***Аипов Т. Ж., главный специалист АО «Народный банк Казахстана», соискатель КазНТУ им.К. Сатпаева***

## ПРАВОВАЯ РЕГЛАМЕНТАЦИЯ И МЕТОДЫ ЗАЩИТЫ БАЗ ДАННЫХ

Согласно законодательству Республики Казахстан, компьютерным программам предоставляется такая же правовая охрана, как и имущественным и личным неимущественным правам. Так, право на защиту нераскрытой информации от незаконного пользователя предусмотрено ст.ст. 1017-1019 Гражданского кодекса. Уголовная же ответственность наступает в соответствии со ст.184 УК РК. Эффективная правовая защита программного обеспечения и информации предусмотрена и российским законодательством. Такая правовая регламентация пользования базами данных и защиты информации является свидетельством того, что авторы компьютерных программ обладают рядом исключительных авторских прав. Лицо, обладающее информацией на законных основаниях, в том числе производствен-

ными секретами, известными только посвященному ограниченному кругу лиц (нераскрытая информация), имеет право на ее защиту от незаконного использования в том случае, когда информация имеет действительную или потенциальную коммерческую ценность, к ней не имеется свободного доступа на законном основании третьих лиц, обладатель информации принимает меры к охране ее конфиденциальности. Право на защиту нераскрытой информации от незаконного использования возникает независимо от выполнения в отношении нее каких-либо формальностей (регистрации, получения свидетельств и т. п.) и действует до тех пор, пока сохраняются вышеуказанные условия. Высокий государственный уровень изложенных мер характеризует специфику и особую роль компьютерных технологий в жизнеобеспечении всей инфраструктуры общества. Вместе с тем, принимаемые меры правовой защиты базы данных обусловливают и актуальность разработки современных технологий хранения и пользования ими.

В этой связи следует отметить, что способы хранения информации на современном этапе развития компьютерных технологий динамично совершенствуются. Связано это с упрощением ее хранения на вычислительных машинах и несравнимо высокой скоростью доступа к ней. Вместе с этим появились и новые способы хищения информации. Основными факторами, способствующими повышению уязвимости информационных ресурсов, являются:

большие объемы информации, хранимые на ЭВМ;

- хранение информации различного содержания и принадлежности в централизованной базе данных, порой даже в одной базе данных;
- увеличение количества пользователей, имеющих доступ к базе данных;
- внедрение сложных систем статистики и учета времени;

большой поток информации при обмене или переносе данных между различными базами данных.

Выделяют четыре основных способа защиты информации: физические (препятствие), законодательные, управление доступом и криптографическое закрытие. Последний способ является самым надежным и эффективным по следующим причинам.

Криптография как отдельная область информационных технологий претерпела если не кардинальные, то достаточно серьезные изменения, в первую очередь, в функциональных возможностях. Теперь она используется не только для защиты информации, но и для аутентификации пользователей, компьютеров, отдельных блоков информации и работающих в сети приложений.

Сегодня принято учитывать, что криптографические технологии обеспечивают три основных типа услуг для электронной коммерции: аутентификацию (которая включает идентификацию), невозможность отказа от совершенного действия (non—repudiation) и сохранение тайны. Идентификация (подвид аутентификации) проверяет, является ли отправитель послания тем, за кого себя выдает. Аутентификация идет еще дальше — проверяет не только личность отправителя, но и отсутствие изменений в послании. Реализация требования невозможности отказа не позволяет кому бы то ни было отрицать, что он отправил или получил определенный файл или данные. И, наконец, сохранение тайны — это защита посланий от несанкционированного просмотра.

На основании изложенного можно сделать предварительный вывод об актуальности использования криптографии как отдельного метода защиты информации. Безусловно, комплексная защита информационных ресурсов, таких, как базы данных, — это необходимое условие сохранения конфиденциальности критически важной информации практически в любых областях коммерческой деятельности, и можно с уверенностью сказать, что криптография является основной частью этой комплексной защиты.

При выборе состава и структуры предметной области возможны два подхода: функциональный и предметный.

Функциональный подход реализует принцип движения «от задач» и применяется, когда определен комплекс задач, для обслуживания которых создается информационная система. В этом случае можно выделить минимальный необходимый набор объектов предметной области, которые должны быть описаны.

В предметном подходе объекты предметной области определяются с таким расчетом, чтобы их можно было использовать при решении множества разнообразных, заранее не определенных задач.

Необходимое программное обеспечение:

- SQL Server 2008 — это проприетарная (закрытая) система управления базами данных, обеспечивающая сетевой многопользовательский доступ, использует расширенный язык запросов T—SQL. Система отвечает поставленным требованиям и имеет необходимые инструменты для обеспечения требуемой защиты базы данных;

MS Visual Studio 2010 — многофункциональный продукт Microsoft, включающий интегрированную среду разработки программного обеспечения на нескольких языках. Данный продукт имеет в своем составе интерфейс для доступа к данным ADO и несколько языков программирования. В качестве языка программирования, на котором будет реализована логика, функциональности и пользовательский интерфейс, можно использовать язык C#. Еще одним важным преимуществом Visual Studio является встроенный «сборщик мусора» — автоматическое управление памятью — удаление объектов, не используемых программой. И конечно же, большое количество NET—ориентированных систем и факт того, что основное количество пользователей работает с программами MS Windows, играют важную роль в выборе именно этой платформы.

Защита базы данных должна быть комплексной и иметь широкий спектр возможностей SQL Serygr. Это аутентификация, создание представлений, использование хранимых процедур, триггеры, шифрование. Каждый из перечисленных способов обладает своей спецификой и ценностью в общей технологии обеспечения эффективной защиты.

**Түйін**

Мақалада автор ақпараттық базалардың құқықтық қорғауы мен қорғау әдістерін қарастырған№

**Resume**

In the present article the author considers legal aspects of preservation of databases and the most widespread methods of their protection.