УДК 621.3.037.37

И.В. Купрейчик, В.П. Степанов

Харьковский национальный экономический университет, Харьков

ЗАЩИТА ИНФОРМАЦИИ В БАЗАХ ДАННЫХ

В современном обществе успех любого вида деятельности все сильней зависит от обладания определенными сведениями и отсутствия их у конкурентов. И чем сильней проявляется указанный эффект, тем больше потенциальные убытки от злоупотреблений в информационной сфере, и тем больше потребность в защите информации.

Среди всего спектра методов защиты данных от нежелательного доступа особое место занимают криптографические методы. В отличие от других методов, они опираются лишь на свойства самой информации и не используют свойства ее материальных носителей, особенности узлов ее обработки, передачи и хранения. Криптографические методы строят барьер между защищаемой информацией и реальным или потенциальным злоумышленником из самой информации.

В настоящее время расширилось использование компьютерных сетей, в частности глобальной сети Интернет, по которым передаются большие объемы информации государственного, военного, коммерческого и частного характера, не допускающего возможность доступа к ней посторонних лиц. С другой стороны, появление новых мощных компьютеров, технологий сетевых и нейронных вычислений сделало возможным дискредитацию криптографических систем еще недавно считавшихся практически не раскрываемыми.

В ходе информационного процесса данные преобразуются из одного вида в другой с помощью методов. Обработка данных включает в себя множество различных операций. По мере развития научно-технического прогресса и общего усложнения связей в человеческом обществе трудозатраты на обработку данных неуклонно возрастают. Прежде всего, это связано с постоянным усложнением условий управления производством и обществом. Второй фактор, также вызывающий общее увеличение объёмов обрабатываемых данных, тоже связан с НТП, а именно с быстрыми темпами появления и внедрения новых носителей данных, средств их хранения и доставки.

Основные операции, которые обычно проводят с данными:

сбор данных – накопление информации с целью обеспечения достаточной полноты для принятия решений;

формализация данных – приведения данных, поступающих из разных источников, к одинаковой форме, чтобы сделать их сопоставимыми между собой, т.е. повысить их уровень доступности;

фильтрация данных – отсеивание лишних данных, в которых нет необходимости для принятия решений; при этом должен уменьшатся уровень «шума», а достоверность и адекватность данных должны возрастать;

сортировка данных – упорядочивание данных по заданному признаку с целью удобства использования; повышает доступность информации;

архивация данных - организация хранения данных в удобной и легкодоступной форме; служит для снижения экономических затрат по хранению данных и повышает общую надёжность информационного процесса в целом;

защита данных – комплекс мер, направленных на предотвращение утраты, воспроизведения и модификации данных;

приём передача данных между удалёнными участниками информационного процесса; при этом источник данных в информатике принято называть сервером, а потребителя – клиентом;

преобразование данных – перевод данных из одной формы в другую или из одной структуры в

другую. Преобразование данных часто связано с изменением типа носителя.

В процессе разработки систем защиты информации выработаны некоторые общие правила:

Простота механизма защиты. Так как средства защиты усложняют и без того сложные программные и аппаратные средства, обеспечивающие обработку данных в ЭВМ, естественно стремление упростить эти дополнительные средства. Чем лучше совпадает представление пользователя о системе защиты с ее фактическими возможностями, тем меньше ошибок возникает в процессе работы.

Разрешения должны преобладать над запретами. Нормальным режимом работы считается отсутствие доступа, а механизм защиты должен быть основан на условиях, при которых доступ разрешается. Допуск дается лишь тем пользователям, которым он необходим.

Проверка полномочий любого обращения к любому объекту информации. Это означает, что защита выносится на общесистемный уровень и предполагает абсолютно надежное определение источника любого обращения.

Разделение полномочий заключается в определении для любой программы и любого пользователя в системе минимального круга полномочий. Это позволяет уменьшить ущерб от сбоев и случайных нарушений и сократить вероятность преднамеренного или ошибочного применения полномочий.

Трудоемкость проникновения в систему. Фактор трудоемкости зависит от количества проб, которые нужно сделать для успешного проникновения. Метод прямого перебора вариантов может дать результат, если для анализа используется сама ЭВМ.

Регистрация проникновений в систему. Иногда считают, что выгоднее регистрировать случаи проникновения, чем строить сложные системы защиты.

Обеспечение защиты информации от несанкционированного доступа – дело сложное, требующее широкого проведения теоретических и экспериментальных исследований по вопросам системного проектирования.

В работе рассмотрены методы и средства защиты информации в базах данных с применением разных приоритетных режимов и систем разграничения доступа, а также различных криптографических методов обработки информации.

Список литературы

1. Барсуков В.С. Безопасность: технологии, средства, услуги / В.С. Барсуков. – М., 2007. – 496 с.

2. Ярочкин В.И. Информационная безопасность: учеб. для вузов / В.И. Ярочкин. – 3-е изд. – М.: Академический проект: Трикста, 2005. – 544 с.