Содержание:

Понятие информационной технологии

Информационная технология – процесс, использующий совокупность средств и методов сбора, обработки и передачи информации для получения информации нового качества о состоянии объекта, процесса или явления.

Информационная технология выявляет закономерности процессов обработки информации с целью обеспечения их экономичности, эффективности и актуальности.

В банковских информационных системах объектом информационной технологии является банк или кредитная организация. Процессом служит деятельность банка в рамках банковской системы.

Информационное обеспечение автоматизированных информационных технологий в банке

Проектирование и функционирование АБС основывается на системотехнических принципах, отражающих важнейшие положения методов общей теории систем, системного проектирования, теории информации и других наук, позволяющих обеспечить необходимую надежность эксплуатации, совместимость и взаимодействие информационных систем различных экономических объектов, экономить труд, время, денежные средства на проектирование и внедрение АБС в практику. Информационное обеспечение (ИО) АБС представляет собой информационную модель банка. Различают внемашинное и внутримашинное ИО: внемашинное - это вся совокупность информации в банке, включая системы показателей, методы классификации и кодирования элементов информации, документов, документооборота информационных потоков; внутримашинное - это

представление данных на машинных носителях в виде разнообразных по содержанию, по назначению и специальным образом организованных массивов (файлов), БД и их информационных связей. Современные системы банковских связей складываются и показателей видов банковских услуг и банковской деятельности, которые отражают расчетно-кассовый, кредитный, депозитный, бухгалтерский, нормативный, законодательный, фондовый, инвестиционный и другие аспекты функционирования банка. С помощью аналитических и сводных показателей анализируются структура активов и пассивов, доходов и расходов, денежных потоков по активным и пассивным операциям, ликвидность и финансовая устойчивость банка и т.п. Показатели банковской деятельности характеризуют соотношения депозитов, кредитов, собственных и привлеченных средств, долю межбанковских операций в общем объеме ресурсов и вложений, определяют удельный вес и значимость тех или иных операций, что позволяет выявлять возможность повышения прибыльности и конкурентоспособности банка. Значительную долю внемашинного ИО составляет документация. При разработке внемашинного ИО к документам, как наиболее распространенным носителям исходной и результативной информации, предъявляется ряд требований по их форме, содержанию, порядку заполнения. Единство требований создает унифицированную систему документации. Унифицированные типовые документы в банковской системы повышают эффективность автоматизации. К таким документам относятся платежные поручения, чеки, кассовые ордера, банковские выписки и другие. Унифицированные формы документов вырабатываются для всей территории РФ, утверждаются Министерством финансов РФ и ЦБ. Современные АБС предоставляют получения информации в различных формах: в виде печатных документов, экранных форм, на машинных носителях; она может быть представлена в текстовом, табличном и графическом виде. ПЭВМ располагают набором готовых форм первичной и результативной информации или удобными средствами их формирования и компоновки. Существует прикладной пакет программных средств общего назначения для работы с документами табличного типа или представления информации в табличной форме. АБС разрабатываются с использованием таких программных продуктов, которые имеют разнообразные версии и могут носить встроенный характер. Внутримашинное ИО формирует информационную среду для удовлетворения разнообразных профессиональных потребностей банковской системы. Оно включает все виды специально организованной на машинных носителях информации для восприятия, передачи, обработки техническими средствами. Поэтому информация представляется в виде файлов, БД, банков данных (БнД). Современные банковские технологии работают

