

Общедоступные программные средства, предназначенные для специалистов, занимающихся настройкой коммуникационного оборудования и локальных сетей, обеспечивают прослушивание сетевого трафика; даже без специального «хакерского» инструмента можно получить сведения о структуре сети, ее ресурсах, списках зарегистрированных в системе пользователей, их паролях (в некоторых случаях). Наличие этих данных позволяет спланировать и реализовать атаку на АБС. Что же касается рабочих станций, то на них вообще обычный вирус может привести к тому, что работа банка будет парализована на достаточно большое время. При подмене штатного программного обеспечения злоумышленник сможет в лучшем случае исказить результаты работы, в худшем — похитить значительные суммы или получить доступ к банковской информации, ущерб от разглашения которой бывает очень большим.

Требования к защите, обусловленные спецификой автоматизированной обработки информации, определяются совокупностью таких факторов, как характер обрабатываемой информации, ее объем, продолжительность обработки информации в АБС, структура АБС, вид защищаемой информации.

В целях обеспечения безопасности в автоматизированных системах следует применять комплексный подход, при этом должны рассматриваться все составляющие таких систем. Существуют следующие критерии оценки безопасности информационных систем:

конфиденциальность (защита от несанкционированного получения информации);

целостность (защита от несанкционированного изменения информации);

доступность (защита от несанкционированного удержания информации и ресурсов).

Удовлетворяющая данным требованиям АБС включает определенный набор функций защиты (сервис безопасности):

идентификация и аутентификация; управление доступом; подотчетность; аудит; точность информации; обмен данными.

Идентификация и аутентификация обеспечивают проверку подлинности действующих пользователей, регистрацию новых и удаление покинувших систему пользователей, проверку аутентификационной информации, контроль целостности и проверку соблюдения ограничений на число повторных попыток аутентификации.

Средства управления доступом ограничивают доступ к базе данных путем распределения прав доступа пользователей и контроля получения информации косвенным путем.

Функции подотчетности действий пользователей в информационной системе и функции аудита обеспечивают контроль на основе проверки правомерности и корректности совершаемых действий.

Точность информации — необходимое требование к любой информационной системе. Ее специальные функции должны поддерживать согласованность различных частей, точность связей между процессами и неизменяемость данных при передаче.

Обмен данными предполагает, что функции системы должны гарантировать безопасность при взаимодействии с внешней информационной средой по каналам связи. Это предъявляет свои требования к обеспечению аутентификации, управлению доступом, соблюдению конфиденциальности и целостности данных, а также к невозвратности совершенных действий. Можно выделить

следующие основные направления защиты АБС:

разграничение доступа в сеть банка извне и изнутри;

периодический аудит системы защиты АБС (используются средства анализа защищенности, позволяющие заблаговременно обнаружить уязвимые места АБС);

разграничение доступа к информационным ресурсам внутри АБС;

применение средств защиты от НСД на рабочих станциях и серверах;

криптографическая защита важных данных, хранимых в АБС или передаваемых по сети (используются системы шифрования данных, сетевого трафика, средства электронно-цифровой подписи).

Средства криптографической защиты рекомендуются для защиты данных, передаваемых по сети в системах «банк-клиент», в приложениях клиент-сервер и для защиты наиболее критичных информационных ресурсов, хранимых на серверах и рабочих станциях. Обязательным условием их применения является наличие средств защиты от НСД для защиты криптографических ключей от компрометации и криптомодулей от подмены или модификации.

Необходимо использовать методы и технологии, позволяющие закрыть характерные для всех современных систем типа клиент-сервер потенциальные пути НСД:

серверы, на которых расположена СУБД и выполняется серверная часть. Несмотря на то что серверные платформы являются достаточно надежными, сегодня известно много способов вывода серверов из строя. Практически все они могут быть реализованы удаленно, т.е. по сети;

клиентская часть, устанавливаемая на рабочих станциях. Клиентская часть системы может быть подменена на другую, выполняющую дополнительные функции, например компрометацию паролей;

канал взаимодействия между сервером и клиентской частью. Прослушивание трафика может дать злоумышленнику информацию о списках пользователей системы и их паролях, о выполняемых операциях. Перехват трафика и его модификация могут привести к искажению результатов банковских операций.

Чтобы уменьшить риск вмешательства в нормальный процесс функционирования системы, обычно применяются следующие дополнительные средства:

для защиты сервера — средства анализа защищенности для обнаружения уязвимых мест операционных систем и их своевременного устранения, средства обнаружения и реагирования на атаки, проводимые по сети;

для защиты клиентской АРМ — программно-аппаратные средства защиты рабочих станций от НСД, осуществляющие регламентацию действий пользователей и контроль целостности используемого программного обеспечения;

для защиты каналов — средства защиты внутренней сети банка от несанкционированного доступа через общедоступные каналы связи, средства шифрования канала между сервером и клиентской частью.

