М.Ю. Романов Б.И. Скородумов

БЕЗОПАСНОСТЬ ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ БАНКОВСКИХ РАСЧЕТОВ

Москва 1998

МИНИСТЕРСТВО ОБЩЕГО И ПРОФЕССИОНАЛЬНОГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

МОСКОВСКИЙ ГОСУДАРСТВЕННЫЙ ИНЖЕНЕРНО-ФИЗИЧЕСКИЙ
ИНСТИТУТ (ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ)

М.Ю. Романов Б.И. Скородумов

БЕЗОПАСНОСТЬ ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ БАНКОВСКИХ РАСЧЕТОВ

Москва 1998

Р69
УДК 004.056.5
ББК 32.973-018.2

Романов М.Ю., Скородумов Б.И. **Безопасность информации в автоматизированных системах банковских расчетов:** *Учебное пособие.* М.: МИФИ, 1998. — 156 с.

Пособие посвящено вопросам информационной безопасности в автоматизированных системах банковских расчетов, а также вопросам развития банковской системы России на современном этапе. Описываются основные проблемы организации электронного документооборота и автоматизированных систем банковских расчетов (АСБР). Подробно рассматриваются вопросы и проблемы защиты информации в АСБР, а также методы их решения на примере применения сертифицированного средства криптографической защиты информации "Янтарь АСБР".

Пособие предназначено для студентов старших курсов МИФИ, изучающих основы организации защиты информации банковского документооборота и автоматизированных систем банковских расчетов, а также для слушателей курсов повышения квалификации сотрудников Центрального банка Российской Федерации (Банка России) по специальности "Телекоммуникационные системы и средства их защиты".

ISBN 5-7262-0181-7

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Банковские автоматизированные системы обработки и передачи данных стремительно развиваются. Калифорнийская фирма INPUT составила прогноз развития банковской отрасли на ближайшие пять лет. По ее оценкам, к 2001 г. число банков, предлагающих банковское обслуживание на дому, возрастет втрое, количество бумажных документов уменьшится на 60%. К 2001 г. банки и другие организации, предоставляющие финансовые услуги, затратят свыше 50 млрд. долл. на разработку, внедрение и функционирование новых электронных банковских услуг для индивидуальных клиентов, а более 90% всех контактов с банком будет происходить электронным образом. Основной побудительной силой развития этих услуг станет уменьшение стоимости банковских транзакций за счет использования передовых информационных технологий. Одна транзакция будет обходиться на две трети дешевле по сравнению с сегодняшним уровнем [1].

Освоение и использование современных информационных и телекоммуникационных технологий является необходимым этапом становления банковского дела в России [2].

Ситуация, сложившаяся во многих крупных банках России, характеризуется следующими обстоятельствами:

- увеличением количества банковских услуг, предоставляемых клиентам, и количества счетов, открываемых в банке. Следствием чего является лавинообразный процесс роста объема информации, обрабатываемой его различными подразделениями;
- устойчивой тенденцией снижения доходности всех финансовых инструментов. Следствием чего является повышение интереса многих финансовых структур к передовым информационным технологиям и аналитическим инструментам, позволяющим отслеживать и повышать эффективность работы всех банковских продуктов.

Появление новых субъектов хозяйственной и экономической деятельности, рост числа коммерческих банков и их филиалов, возрастание информационной нагрузки на банковские системы, необходимость интеграции с международной банков-

ской структурой — вот характерные черты современного этапа в нашей стране.

Все эти факторы определяют актуальность задачи комплексной автоматизации банковской деятельности в России на основе современных информационных технологий и средств телекоммуникаций.

Создание телекоммуникационной банковской инфраструктуры требует всесторонне проработанной концептуальной модели единой информационно-телекоммуникационной банковской сети ЦБ РФ (ЕТКБС).

Единое телекоммуникационное пространство в первую очередь необходимо для достижения высокой надежности современной системы платежей и автоматизации всех видов деятельности ЦБ РФ, а также для поддержки функционирования прикладных систем ускорения обработки и сокращения сроков прохождения банковских электронных документов по всей территории Российской Федерации с обеспечением высоконадежного механизма передачи платежей как внутри регионов, так и между ними. При этом необходимо добиться непрерывного круглосуточного функционирования системы во всех регионах страны.

