4,5 – в качестве пароля используются только первые 8 знаков. Проведя эксперимент, окажется, что, например, для пользователя root, пароли rootroot, rootroot1, rootroot2 и т.д. являются с точки зрения ОС одинаковыми, т.е. одинаково проходными. Так что, если вы набираете 10 знаков при подключении к серверу, то фактически вы набираете только первые 8. Спрашивается, имеет ли смысл защищать СУБД, если защита самого сервера слабее? В ОС Линукс и Solaris 10 ситуация с паролями намного лучше.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. *Joshua Wright, Carlos Cid.* An assessment of the Oracle password hashing algorithm.
2. http://www.red-database-security.com/

УДК 004.414.2

В.А. Михеев

ОСНОВЫ ПОСТРОЕНИЯ ПОДСИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ МНОГОФУНКЦИОНАЛЬНОЙ ИНФОРМАЦИОННОЙ СИТЕМЫ

При проектировании крупной территориально-распределенной многофункциональной информационной системы (МИС) холдинга, одной из основных задач которой является построение единого информационного пространства, необходимо учитывать, что в системе предполагается циркуляция, как общедоступной информации, так и информации ограниченного доступа.

Для обеспечения защиты информации в МИС необходима разработка и внедрение подсистемы защиты информации. Таким образом, разработка основ построения подсистемы защиты информации является актуальной задачей, позволяющей уже на этапе проектирования МИС заложить требуемый уровень защиты.

Подсистема защиты информации является неотъемлемой составной частью МИС и к ней могут предъявляются требования, аналогичные требованиям, предъявляемым к автоматизированным системам в защищенном исполнении. Общие требования по безопасности информации и порядок создания автоматизированных систем в защищенном исполнении определен в национальных стандартах [1,2].

Основные цели защиты информации в МИС должны предусматривать:

- предотвращение утечки информации по техническим каналам (в том числе за счет возможно внедренных в технические средства специальных устройств негласного получения информации);
- предотвращение несанкционированного уничтожения, искажения, копирования, блокирования информации;
- сохранение возможности управления процессом обработки, хранения и использования информации в условиях несанкционированных воздействий на защищаемую информацию.

Подсистема защиты информации должна обеспечивать комплексную защиту информации, передаваемой, накапливаемой и обрабатываемой в МИС, в том числе:

- конфиденциальность информации;
- целостность информации;
- достоверность информации;
- доступность информации;

- обеспечение подконтрольности (регистрации действий и событий в отношении защищаемых ресурсов).

Для достижения указанных целей подсистема защиты информации должна реализовывать следующие основные функции:

- предупреждение о появлении угроз безопасности информации;
- обнаружение, нейтрализацию и локализацию воздействия угроз безопасности информации;
- управление доступом к защищаемой информации;
- восстановление системы защиты информации и защищаемой информации после воздействия угроз;
- регистрацию событий и попыток несанкционированного доступа к защищаемой информации и несанкционированного воздействия на нее;
- обеспечение контроля функционирования средств и системы защиты информации и немедленное реагирование на их выход из строя.

Подсистема защиты информации должна включать в себя комплекс взаимосвязанных организационных мер, технологий, сертифицированных программно-технических средств защиты информации и документированных процедур по обеспечению в МИС необходимого уровня защиты информации в соответствии с утвержденной политикой безопасности.

Основными целями политики безопасности должны являться:

- обеспечение защиты информационных и технических ресурсов (программных и аппаратных средств обработки информации) многофункциональной информационной системы от несанкционированного доступа к информации;
- обеспечение контроля целостности баз данных и их восстановления в случае нарушения целостности;
- поддержание требуемого уровня защищенности подсистемы защиты информации в процессе ее функционирования и развития;
- обеспечение оперативного контроля работы подсистемы защиты информации и мониторинга действий пользователей.

Подсистема защиты информации должна создаваться с учетом возможных угроз безопасности и модели вероятного нарушителя применительно к конкретным условиям функционирования.

Содержание работ по созданию подсистемы защиты информации и их последовательность рассмотрена в [3] и регламентирована рядом документов, руководящих документов и национальных стандартов [1-2,4-5].

Построение подсистемы защиты информации МИС должно основываться на ряде системотехнических принципов [6], к основным из которых необходимо отнести:

- системность и комплексность реализации (необходимость учета всех факторов, влияющих на защищенность объектов подсистемы защиты информации, при ее проектировании, разработке, внедрении, эксплуатации, модернизации и развитии);
- простота и гибкость реализации (используемые меры и средства защиты должны быть понятны и просты в использовании, а существование подсистемы защиты информации не должно существенно затруднять работу пользователей, а также не ухудшать основные функциональные характеристики многофункциональной информационной системы (надежность, быстродействие, возможность изменения конфигурации и т.д.). Предпочтительно использование мер и средств защиты, обеспечивающих широкие

возможности по настройке и совместимости с общесистемным и прикладным программным обеспечением, используемым в МИС);

- разумная достаточность при выборе мер и средств обеспечения информационной безопасности и защиты информации (необходимость выбора той степени защиты, которая оптимизирует соотношение риска, размера возможного ущерба и требуемых затрат);
- непрерывность защиты (необходимо обеспечение информационной безопасности и защиты информации осуществлять на всех этапах жизненного цикла МИС, а развитие подсистемы защиты информации вести параллельно с развитием самой МИС);
- доверие к надежности защиты и равнопрочность защиты (необходимо применять сертифицированные средства защиты, использовать технические, программные и криптографические средства защиты информации и организационные меры, обеспечивающие создание равнопрочного периметра безопасности для всех узлов МИС, а также защищенные доверенные каналы связи между ними);
- минимизация прав пользователей (каждому лицу из числа пользователей МИС, обслуживающего и эксплуатирующего персонала необходимо предоставлять наименьший набор полномочий по доступу к информации и процедурам ее обработки, в то же время эти полномочия должны быть достаточными для успешного выполнения ими своих служебных обязанностей);
- возможность контроля работоспособности и корректности функционирования применяемых механизмов защиты (создание специальных средств и методов, направленных на предотвращение попыток несанкционированного вмешательства в работу механизмов защиты, путем разработки мероприятий по проверке работоспособности и корректности этих механизмов).

Необходимо учитывать, что при проектировании подсистемы защиты информации могут возникнуть дополнительные системотехнические принципы построения, дополняющие принципы, сформулированные в статье.

Таким образом, применение рассмотренных подходов и системотехнических принципов образует основу для построения подсистемы информационной безопасности МИС, отвечающей требуемому уровню защиты.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. ГОСТ Р 51624-2000. «Защита информации. Автоматизированные системы в защищённом исполнении. Общие требования».

2. ГОСТ Р 51583-2000. «Защита информации. Порядок создания автоматизированных систем в защищённом исполнении. Общие положения».

3. *Михеев В.А.* Методология разработки и аттестации автоматизированных систем в защищенном исполнении // Материалы IX Международной научно-практической конференции «Информационная безопасность». – Таганрог: Изд-во ТТИ ЮФУ, 2007.

4. ГОСТ Р 34.601-90. «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания».

5. Руководящий документ «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации», 1992.

6. *Малюк А.А.* Информационная безопасность: концептуальные и методологические основы защиты информации. – М.: Горячая линия – Телеком, 2004.