**А. ЛИТВИНЕНКО, к.э.н.,**  
доцент кафедры

«Информационные технологии»  
Финансовой академии при  
Правительстве Российской Федерации

«Финансовая газета»  
на компакт-диске  
Тел.: (499) 166-03-71, (495) 956-48-18

**Итоги XI Инновационного форума**

10-12 октября 2008 г. в Томске состоялся XI Инновационный форум с международным участием. Основная цель форума — создание площадки для открытого диалога представителей федеральной и региональной власти, международных организаций, бизнеса и финансовых структур по вопросам взаимовыгодного сотрудничества в развитии региональных инновационных систем и инновационной экономики России в целом.

XI Инновационный форум был организован на основе концепции, базирующейся на потенциале инновационного сектора экономики Томской области и Томского научно-образовательного комплекса. Главный упор был сделан на бизнес, его заинтересованность в развитии инновационных проектов и создании необходимых для этого условий.

В форуме приняли участие полторы тысячи человек, представляющих 29 регионов России, 12 иностранных государств, десятки бизнес-структур, 39 вузов страны. Делегаты обсуждали проблемы развития инновационного сектора экономики России в ходе пленарных заседаний и тематических «круглых столов».

В первый день работы Форума состоялось открытие экспозиции 13-й Всероссийской научно-производственной инновационной выставки-ярмарки «Интеграция-2008». На выставке работала Биржа деловых контактов.

Во время проведения Инновационного форума было приурочено проведение сессии Сибирского отделения Российской академии наук в Томске, а также банковской конференции «Устойчивость банковской системы и инвестиции: текущая ситуация, проблемы и перспективы» (при участии Центрального банка Российской Федерации).

**Форум ARIS 2008: повышение эффективности бизнеса**

28 октября в Москве в офисно-гостиничном комплексе Holiday Inn Sokolniki пройдет Форум ARIS 2008, организованный компанией IDS Scheer. Это ставшая уже традиционной ежегодная встреча специалистов в области управления бизнес-процессами и руководителей, отвечающих за эффективность бизнеса.

На форуме будет представлена новая версия платформы ARIS — Business Performance

Edition, объединившая все выпущенные в этом году новые и усовершенствованные продукты семейства ARIS.

В программе форума предусмотрены выступления российских клиентов IDS Scheer. Они поделятся опытом реализации BPM-проектов, которых за 12 лет использования платформы ARIS в России накопилось уже немало в «русском» портфеле IDS Scheer.

В рамках форума состоится также выставка ведущих технологических партнеров IDS Scheer.

Ознакомиться с условиями участия можно на сайте IDS Scheer: [www.ids-scheer.com/ru/processday](http://www.ids-scheer.com/ru/processday) или по тел. +7 (495) 781-77-81.

**Форум SAS в области бизнес-аналитики**

SAS FORUM RUSSIA 2008 пройдет 27 октября 2008 г. в офисно-гостиничном комплексе Holiday Inn Sokolniki. Этот форум проводится третий год подряд, собирая заинтересованную аудиторию — топ-менеджеров (генеральных, финансовых и коммерческих директоров, CIO, руководителей департаментов маркетинга и управления рисками) предприятий финансового, государственного, телекоммуникационного, транспортного, производственного, топливно-энергетического и розничного секторов российской экономики.

Форум проводится под девизом — «Прогнозируй будущее! Оптимизируй бизнес!». Российские и международные эксперты обсудят различные аспекты функционирования российского бизнеса в условиях глобального экономического кризиса.

Участникам и гостям форума будет представлен готовый к выпуску новый релиз программной платформы SAS 9.2. Специалисты SAS Россия/СНГ, клиенты и партнеры компании представят свои доклады по средствам интеграции, бизнес-аналитики, прогнозного моделирования, управления эффективностью, риск-менеджмента.

Организатор форума — компания SAS Россия/СНГ, московское отделение корпорации SAS, одного из лидеров в области разработки программных продуктов бизнес-анализа и управления эффективностью.

Информация о форуме на сайте: [www.sasevents.ru](http://www.sasevents.ru).

Соб. инф.



**ПРАВОВОЙ КОНСАЛТИНГ**

**ПРОФЕССИОНАЛЬНО,  
ОПЕРАТИВНО, УДОБНО!**

**ВЫГОДНЫЕ  
УСЛОВИЯ  
ПОДКЛЮЧЕНИЯ!\***



\* Акция проводится до 31.12.2008 года

- Уникальный информационный банк объемом более 13 тысяч консультаций по наиболее актуальным практическим вопросам
- Право на получение индивидуальных письменных консультаций
- Консультации готовятся высококвалифицированными юристами, налоговыми консультантами, аудиторами и проходят проверку в экспертном центре в Москве

© ООО «НПП «ГАРАНТ-СЕРВИС», 2008.  
Система ГАРАНТ выпускается с 1990 года.  
Компания «Гарант» и ее партнеры являются участниками  
Российской ассоциации правовой информации ГАРАНТ. Реклама.

ООО «НПП «ГАРАНТ-СЕРВИС»  
Тел.: 8 800 200 8888 (бесплатный  
междугородный звонок),  
8 495 647 6238 (для Москвы)  
Интернет: [www.garant.ru](http://www.garant.ru)