только с БД. Существуют различные инструментальные программные средства как для проектирования, так и для управления и поддержания БД - это, прежде всего, СУБД. В зависимости от выполняемых функций их спектр может включать как простые, так и сложные разработки. К внутримашинному ИО банковских систем предъявляется ряд требований. Рассмотрим наиболее важные из них. Система должна предоставлять возможность экспорта (импорта) данных в текстовом и DBF - форматах, что позволяет обмениваться информацией со специальными программами, электронными таблицами и т.д., а экспортируемый из системы документ может быть послан по электронной почте.[3] Внутримашинное ИО банковских систем должно реализовываться в режиме реального масштаба времени, при котором изменение в данных. произведенные одним пользователем, сразу должны становиться доступными остальным пользователям системы. Следует отметить, что действительный режим реального времени обеспечивают только системы, использующие сетевую СУБД, основанную на архитектуре сервера БД («Clarion», «Oracle»…), а при использовании СУБД, основанной на модели «файл - сервер» (Clipper, dBase…) режим реального времени эмитируется. В настоящее время наиболее распространенной СУБД является «Btrieve Tecors Manager» фирмы NOVELL. Программный продукт «Btrieve» является частью ОС Net Ware и позволяет эффективно и надежно использовать ресурсы банковской системы. Среди набора возможностей «Btrieve» отметим основные: реализация модели взаимодействия клиент - сервер, обеспечивающей высокую производительность при многопользовательском доступе к данным; интерфейс с различными языками программирования (C, Pascal, Assembler и другие); управление файлами размером до 4 Гбайт; обработка трансакций, позволяющая выполнять логически связанные изменения в различных файлах; системное журналирование всех изменений в файлах; мониторинг использования системных ресурсов. Альтернативный подход состоит в использовании в качестве основы для построения банковских систем распределенной переносимой реляционной СУБД «Oracle».В ней обеспечиваются надежные методы хранения и обработки данных, защита от сбоев и несанкционированного доступа, эффективная работа в многопользовательской среде и во всех популярных сетях, высокая производительность. Прикладные системы, созданные на базе СУБД «Oracle»,одинаково эффективно функционируют на всех типах ЭВМ: персональных, мини- и больших ЭВМ и лишены недостатков, присущих многим другим СУБД на ПЭВМ. Ввиду полной переносимости прикладных систем сохраняются все вложения в их разработку. Не требуется персонала, а закупка нового оборудования не приводит к полному отказу от старого, ибо последнее может использоваться параллельно с новым. Недостатком СУБД

«Oracle» является достаточно высокая стоимость, поэтому система доступна, как правило, крупным и средним банкам.

Программное обеспечение АБС

Отличительной чертой функционирования АБС является необходимость обработки больших объемов данных в сжатые сроки. При этом основная тяжесть падает на операции ввода, чтения, записи, передачи данных. Это предъявляет весьма жесткие требования к производительности ОС, СУБД и средств передачи данных. Кроме того, значительные объемы информации должны быть доступны в оперативном режиме для обеспечения возможностей анализа, прогнозирования, контроля и прочего. Поэтому базовые средства должны быть в состоянии поддерживать доступ к большим (и постоянно возрастающим) объемам данных без потери производительности. Базовые средства используются для обеспечения эксплуатации АБС, для разработки прикладной части программных средств. Базовыми являются ОС, СУБД и другие программные средства системного назначения. В их окружение, под их действием функционируют прикладные программы. Наличие в спектре базовых средств сетевых функций является непременным атрибутом современных АБС. Сетевые функции придают системе свойства многоуровневости и многозвенности, а также обеспечивают возможность объединения различных программных платформ (MS DOS, NetWare, Windows NT, Unix и другие) и, как следствие, возможность гибкого расширения и наращивания системы - дополнения ее новыми рабочими системами, новыми серверами различных классов. Основным свойством АБС, с точки зрения прикладных потребительских свойств, является достаточная широта функционального набора. Перечень функций, реализуемых банковской системой, можно разделить на две части: обязательные; дополнительные. К первым следует отнести те направления деятельности, которые , как правило, имеют место в любом КБ. Выбор вторых зависит от спеацилизации банка. Прикладные характеристики АБС, кроме функциональных свойств, должны отвечать также требованиям интегрированности, конфигурируемости, открытости и настраиваем ости системы. Конфигурируемость банковской системы означает возможность приобретения различных конфигураций системы (минимальной с последующим расширением путей введения дополнительных модулей). При этом важно учитывать такие характеристики системы, как набор модулей и реализуемых ими функций, степень автономности модулей, наличия межмодульного взаимодействия и формы его реализации (почта между модулями, пересылка управляющих сообщений и

другое), возможные конфигурации системы, ее минимальный состав, независимо функционирующие части, варианты расширения. Интегрированная АБС, объединяющая все банковские процессы, повышает уровень управляемости банка. Такая система адекватно отражает все функциональные и информационные связи, существующие в банке, обеспечивает доступ к данным любого уровня, тем самым предоставляя возможность контролировать работу банка с необходимой степенью детализации. Открытость системы предполагает в ней наличие средств для развития и модификации. Современная методология и инструментальные программные средства даю дают такую возможность. Они получили название CASE средств, позволяют автоматизировать создание и сопровождение ПО. Настраиваемость системы необходима для адаптации к технологии конкретного банка. Необходимость настройки и обычно возникает при установке ЛВС в банке, но может быть и следствием технологических изменений в операциях банка. Тогда настраиваем ость непосредственно граничит с открытостью. Настраиваемость предполагает возможность процедурной настройки системы: регламентацию прав пользователей, конфигурирование рабочих мест, определение набора процедур при открытии и закрытии операционного дня и прочее.

