Д. Е. Оношко, В. В. Бахтизин
(БГУИР, Минск)

ОЦЕНКА НАДЁЖНОСТИ WEB-ПРИЛОЖЕНИЙ МЕТОДОМ СТАТИЧЕСКОГО АНАЛИЗА ИСХОДНОГО КОДА

В настоящее время в области разработки программных средств (ПС) наблюдается тенденция к переходу от классических desktop-приложений к web-приложениям и, как развитие этого направления, облачным вычислениям. Между тем, размещение приложений на общедоступных серверах повышает требования к качеству этих приложений и, в частности, к корректности обработки поступающих от пользователей данных.

Частично задача защиты ПС от некорректных входных данных решается за счёт использования хранимых процедур, подготовленных выражений и т.п. Между тем, эти приёмы являются необходимыми, но не достаточными для обеспечения заданного уровня надёжности функционирования ПС, поскольку лишь упрощают некоторые аспекты обработки данных.

Наиболее уязвимой частью ПС остаётся код, отвечающий за обмен данными с пользователем. Наличие в нём ошибок может быть использовано злоумышленником для выполнения произвольных действий на сервере приложений или компьютерах других пользователей ПС. Единственный способ обнаружения всех подобных ошибок — анализ исходных кодов — является рутинной процедурой, трудоёмкость которой очевидно выше трудоёмкости разработки оцениваемого ПС. Поэтому целесообразно использование автоматизированных средств контроля качества кода, ориентированных на обнаружение типовых уязвимостей.

Количество обнаруживаемых такими ПС проблем безопасности может использоваться в качестве оценки общего уровня надёжности ПС, но более целесообразно применять относительные величины. Для этого предлагается ввести понятие «точка входа данных» и определить его как семантически неделимую единицу данных, поступающих в оцениваемое ПС извне. Примерами таких точек входа могут быть поля ввода имени пользователя, пароля, текстов сообщений и т.д. Предполагается, что статический анализ исходных кодов оцениваемого ПС позволяет не только обнаружить уязвимость, но и определить множество точек входа, которые могут быть использованы злоумышленником для её эксплуатации. Тогда для оценки надёжности ПС может использоваться отношение количества точек входа, через которые не может быть задействована ни одна из обнаруженных уязвимостей, к их общему количеству.

Данный способ оценки надёжности позволяет получать числовые характеристики, не зависящие от размеров оцениваемого ПС, и, следовательно, может применяться для оценки надёжности ПС на всех этапах жизненного цикла начиная с момента появления первого прототипа, а также при сравнении различных ПС по уровню надёжности.