ПРОЕКТИРОВАНИЕ АППАРАТНОЙ АРХИТЕКТУРЫ РАСПРЕДЕЛЕННЫХ ИНТЕРНЕТ-ПРИЛОЖЕНИЙ С УЧЕТОМ ТРЕБОВАНИЙ К ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

И.О. Сильванович

В текущее время наблюдается бурное развитие массовых интернет-сервисов. Это социальные сети, офисные приложения, онлайн-игры и прочее.

Популярность такого рода сервисов очень высока, следовательно, их программному обеспечению приходится постоянно испытывать большую нагрузку. Поэтому абсолютное большинство таких приложений имеет распределенную архитектуру. Но с ростом количества компьютеров обслуживающих приложение возрастает и уязвимость самого приложения — вероятность потери информации или несанкционированного доступа к данным.

Предлагаемый подход сводится к использованию так называемых уровней защиты, доступ к каждому из которых строго регламентируется. "Первый" уровень — это серверы хранилища данных, включающие в себя всю пользовательскую информацию, как в виде файлов, так и в виде содержимого базы данных. "Второй" уровень включает в себя непосредственно прикладную логику приложения в виде

исполняемых файлов. "Третий" уровень — это программное обеспечение распределяющее пользовательские запросы, то есть прокси-серверы и балансировщики нагрузки. "Четвертый" уровень представляет собой серверы авторизации и управления доступом, хранения и обработки пользовательских сессий. Также на этом уровне может выполнятся шифрование данных. Каждый уровень представляет собой отдельную подсеть, к которой имеют доступ только серверы следующего уровня. Только к последнему уровню есть возможность доступа извне. Физический доступ к серверам первого и второго уровня не должны иметь даже работники датацентров, а только специально акредитованный персонал. Второй и последующие уровни должны быть разделены между собой аппаратными файрволами.

Достоинства такого построения приложения очевидны. Каждый уровень можно обслуживать отдельно, использую разных сотрудников и разные дата-центры. Упрощается масштабирование. Но самое главное — безопасность пользовательских данных, что отражается на репутации и материальном состоянии компании владельца.

Область применения данного подхода — крупные интернет-сервисы, либо распределенные приложения, требующие повышенных мер безопасности.