Техническое оснащение современных АБС

Современные банковские системы имеют состав аппаратных средств, в которой входят: средства вычислительной техники (ВТ); оборудование локальных вычислительных сетей (ЛВС); средства телекоммуникации и связи; оборудование, автоматизирующее различные банковские услуги: автоматы-кассиры и т.д. средства, автоматизирующие работу с денежной наличностью (для полсчета и подтверждения подлинности купюр и другие). Важнейшими факторами, влияющими на функциональные возможности и эффективную работу банковских систем, являются состав технических средств, их архитектура и набор базового (системного) ПО, на основе которого строится прикладная часть системы. Использование средств ВТ, в основном, ориентировано на персональные компьютеры, в частности, на IBM совместимые. Широко применяются локальные сети ПЭВМ с центральным ПЭВМ - сервером. Создание информационных систем для крупных банков строится на основе более мощной центральной мини - ЭВМ и относительно дешевых терминалов или ПЭВМ. В качестве центральной ЭВМ могут

использоваться, например, многопроцессорные системы, а также системы на RISC - процессорах. Создание распределенных систем на основе локальных сетей с высокопроизводительными ЭВМ, выполняющими роль серверов и ПЭВМ в качестве рабочих станций - основное современное направление технической базы банковских систем. Автоматизация банковских операций при работе с наличностью предполагает использование детекторов валют и ценных бумаг, счетчиков купюр и монет, упаковщиков банкнот, машины для уничтожения бумаг и документов. Это оборудование при больших объемах операций значительно сокращает трудоемкость работы, экономит время кассиров, операционистов. Защита от фальшивой наличности при значительных оборотах в обменных пунктах и многочисленных филиалах банка обеспечивает достоверность денежных средств и их сохранность С целью повышения производительности и надежности автономных банковских технологий компьютеры объединяются в сети с помощью определенных дополнительных технических и программных средств. В практике банковской деятельности широко распространены ЛВС в пределах одного здания, либо с удаленностью объектов до 1км друг от друга. Для подключения устройств к ЛВС достаточно иметь один канал, соединяющий компоненты сети, кроме того, требуются сетевые адаптеры, которые обеспечивают физическое согласование различных устройств Наиболее распространенные режимы обслуживания пользователей в сети организуются как файл - сервер и клиент - сервер. Обе модели, имея общую схему обслуживания пользователей, различаются сложностью, объемами работ, разнообразием функций, программно-технической оснащенностью, а так же производительностью. Модель клиент - сервер имеет больше ресурсных возможностей, дает ответы на запросы, тогда как первая - передает файлы по сети.

Безопасность АИС в банках

Банки играют огромную роль в экономической жизни общества, их часто называют кровеносной системой экономики. Существуют два аспекта, выделяющих банки из круга остальных коммерческих систем: Информация в банковских системах представляет собой «живые деньги», которые можно получить, передать, истратить, вложить и т.д. Она затрагивает интересы большого количества организаций и отдельных лиц. Поэтому информационная безопасность банка - критически важное условие его существования. Безопасность электронных банковских систем зависит от большого количества факторов, которые необходимо учитывать еще на этапе проектирования этой системы. Основные изменения в