Центробанк сможет взять на себя полную ответственность с предоставлением гарантий по производимым электронным платежам в случае безусловного выполнения в ЕТКБС всей совокупности организационных и технологических процессов с техническим обслуживанием и сопровождением, включая управление безопасностью при обработке и передаче данных. Последнее весьма важно в современных российских условиях. Так, на семинаре "Практические вопросы информационно-аналитической работы в коммерческом банке", который состоялся 28-30 октября 1997 г. в Москве, был сделан доклад "О проблемах безопасности в кредитно-финансовой сфере". В.И.Сергеев, заместитель начальника Управления ЭК ФСБ России сообщил, что в нашей стране «криминализация системы кредитно-финансовых отношений стимулирует так называемую "беловоротничковую" преступность — совершение банковскими служащими и руководителями банковских учреждений, оказавшихся в сложном положении, противозаконных финансовых действий. Набирает силу "электронная" преступность, "взламывание" систем защиты банковской информации, махинации

с пластиковыми платежными средствами. Так, подразделениями экономической контрразведки получены данные о попытках проникновения в электронную сеть системы межбанковских расчетов Национального банка Республики Башкортостан с целью проводки фальшивых платежей».

В последние годы произошли существенные изменения в технологии обработки информации. Эти изменения связаны с объединением автономных территориально распределенных процессов и систем обработки информации в единую структуру с использованием средств связи или в информационно-телекоммуникационную систему. Вместе с тем по данным, опубликованным в статье "Электронная отмычка" ("Независимая газета" от 26.09.95) в последние годы все большее распространение в России получает новый вид интеллектуальных преступлений — хищение денег и информации с использованием электронных средств доступа (компьютеры, кредитные карточки и т.п.). В США этот вид преступной деятельности по доходности занимает 3-е место после торговли оружием и наркотиками. В нашей стране этот промысел, несмотря на свою молодость, также прогрессирует довольно быстро.

Особенно остро эта проблема встала в начале 90-х гг., когда отечественные банки и финансовые структуры начали переходить на расчеты с использованием компьютерных сетей. Между тем межбанковские расчеты в то время оказались совершенно незащищенными. К этому же времени относятся и первые попытки совершения преступлений в этой области. Так, в 1991 г. в системе Внешэкономбанка была разоблачена преступная группа, один из участников которой, изменив компьютерную программу обработки валютных счетов клиентов, увеличил остаток по ним более чем на 225 тыс. долл. До задержания преступники успели перевести на подставных лиц и похитить 125 тыс. долл.

О масштабах хищений с использованием электронных средств доступа можно судить потому, что только в 1993—1994 гг. было совершено более 300 попыток проникновения в компьютерные сети Центрального банка России. К наиболее крупной из них МВД относит "взлом" в 1993 г. компьютерной системы ГРКЦ ГУ РФ по г. Москве. Тогда злоумышленники попытались похитить около 70 млрд. руб. путем перечисления их "электронной почтой" на корреспондентские

счета восьми коммерческих банков. В 1995 г. в России было выявлено 185 хищений, совершенных с использованием электронных средств доступа, ущерб от которых составил 250 млрд. руб. При этом следует помнить, что, по утверждению специалистов, ревизия в состоянии выявить не более 10% хищений.

Необходимо отметить, что финансовые потери определяются не только преступными воздействиями. Статистика финансовых потерь в банках Великобритании констатирует, что треть убытков обусловлена случайными причинами, например, авариями банковских автоматизированных систем обработки данных, которые произошли из-за халатности персонала или стихийных бедствий [27].

