А. В. Зязин, **А. Б. Шишков** (Москва, МИРЭА (ТУ))**. Об использовании модели Take-Grant для проверки соответствия информационных систем нормативным требованиям по обработке персональных данных.**

В настоящее время многие организации, создающие информационные системы (ИС), формулируют самостоятельные представления о необходимой степени обеспечения информационной безопасности. Такие представления могут быть весьма разнообразными. Иногда в политике безопасности организации на первом месте стоят задачи доступности или целостности данных, а угрозы конфиденциальности обрабатываемой информации не считаются актуальными.

Вместе с тем, в 2007 году вступил в действие Закон «О персональных данных» (ФЗ № 152), предъявляющий определенные требования ко всем частным и государственным операторам информационных систем, обрабатывающим персональные данные (ПД), призванный защитить права их субъектов.

Закон устанавливает ряд принципов обработки персональных данных. Часть из них, например, «соответствие целей обработки и достаточность обрабатываемых данных заранее определенным и заявленным оператором» (статья 5), может быть обеспечена обычными организационными мерами. Выполнение в созданной ИС ряда других требований Закона требует учета в формализованном описании и обосновании политики безопасности. К таким требованиям относятся право на изъятие ПД субъекта из ИС по его заявлению, получение субъектом сведений о лицах, которые имеют доступ к его ПД или которым может быть предоставлен такой доступ (статья 14).

В докладе рассматривается возможность применения широко известной модели распространения прав доступа Take-Grant (расширенный вариант, [1]) для формального описания заявляемых оператором целей и способов обработки ПД и обоснования соответствия реализуемой ИС нормативным требованиям. Особенности применения этой модели состоят в следующем: 1) субъект ПД должен быть представлен вершиной-субъектом в графе доступа и наделен определенными правами по отношению к вершинам-объектам, соответствующим его ПД; 2) целью рассмотрения графа доступа является не только поиск возможных информационных потоков в системе, приводящих к «похищению» прав на доступ к данным одного из субъектов ПД, но и проверка постоянного наличия права «удалить» субъектов ПД по отношению к объектам, представляющим их ПД; 3) заранее декларируется, что именно подразумевается под достаточным уровнем обезличенности ПД (например, хранение в отдельных объектах вместо ПД значений хэш-функций, позволяющее при необходимости установить совпадение значений); 4) сокращение числа вершин графа доступа, которые надо учитывать при анализе ИС, происходит путем вывода из рассмотрения вершин-объектов, соответствующих обезличенным данным.

Выбор модели Take-Grant, по мнению авторов, удобен тем, что она достаточно проста для понимания пользователями без специального образования и, в то же время, достаточно точно описывает требования к практической реализации ИС.

СПИСОК ЛИТЕРАТУРЫ

1. *Девянин П. Н.* Модели безопасности компьютерных систем. М.: Академия, 2005.