банковской индустрии за последние десятилетия связаны именно с развитием информационных технологий. Компьютеризация банковской деятельности позволила значительно повысить производительность труда сотрудников банка, внедрить новые финансовые продукты и технологии. Современные АБС - это сложные, структурированные, территориально распределенные сети. Как правило, они строятся на основе передовых технологий и программных средств, которые в силу своей универсальности не обладают достаточной защищенностью. Особенно актуальна данная проблема в России. Самым уязвимым для несанкционированных действий звеном информационной системы банка являются автоматические групповые операции, сумма и счета которых обычно не подлежат тщательному контролю. Рассмотрим некоторые из этих операций. Начисление процентов на расчетные счета и счета до востребования. Обычно известна только общая сумма данной групповой операции, причем приблизительно. Незначительные изменения в каждой проводке с последующим сбросом суммы на счет злоумышленника практически не поддаются визуальному контролю. Для предотвращения подобного рода хищений рекомендуется иметь в рамках службы безопасности специализированную службу для параллельного контроля автоматических операций по закрытым для остальных сотрудников методикам. О попытках хищения денежных средств со счетов клиентов с использованием систем «Клиент-Банк» За последние несколько лет в российских банках были выявлены случаи хищения (предотвращенные и свершившиеся) денежных средств с расчетных счетов корпоративных клиентов путем совершения электронных платежей по системе «Клиент-Банк». Анализ выявленных ситуаций показывает, что хищения денежных средств с расчетных счетов осуществляются: . Ответственными сотрудниками корпоративных клиентов, имевшими доступ к секретным ключам ЭЦП организации. Как правило, это уволенные директора, бухгалтеры и их заместители, а также совладельцы организации. . Штатными ИТ-сотрудниками корпоративных клиентов, имевшими технический доступ к носителям (дискеты, флеш-носители, жесткие диски и пр.) с секретными ключами ЭЦП клиентов, а также доступ к компьютерам клиентов, с которых осуществлялась работа по системе «Клиент-Банк». . Нештатными, приходящими по вызову, ИТ-специалистами, обслуживающими компьютеры корпоративного клиента, с которых осуществлялась работа по системе «Клиент-Банк». Как правило, это приходящие ИТ-специалисты, осуществляющие профилактику и подключение к Интернет, установку и обновление бухгалтерских и информационно-правовых программ, установку, обновление и настройку другого ПО. . Злоумышленниками путем заражения через Интернет компьютеров корпоративных клиентов вредоносными

программами. Используя уязвимости системного и прикладного ПО (операционные системы, Web-браузеры, почтовые клиенты и пр.), злоумышленники заражали компьютеры корпоративных клиентов троянскими программами с последующим дистанционным похищением секретных ключей ЭЦП клиента и паролей или дистанционно управляли компьютером клиента. Во всех выявленных случаях злоумышленники тем или иным образом получали доступ к секретным ключам ЭЦП и паролям корпоративного клиента и направляли в банк платежные поручения с корректной ЭЦП клиента. Успешно прошедшие проверку ЭЦП, но при этом подозрительные, абсолютно не свойственные данному клиенту платежные поручения в большинстве случаев пресекались банковскими операционистами на этапе принятия решения об исполнении документов. В то же время часть платежей, направленных злоумышленниками с использованием действующих секретных ключей ЭЦП клиента, не вызывала подозрений у банка. Такие документы имели корректную ЭЦП, вполне обычные реквизиты получателей и типовое назначение платежа. Их исполнение банком приводило к хищению денежных средств с расчетного счета клиента. При этом вся ответственность за убытки безусловно и полностью возлагалась на клиента как единственного владельца секретных ключей ЭЦП. Вся ответственность за конфиденциальность Ваших секретных ключей ЭЦП полностью лежит на Вас, как на единственных владельцах Ваших секретных ключей ЭЦП. Банк информирует Вас, что не осуществляет рассылку электронных писем с просьбой прислать секретный ключ ЭЦП или пароль. Банк не рассылает по электронной почте программы для установки на Ваши компьютеры. Если Вы сомневаетесь в конфиденциальности своих секретных ключей ЭЦП, если есть подозрение об их компрометации (копировании), Вы должны немедленно заблокировать свои ключи ЭЦП позвонив в банк. Для продолжения работы в системе «Клиент-Банк» Вам потребуется сгенерировать и зарегистрировать в Банке новые ключи ЭЦП. Настоящим письмом Банк еще раз информирует Вас о необходимости строгого соблюдения правил информационной безопасности, правил хранения и использования секретных ключей ЭЦП и об ограничении по возможности доступа к персональным компьютерам, с которых осуществляется работа по системе «Клиент-Банк». Действия злоумышленников направлены на: · похищение файла с секретным ключом ЭЦП; · передачу в банк электронных платежных документов, заверенных похищенным ключом ЭЦП. Для обеспечения безопасности Вашей работы с системой «Клиент-Банк» требуется придерживаться приведенных ниже правил и рекомендаций. Чтобы предотвратить хищение секретного ключа ЭЦП, необходимо: . Использовать для хранения файлов с секретными ключами