Поэтому в данной работе предпринята попытка закрыть отдельные пробелы в вопросах комплексного обеспечения безопасности информации в отечественных автоматизированных системах банковских расчетов, ознакомить потенциальных пользователей новых технических средств с основами технологии защиты информации и помочь им ориентироваться в эффективности необходимых средств защиты. С этой целью рассматриваются требования по защищенности автоматизированных систем банковских расчетов (АСБР) и практическое обеспечение безопасности информации в этих системах. Дается краткое описание функций АСБР и их место в автоматизированных банковских системах. На базе анализа, систематизации и обобщения зарубежного и отечественного опыта рассмотрены методы и средства обеспечения безопасности информации в автоматизированных банковских системах, особенности аппаратной и программной реализации возможных механизмов защиты (в том числе с использованием современных криптографических систем), организационно-технические документы и меры защиты. В работе нашли отражение актуальные вопросы обеспечения безопасности информации сетей и вычислительных систем. При этом использовался практический опыт авторов в области защиты информации.

Учитывая упомянутые главные задачи, специфику и ограниченный объем работы, авторам пришлось бегло изложить описание функционирования АСБР и ряд проблем информационной безопасности, которые подробно рассмотрены в доступной литературе. Основное внимание сосредоточено на структуре

комплексного изложения материала и малоизвестных сведениях, которые важны для раскрытия данной темы.

Представленный материал излагается в той последовательности, которой следует придерживаться при обеспечении информационной безопасности электронных систем. Первоначально изучаются угрозы для информационных ресурсов системы, затем ставятся основные задачи обеспечения безопасности информации, которые базируются на изучении объекта защиты. Особое внимание уделяется комплексности выявления, предупреждения, ранжирования, компенсации или устранения различных угроз информационных ресурсов АСБР.

Прежде, чем углубится в решение обозначенной проблемы, целесообразно кратко рассмотреть предметную область автоматизации банковской системы, что, очевидно, повышает эффективность реализации поставленных задач.

1. ОБЩЕЕ СОСТОЯНИЕ И ПЕРСПЕКТИВЫ РАЗВИТИЯ БАНКОВСКОЙ СИСТЕМЫ РОССИИ

Банковская система России представляет собой иерархическую территориально-распределенную структуру. Ядром ее является Центральный банк РФ, который имеет трехуровневую иерархию:

- ♦ центральный аппарат ЦБ РФ, межрегиональный и региональные центры информатизации, главные управления и национальные банки;
- ♦ главные расчетно-кассовые центры (ГРКЦ) и расчетно-кассовые центры (РКЦ) национальных банков республик и главных управлений ЦБ РФ;
- ♦ коммерческие банки и их филиалы.

При создании ЕТКБС учитывается существующая структура банковской системы с исторически сложившимся административно-территориальным делением. В структуре создаваемой сети находят отражение иерархия организационных взаимосвязей и принятые процедурные правила функционирования учреждений в условиях соподчинения, а также привносятся новые элементы автоматизации подготовки документов, их учета и оборота и передачи банковских платежей в электронной форме.

По данным на начало 1997 г., на территории России функционировало 1500 расчетно-кассовых центров и других учреждений Банка России, осуществляющих расчетное обслуживание 2530 кредитных организаций, 6116 их филиалов, а также счетов бюджетов всех уровней и государственных внебюджетных фондов, органов федерального казначейства и других юридических лиц в случаях, предусмотренных законодательством [2]. Банком России издан "Справочник банковских идентификационных кодов участников расчетов на территории Российской Федерации" (Справочник БИК РФ), который содержит информацию о наименовании кредитной организации-участнике расчетов, ее банковском идентификационном коде, корреспондентском счете в Банке России, местонахождении и др. Справочник БИК РФ периодически корректируется.

Кредитные организации, расположенные на территории Российской Федерации (резиденты), имеющие лицензию Центрального банка Российской Федерации на совершение банковских операций, открывают только один корреспондентский счет в одном из учреждений Банка России (расчетно-кассовом центре или операционном управлении), которое осуществляет их обслуживание. Филиалы кредитных организаций имеют корреспондентские субсчета, но некоторые филиалы осуществляют расчеты только через корреспондентский счет головного банка.

Платежная система как совокупность организационных форм, инструментов и процедур, способствующих обращению денежных средств, имеет большое значение для осуществления Банком России эффективной денежно-кредитной политики. Порядок, формы и правила расчетов в Российской Федерации являются обязательными для всех субъектов хозяйствования, предприятий, организаций и населения. Формы безналичных расчетов определены Гражданским кодексом Российской Федерации [33].

