Защита корпоративных сетей

Печкурова В. А., Сороко Е. Н., студ. II к. БГЭУ,
науч. рук. Акинфина М. А., канд. физ.-мат. наук, доц.

В современных условиях любая деятельность связана с оперированием большими объемами информации, которое производится широким кругом лиц. Защита данных от несанкционированного доступа является одной из приоритетных задач при проектировании любой информационной системы. Следствием возросшего в последнее время значения информации стали высокие требования к конфиденциальности данных. Системы управления базами данных стали доминирующим инструментом в этой области

Для СУБД важны три основных аспекта информационной безопасности: конфиденциальность, целостность и доступность. Темой данной статьи является первый из них — средства защиты от несанкционированного доступа к информации.

Методы защиты баз данных в различных СУБД несколько отличаются друг от друга. Анализ современных СУБД фирм Borland и Microsoft показывает, что они условно делятся на две группы: основные и дополнительные.

К основным средствам защиты относится:

защита паролем. Пароли устанавливаются пользователями или администраторами БД;

шифрование данных и программ — преобразование читаемого текста в нечитаемый текст при помощи некого алгоритма;

разграничение прав доступа к объектам базы данных;

защита полей и записей таблиц БД.

К дополнительным средствам защиты БД можно отнести такие, которые нельзя прямо отнести к средствам защиты, но которые непосредственно влияют на безопасность данных. Их составляют следующие средства:

встроенные средства контроля значений данных в соответствии с типами;

повышение достоверности вводимых данных;

обеспечение целостности связей таблиц;

организация совместного использования объектов БД в сети [1].

Для того, чтобы обеспечить надежную защиту ресурсов корпоративной сети сегодня и в ближайшем будущем, разработчики системы безопасности предприятия должны учитывать следующие основные тенденции:

координированный контроль доступа в нескольких точках (ограничение проникновения трафика во внутренние подсети предприятия, тем самым существенно снижая потенциальные угрозы для ресурсов корпоративной сети);

развитие методов и средств аутентификации. Сегодня в корпоративных сетях широко используются средства аутентификации, основанные на

централизованной службе каталогов, такой как NDS компании Novell или DirectoryServices компании Microsoft;

контроль доступа на основе содержания передаваемой информации. Во многих случаях необходимо контролировать доступ не на основе IP-адресов или каких-либо данных об отправителях/получателях, а в зависимости от содержания передаваемой информации;

защита данных при передаче через публичные сети;

интеграция средств контроля доступа и средств VPN;

обнаружение вторжений;

надежность и отказоустойчивость средств защиты;

централизованное управление средствами безопасности. Оно подразумевает наличие некой единой (возможно, распределенной) базы правил, описывающих согласованную политику безопасности предприятия;

использование открытых стандартов для интеграции средств защиты разных производителей. Переход на открытые стандарты составляет одну из основных тенденций развития средств безопасности. Такие стандарты, как IPSec и PKI обеспечивают защищенность внешних коммуникаций предприятий и совместимость с соответствующими продуктами предприятий-партнеров или удаленных клиентов [2].

Литература

1. Белорусский государственный экономический университет. [Электронный ресурс]/ Лекции на тему «Администрирование баз данных». — Минск, 2013. — Режим доступа: http://www.bseu.by/new/tohod/lekcii9_2.htm. — Дата доступа: 01.04.2013.

2. Citforum. [Электронный ресурс] / Направления развития средств безопасности предприятия. — Минск, 2013. — Режим доступа: http://citforum.ru/security/internet/napravl_razv.shtml. — Дата доступа: 01.04.2013.

Корреляционно-регрессионный анализ в оценочной деятельности и фактический объем выборки для него

Прохорова О. А., магистрант БНТУ,
науч. рук. Трифонов Н. Ю., канд. физ.-мат. наук, доц.

В работах зарубежных и отечественных авторов существует большое количество различных определений оценки рыночной стоимости, и все они сводятся к установлению наиболее вероятной цены, которую независимый осведомленный покупатель готов добровольно заплатить независимому осведомленному продавцу на открытом конкурентном рынке. Таким образом,