ЭЦП отчуждаемые носители: дискеты, флеш-носители, CD-диски, специализированные устройства. . Отключать и извлекать носители с ключами ЭЦП в то время, когда они не используются для работы с системой «Клиент-Банк». . По возможности ограничить доступ к компьютерам, используемым для работы с системой «Клиент-Банк» . На компьютерах, используемых для работы с системой «Клиент-Банк», исключить посещение Интернет-сайтов сомнительного содержания, загрузку и установку сомнительного ПО и т. п. . Применять на рабочем месте (в рабочей локальной сети) надежные, по возможности лицензионные средства антивирусной защиты, обеспечить регулярное автоматическое обновления антивирусных баз. . Исключить обслуживание компьютеров, используемых для работы с системой «Клиент-Банк», ненадежными ИТ-сотрудниками. . При обслуживании компьютера ИТ-сотрудниками - обеспечивать контроль за Выполняемыми ими действиями. . Никогда не передавать ключи ЭЦП ИТ-сотрудникам для проверки работы системой «Клиент-Банк», проверки настроек взаимодействия с банком и т.п. При необходимости таких проверок только лично владелец ключа ЭЦП должен сам подключить носитель к компьютеру и лично ввести пароль, исключая его подсматривание. . При увольнении ответственного сотрудника, имевшего доступ к секретному ключу ЭЦП, обязательно заблокировать ключи ЭЦП и сгенерировать новые. . При увольнении ИТ-специалиста, осуществлявшего обслуживание компьютеров, используемых для работы с системой «Клиент-Банк», принять меры для проверки компьютеров на отсутствие вредоносных программ. . Если Вы заметили проявление необычного поведения ПО «Клиент-Банк» или какие-то изменения в интерфейсе программы - позвонить в банк и Выяснить, не связаны ли такие изменения с обновлением версии ПО. Если нет - возможно, изменения Вызваны работой программы-шпиона. Обязательно сразу же заблокировать ключи ЭЦП и сообщить в Банк о ситуации.

Тенденции развития ИБС

Требования функционального и структурного плана к автоматизации банковской деятельности, надёжности и защищённости банковской информации определяют особенности ИБС и неприемлемость ИС, созданных для предприятий при решении всего спектра задач в банковской сфере. Если главная цель функционирования ИС на предприятии - обеспечить руководство предприятия финансовой информацией для принятия обоснованных решений при выборе альтернативных вариантов

использования ограниченных ресурсов, при этом данные о хозяйственной деятельности являются входом в ИС, а полезная информация для лиц, принимающих решения, - выходом из нее, то ИБС предоставляют возможность ведения учета всего набора операций, осуществляемых банком, с приемлемой степенью скорости и надежности, получения всей бухгалтерской и финансовой отчетности, возможность автоматизации реального банковского документооборота, а функциональные подсистемы реализуют банковские услуги, бизнес процессы и любые комплексы задач, отражающие содержательную или предметную направленность банковской деятельности. Уникальность ИБС определяется и особенностями реализации внешних взаимодействий банка. Системы управления деятельностью кредитных организаций сегодня представляют собой самостоятельное направление в сфере информационного бизнеса. Информационные системы для кредитных организаций прошли достаточно долгий путь развития, и в настоящее время можно с уверенностью утверждать, что процесс информатизации банковской деятельности продолжится. Основными тенденциями станут повышение качества и надежности предлагаемых продуктов и услуг, увеличение скорости осуществления расчетных операций, организация электронного доступа клиентов к банковским продуктам. Все это и в дальнейшем будет способствовать активному внедрению в банковскую практику самых последних достижений в области вычислительной техники, сетевых и информационных технологий, методов защиты информации и обработки данных. Рынок программных продуктов для кредитных организаций представлен широким спектром систем, различающихся как в функциональной части, так и в технической реализации. Кроме того, ряд банков (около 50%) разрабатывают собственное программное обеспечение. Качественная эволюция деятельности банков, их возрастающие требования и финансовые возможности будут развивать и направлять подходы к организации программного обеспечения банковских технологий, к выбору той или иной ИБС или фирмы - разработчика программного продукта.

Международная система SWIFT

Сообщество SWIFT (Society for Worldwide Interbank Financial Telecommunication - Сообщество Всемирных Интербанковских Финансовых Телекоммуникаций), созданное в 1973 г., является ведущим международным объединением в сфере