Основными формами безналичных расчетов являются платежные поручения, в меньшей степени применяются платежные требования (по инкассо), аккредитивы и чеки используются незначительно. Постоянно растущее число операций по расчетам юридических и физических лиц производится автоматизированными системами банковских расчетов (АСБР), обеспечению безопасности информации которых посвящена данная работа.

Часть расчетов юридических и физических лиц осуществляется посредством систем электронных платежей с пластиковыми картами, их применение получает все большее развитие. Коммерческие банки выпускают собственные платежные карты, карты российских систем (STB Card, Union Card, Золотая Корона), а также международные платежные карты, в частности VISA, Eurocard/MasterCard, Diners Club, JCB и American Express [4].

Большая часть платежей осуществляется через расчетную сеть Банка России, который проводит политику обеспечения бесперебойности функционирования системы расчетов, ее быстродействия и надежности.

Для осуществления безналичных расчетов юридическим и физическим лицам открываются счета в коммерческих банках,

в особых случаях счета юридическим лицам также могут быть открыты в учреждениях Банка России. Взаиморасчеты клиентов учреждений банков, их расчеты с бюджетом и внебюджетными фондами производятся через корреспондентские счета. Что касается расчетов между клиентами одного банка, то они проводятся списанием или зачислением средств на соответствующие счета клиентов, минуя корреспондентский счет банка.

Расчеты между одногородними банками, или банками, обслуживаемыми одним вычислительным центром, часто организуются через счет взаимных расчетов. Вся информация по расчетно-денежным документам, обработанная в установленном порядке в коммерческом банке, вводится в ЭВМ. На корреспондентском счете банка в расчетно-кассовом центре отражается только сальдо проведенных операций. Такие расчеты называются локальным клирингом.

Расчеты между расчетно-кассовыми центрами по операциям кредитных организаций, а также по их собственным операциям осуществляются через счета межфилиальных оборотов (МФО). Средством межфилиальных расчетов являются авизо по МФО.

Правильность совершения расчетов со стороны расчетно-кассовых центров подтверждается совпадением начальных и ответных оборотов в процессе квитовки, т.е. сопоставления каждого ответного провода с начальным. Платежи осуществляются при наличии и в пределах средств на корреспондентских счетах. Не исключена ситуация, когда у банка не достает средств, в этом случае порядок списания средств с корреспондентских счетов банков по платежам клиентов, располагающих необходимыми ресурсами, а также по собственным платежам банков производится в очередности, установленной Гражданским кодексом Российской Федерации. Неоплаченные расчетные документы при этом помещаются в картотеку к корреспондентскому счету кредитной организации.

Платежи осуществляются почтовым и телеграфным способом (бумажная технология) и электронным способом (безбумажная технология). Доля электронных платежей в течение последних лет постоянно увеличивалась по количеству и сумме проведенных документов за счет снижения доли почтовых и телеграфных платежей.

Общий срок безналичных расчетов установлен Федеральным законом "О Центральном банке Российской Федерации

(Банке России)" [3] и не должен превышать двух операционных дней в пределах субъекта Российской Федерации и пяти операционных дней в пределах Российской Федерации.

Межбанковские расчеты в России проводятся в соответствии с платежной системой ЦБ РФ, базирующейся на осуществлении платежей через корреспондентские счета коммерческих банков, открытые в расчетно-кассовых центрах ЦБ РФ. В каждом регионе существуют главный и районные РКЦ, являющиеся самостоятельными расчетными единицами. Каждый РКЦ ведет корреспондентские счета коммерческих банков и счета своих клиентов, организует их взаимные расчеты, а также расчеты через другие РКЦ и ГРКЦ.

Сеть связи ЕТКБС имеет иерархическую структуру, региональный фрагмент которой представлен на рис.1.

