включать несколько Библиотек документов для различных рабочих групп и отдельных пользователей. В библиотеках работает мгновенный поиск по файлам и содержимому. Весь раздел или папка с документами Библиотеки подключается как сетевой диск. Если Портал размещен на внешнем хостинге, или у сотрудников есть доступ в Интернет, необходимо обеспечить защиту от большинства известных атак на веб-приложения. Для этого настроен модуль «Проактивная защита», который позволяет повысить уровень защищенности портала благодаря встроенному проактивному фильтру (Web Application Firewall). Проактивная защита – это целый комплекс технических и организационных мер, которые объединены общей концепцией безопасности и позволяют значительно расширить понятие защищенности и реакции веб-приложений на угрозы.

В данной реализации обеспечения сохранности документов в электронной форме стала возможность бесплатно делать «облачный» бэкап. Владельцы такого портала могут сохранять копию своего портала в облачной инфраструктуре и делать это штатными средствами системы. Все данные пользователей, которые хранятся в «облаке», шифруются ключом администратора портала. Используемый ключ нигде не сохраняется, в том числе и на серверах компании предоставляющей облачный сервис. Таким образом даже сотрудники компании-разработчика не имеют доступа к «бэкапам» данных своих клиентов. И это обеспечивает надежную защиту данных от постороннего проникновения.