передачи финансовых сообщений. В настоящее время пользователями SWIFT являются более 9000 ведущих банков (включая центральные/национальные банки), финансовых организаций (инвестиционных компаний, брокерских фирм, фондовых бирж, депозитариев) и крупнейших корпораций из 209 стран. Ежедневно по сети SWIFT передается около 15 млн сообщений. Сообщество SWIFT создало высоконадежную сеть передачи финансовой информации, гарантирующую точную и оперативную ее доставку, с документальным подтверждением времени отправления и получения. При этом SWIFT принимает на себя финансовую ответственность за идентичность, безопасность и своевременность доставки финансовых сообщений. На базе SWIFT реализовано более 150 инфраструктурных проектов в 60 странах мира, включая платежные системы большинства государств Евросоюза, Европейскую систему трансграничных платежей TARGET, мировую валютообменную систему CLS, а также инфраструктуры центральных депозитариев (STRATE - Южная Африка и др.). В последние годы пользователями SWIFT стали более 300 ведущих мировых корпораций (Arcelor, General Electric, EADS, Microsoft, ЛУКОЙЛ и др.). Реализованные SWIFT концепция, форматы и правила передачи финансовой информации приобрели статус общепринятого международного стандарта. SWIFT является уполномоченным органом Международной Организации по Стандартизации (ISO) по ведению стандартов ISO 9362 (Банковские идентификационные коды BIC), ISO 13616 (международный код банковского счета IBAN), ISO 15022 (Сообщения рынков ценных бумаг), ISO 20022 (Словарь финансовых терминов) и др. В этой связи опыт SWIFT широко используется для совершенствования стандартов российской финансовой индустрии. В РОССИИ. Одной из основных тенденций развития SWIFT стало повышение удельного веса сообщений, связанных с ценными бумагами в общем трафике SWIFT. Об использовании SWIFT на рынке ценных бумаг можно судить по доле сообщений 5-й категории, которую они составляют в общем трафике сообщений SWIFT за год. В 1992 г. сообщения 5-й категории составляли лишь 3% от общего трафика. К концу 2009 г. эта доля выросла более чем в 14 раз и составила 44% от общего числа сообщений, отправляемых по сети SWIFT. В России SWIFT для передачи сообщений на фондовом рынке используется сравнительно недавно и не столь широко, однако его использование следует тенденции мирового рынка. Несмотря на тот факт, что доля сообщений 5-й категории в общем трафике еще не велика (около 11% по данным на ноябрь 2009 г.), наблюдается довольно быстрый рост их использования. Наиболее активными пользователями сообщений SWIFT по ценным бумагам являются расчетные депозитарии, а также кастодианы. Они используют 5-ю категорию сообщений в первую очередь для выверки и расчетов по ценным бумагам. Также пользователями SWIFT являются крупные инвестиционные

компании, которые используют стандарты SWIFT как для взаимодействия по ценным бумагам, так и для осуществления платежей и расчетов. Согласно Уставу SWIFT в каждой стране, представленной в Сообществе, создаются Национальная группа членов SWIFT и Группа пользователей SWIFT, объединяющие всех пользователей сети. В Российской Федерации организацией, представляющей интересы обеих групп и действующей от их имени, является Российская Национальная Ассоциация SWIFT (РОССВИФТ), которая была создана в мае 1994 г. и представляет собой негосударственную, некоммерческую организацию. В России пользователями SWIFT являются более 500 крупнейших кредитных и финансовых организаций из 67 городов, расположенных в 10 временных зонах. Россия занимает второе место в мире (после США) по количеству пользователей SWIFT. В соответствии со «Стратегией SWIFT до 2010 г.» Россия была внесена в список приоритетных с точки зрения развития стран SWIFT. В этой связи особое значение имеет взаимодействие SWIFT с Банком России в рамках внедрения стандартов и практики сообщества на российском рынке, а также использование инфраструктуры SWIFT при построении системы БЭСП Банка России. Развитие данного процесса определяется Меморандумом о взаимопонимании между Банком России и SWIFT касательно построения в России Системы валовых расчетов в режиме реального времени (RTGS), подписанным в 2004 г. Для осуществления платежей и расчетов в рублях с использованием SWIFT совместно с Банком России подготовлен специальный документ - Рекомендации SWIFT-RUR. Фактически Рекомендации SWIFT-RUR - это набор правил, полностью соответствующих международным стандартам SWIFT и отвечающих требованиям российского законодательства для проведения расчетов в национальной валюте Российской Федерации. Рекомендации позволяют также учитывать особенности организации расчетов в различных кредитных организациях и дают возможность использовать единые технологии для автоматизации обработки финансовых сообщений при операциях как в российских рублях, так и в иностранных валютах. Процессу расширения использования SWIFT на Российском фондовом рынке способствует деятельность Рабочей группы РОССВИФТ по выработке рекомендаций по использованию стандартов SWIFT для передачи сообщений 5-й категории при взаимодействии российских пользователей. В целях унификации использования сообщений SWIFT при взаимодействии участников российского рынка ценных бумаг Рабочей группой РОССВИФТ по анализу практики фондового рынка были созданы и утверждены рекомендации SWIFT-RUS. Данный документ содержит набор правил и примеров, учитывающих специфику российского рынка и требования регулятора. Рекомендации SWIFT-RUS охватывают расчеты по ценным бумагам и активно используются депозитариями и кастодианами. В настоящее время готовятся