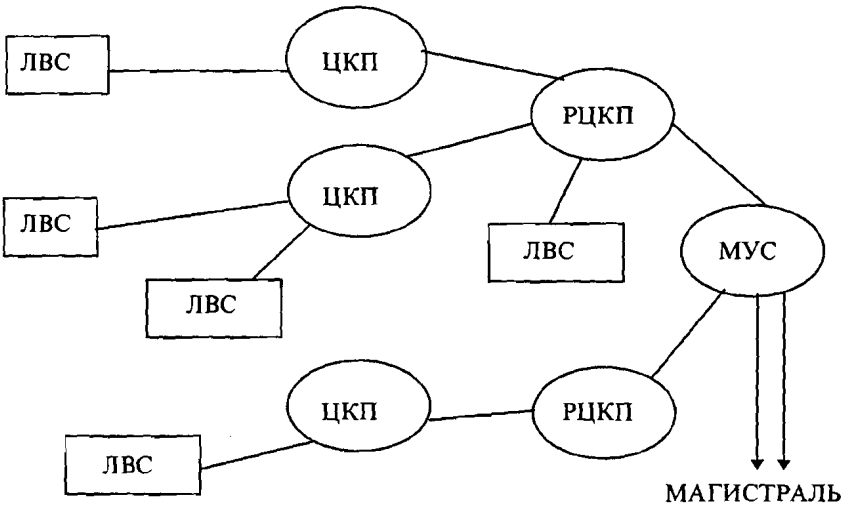

Рис.1. Структурная схема регионального фрагмента ЕТКБС:
ЛВС — локальные вычислительные сети абонентов сети; ЦКП — центры коммутации в районах; РЦКП — региональный узел сети, ЦКП; МУС — магистральный узел сети, включающий ЦКП и систему Tandem, для межрегиональной взаимосвязи

Информационное объединение структурных учреждений ЦБ РФ и ускорение межбанковских расчетов при одновременном повышении их надежности и безопасности основываются на современных информационных технологиях, средствах защиты

и телекоммуникационном оборудовании с разделением задач обработки и транспортировки (передачи) информации, обеспечивающем независимость и гармоничность их развития.

Высокая надежность и эффективность системы платежей достижима лишь на базе самых современных технологий, обладающих высокой степенью эффективности и отказоустойчивости.

1.1. ТЕЛЕКОММУНИКАЦИОННАЯ СРЕДА

Для достижения взаимосвязи прикладных банковских и финансовых систем различных регионов ЕТКБС используются универсальные средства организации интерфейса между системами обработки и обмена банковской информацией по электронной почте в форматах, унифицированных в соответствии с рекомендациями международных стандартов ISO и МККТТ (X.400, X.435), а также справочной службы (X.500).

Независимо от величины банка его документооборот и информационные потоки можно условно разделить на два класса. Это внутрибанковский поток информации и поток внешней информации, среди которой можно выделить:

- связи с клиентами;
- связи с отделениями и филиалами;
- межбанковские связи и связи с подразделениями Центрального Банка (ГРКЦ, РКЦ и тому подобное).

Для многих российских банков существует проблема внешних связей, тогда как для западных банков предоставление клиенту возможности удаленного доступа к банковской системе (банк "на дому") является стандартной услугой. Это объясняется недостаточной развитостью на территории России телекоммуникационных средств и услуг, чьи параметры должны удовлетворять реально существующим требованиям международной стандартизации, надежности передачи данных и защищенности от случайного или преднамеренного доступа.

Для защиты информации внедряется система санкционирования доступа и криптографической обработки данных, реализующая рекомендации международных стандартов и соответствующая требованиям государственных стандартов, регламентирующих услуги по информационной безопасности сети.

Транспортная система и физическая среда передачи данных поддерживают передачу информационных потоков. Единица обмена — блок данных (пакет).

Для примера кратко рассмотрим часто используемое в нашей стране оборудование французской фирмы OST, которой было создано несколько поколений центров коммутации пакетов (ЦКП), сборщиков-разборщиков пакетов (СРП) и программного обеспечения (ПО) управления сетями [9]. Аппаратура OST в основном служит для обеспечения функционирования транспортной подсистемы передачи данных, а также для сопряжения сетей различных типов, например телефонной сети и сети с протоколом X.25. Подобная гибкость обусловливается как развитым ПО устройств, записанным в памяти ЦКП, так и особенностями ПО ПЭВМ, управляющих сетью и позволяющих не только дистанционно контролировать деятельность отдельных устройств сети, но и производить большое количество операций, связанных с перезагрузкой и перепрограммированием удаленных объектов телекоммуникационных сетей (ТКС).