рекомендации по использованию сообщений SWIFT о корпоративных действиях. Рабочая группа РОССВИФТ является частью структуры SMPG (Securities Market Practice Group), инициативы SWIFT по гармонизации практики фондовых рынков разных стран. Одной из отличительных особенностей российского фондового рынка является большое количество профессиональных участников. Такая ситуация, с одной стороны, представляет собой большой потенциал для развития SWIFT, с другой - накладывает дополнительные требования, в первую очередь с точки зрения стоимости услуг для указанного сегмента пользователей. Новшеством в данном направлении стало внедрение такого способа подключения к SWIFT, как Alliance Lite, предназначенного специально для средних и мелких участников финансового рынка. .2 Безопасность АИС в банках Банки играют огромную роль в экономической жизни общества, их часто называют кровеносной системой экономики. Существуют два аспекта, выделяющих банки из круга остальных коммерческих систем: Информация в банковских системах представляет собой «живые деньги», которые можно получить, передать, истратить, вложить и т.д. Она затрагивает интересы большого количества организаций и отдельных лиц. Поэтому информационная безопасность банка - критически важное условие его существования. Безопасность электронных банковских систем зависит от большого количества факторов, которые необходимо учитывать еще на этапе проектирования этой системы. Основные изменения в банковской индустрии за последние десятилетия связаны именно с развитием информационных технологий. Компьютеризация банковской деятельности позволила значительно повысить производительность труда сотрудников банка, внедрить новые финансовые продукты и технологии. Современные АБС - это сложные, структурированные, территориально распределенные сети. Как правило, они строятся на основе передовых технологий и программных средств, которые в силу своей универсальности не обладают достаточной защищенностью. Особенно актуальна данная проблема в России. Самым уязвимым для несанкционированных действий звеном информационной системы банка являются автоматические групповые операции, сумма и счета которых обычно не подлежат тщательному контролю. Рассмотрим некоторые из этих операций. Начисление процентов на расчетные счета и счета до востребования. Обычно известна только общая сумма данной групповой операции, причем приблизительно. Незначительные изменения в каждой проводке с последующим сбросом суммы на счет злоумышленника практически не поддаются визуальному контролю. Для предотвращения подобного рода хищений рекомендуется иметь в рамках службы безопасности специализированную службу для параллельного контроля автоматических операций по закрытым для остальных сотрудников методикам. О попытках

хищения денежных средств со счетов клиентов с использованием систем «Клиент-Банк» За последние несколько лет в российских банках были выявлены случаи хищения (предотвращенные и свершившиеся) денежных средств с расчетных счетов корпоративных клиентов путем совершения электронных платежей по системе «Клиент-Банк». Анализ выявленных ситуаций показывает, что хищения денежных средств с расчетных счетов осуществляются: . Ответственными сотрудниками корпоративных клиентов, имевшими доступ к секретным ключам ЭЦП организации. Как правило, это уволенные директора, бухгалтеры и их заместители, а также совладельцы организации. . Штатными ИТ-сотрудниками корпоративных клиентов, имевшими технический доступ к носителям (дискеты, флеш-носители, жесткие диски и пр.) с секретными ключами ЭЦП клиентов, а также доступ к компьютерам клиентов, с которых осуществлялась работа по системе «Клиент-Банк». . Нештатными, приходящими по вызову, ИТ-специалистами, обслуживающими компьютеры корпоративного клиента, с которых осуществлялась работа по системе «Клиент-Банк». Как правило, это приходящие ИТ-специалисты, осуществляющие профилактику и подключение к Интернет, установку и обновление бухгалтерских и информационно-правовых программ, установку, обновление и настройку другого ПО. . Злоумышленниками путем заражения через Интернет компьютеров корпоративных клиентов вредоносными программами. Используя уязвимости системного и прикладного ПО (операционные системы, Web-браузеры, почтовые клиенты и пр.), злоумышленники заражали компьютеры корпоративных клиентов троянскими программами с последующим дистанционным похищением секретных ключей ЭЦП клиента и паролей или дистанционно управляли компьютером клиента. Во всех выявленных случаях злоумышленники тем или иным образом получали доступ к секретным ключам ЭЦП и паролям корпоративного клиента и направляли в банк платежные поручения с корректной ЭЦП клиента. Успешно прошедшие проверку ЭЦП, но при этом подозрительные, абсолютно не свойственные данному клиенту платежные поручения в большинстве случаев пресекались банковскими операционистами на этапе принятия решения об исполнении документов. В то же время часть платежей, направленных злоумышленниками с использованием действующих секретных ключей ЭЦП клиента, не вызывала подозрений у банка. Такие документы имели корректную ЭЦП, вполне обычные реквизиты получателей и типовое назначение платежа. Их исполнение банком приводило к хищению денежных средств с расчетного счета клиента. При этом вся ответственность за убытки безусловно и полностью возлагалась на клиента как единственного владельца секретных ключей ЭЦП. Вся ответственность за конфиденциальность Ваших секретных ключей ЭЦП полностью лежит на Вас, как на единственных

владельцах Ваших секретных ключей ЭЦП. Банк информирует Вас, что не осуществляет рассылку электронных писем с просьбой прислать секретный ключ ЭЦП или пароль. Банк не рассылает по электронной почте программы для установки на Ваши компьютеры. Если Вы сомневаетесь в конфиденциальности своих секретных ключей ЭЦП, если есть подозрение об их компрометации (копировании), Вы должны немедленно заблокировать свои ключи ЭЦП позвонив в банк. Для продолжения работы в системе «Клиент-Банк» Вам потребуется сгенерировать и зарегистрировать в Банке новые ключи ЭЦП. Настоящим письмом Банк еще раз информирует Вас о необходимости строгого соблюдения правил информационной безопасности, правил хранения и использования секретных ключей ЭЦП и об ограничении по возможности доступа к персональным компьютерам, с которых осуществляется работа по системе «Клиент-Банк». Действия злоумышленников направлены на: · похищение файла с секретным ключом ЭЦП; · передачу в банк электронных платежных документов, заверенных похищенным ключом ЭЦП. Для обеспечения безопасности Вашей работы с системой «Клиент-Банк» требуется придерживаться приведенных ниже правил и рекомендаций. Чтобы предотвратить хищение секретного ключа ЭЦП, необходимо: . Использовать для хранения файлов с секретными ключами ЭЦП отчуждаемые носители: дискеты, флеш-носители, CD-диски, специализированные устройства. . Отключать и извлекать носители с ключами ЭЦП в то время, когда они не используются для работы с системой «Клиент-Банк». . По возможности ограничить доступ к компьютерам, используемым для работы с системой «Клиент-Банк» . На компьютерах, используемых для работы с системой «Клиент-Банк», исключить посещение Интернет-сайтов сомнительного содержания, загрузку и установку сомнительного ПО и т. п. . Применять на рабочем месте (в рабочей локальной сети) надежные, по возможности лицензионные средства антивирусной защиты, обеспечить регулярное автоматическое обновления антивирусных баз. . Исключить обслуживание компьютеров, используемых для работы с системой «Клиент-Банк», ненадежными ИТ-сотрудниками. . При обслуживании компьютера ИТ-сотрудниками - обеспечивать контроль за Выполняемыми ими действиями. . Никогда не передавать ключи ЭЦП ИТ-сотрудникам для проверки работы системой «Клиент-Банк», проверки настроек взаимодействия с банком и т.п. При необходимости таких проверок только лично владелец ключа ЭЦП должен сам подключить носитель к компьютеру и лично ввести пароль, исключая его подсматривание. . При увольнении ответственного сотрудника, имевшего доступ к секретному ключу ЭЦП, обязательно заблокировать ключи ЭЦП и сгенерировать новые. . При увольнении ИТ-специалиста, осуществлявшего обслуживание компьютеров,

используемых для работы с системой «Клиент-Банк», принять меры для проверки компьютеров на отсутствие вредоносных программ. . Если Вы заметили проявление необычного поведения ПО «Клиент-Банк» или какие-то изменения в интерфейсе программы - позвонить в банк и Выяснить, не связаны ли такие изменения с обновлением версии ПО. Если нет - возможно, изменения Вызваны работой программы-шпиона. Обязательно сразу же заблокировать ключи ЭЦП и сообщить в Банк о ситуации.