При этом следует отметить, что ранее установленное оборудование и ПО не всегда отвечает самым современным и жестким требованиям, определяемым большим количеством национальных и международных стандартов.

Аппаратура OST в основном служит для обеспечения функционирования транспортной подсистемы передачи данных, а также для сопряжения сетей различных типов, например телефонной сети и сети с протоколом X.25.

Наиболее известными аппаратными средствами, выпускаемыми фирмой OST, являются ЦКП типа ECOM и PASS. Данные устройства имеют практически одинаковую структуру аппаратной части и одинаковое ПО. Эти устройства поддерживают все наиболее распространенные телекоммуникационные протоколы, что позволяет оборудованию OST работать в составе практически любой ТКС. Следует также заметить, что этому способствует большой диапазон скоростей передачи информации и возможность установки значительного числа интерфейсов. За время деятельности фирмы были выпущены различные модификации или классы устройств, отличающихся степенью совершенства ПО и быстродействием. Ограничимся рассмотрением ЦКП и СРП серийного класса — класса "Т".

Центры коммутации пакетов являются узловыми элементами любой современной ТКС, в функции которых помимо соединения абонентов входят также проверка получаемых пакетов на наличие ошибок (как в адресных, так и в информационных полях), сбор статистической информации и передача в ЦУС данных, характеризующих в реальном масштабе времени состояние устройства. Кроме того, ЦКП фирмы OST могут быть использованы для подключения локальных вычислительных сетей к транспортной подсистеме с протоколом X.25. В этом случае ЦКП (только устройство типа PASS), снабженные соответствующими платами, выполняют дополнительные функции межпротокольных маршрутизаторов.

Структурная схема ЦКП достаточно сложна, однако для понимания принципа действия таких устройств достаточно выделить в них четыре основные части:

- центральный процессор (в документации по устройству ECOM принято название "хостпроцессор");
- встроенная память;
- предпроцессор (в документации OST-FEP от английского слова front-end-processor);
- интерфейс.

Центральный процессор, построенный на основе микросхемы серии 68000 (производство фирмы Motorolla), сосредоточивает функции управления ЦКП, в частности сбор и обработку статистической информации, координацию работы предпроцессоров, формирование служебной информации, передаваемой в центр управления телекоммуникационной сети ЦУС, а также хранение адресных пользовательских данных, необходимых для защиты их информации (см. далее). Центральный процессор может координировать работу различного числа предпроцессоров. В ЦКП типа PASS всего один предпроцессор, а в устройствах типа ECOM их может быть до 9. При этом следует учитывать, что каждый из предпроцессоров может управлять работой 8 (или до 20 в ЦКП PASS-20) линий передачи с числом виртуальных каналов до 250. Память ЦКП состоит из четырех фрагментов:

программируемое энергонезависимое запоминающее устройство (ЗУ), хранящее информацию о загрузке ЦКП (например, операционные таблицы конфигурации и маршрутизации), а также содержащее штатное ПО ЦКП;

динамическое ЗУ с перераспределяемыми зонами памяти, в которых могут быть записаны, например, словари кодирования/декодирования при сжатии информации и другие служебные данные;

статическое ЗУ, содержащее конфигурационные, трассировочные и статистические таблицы;

буферное динамическое ЗУ, в памяти которого могут накапливаться пакеты, ожидающие своей очереди на передачу или на прием.

Данные, относящиеся к конфигурированию, трассировке (маршрутизации) и параметрам пакетной передачи информации, хранятся в памяти ЦКП в табличном виде. Существует два вида таблиц: рабочие и операционные. По своей структуре эти таблицы совершенно идентичны друг другу. Однако операционные таблицы хранятся в энергонезависимом ЗУ и, следовательно, при включении должны автоматически загружаться в память центрального процессора. Рабочие таблицы предназначены для записи сценариев загрузки, предлагаемых оператором. После утверждения сценария загрузки данные таблицы могут быть перегружены в операционные с помощью соответствующих команд меню управления памятью ЦКП [9].

Функции предпроцессора весьма разнообразны и включают в себя контроль за работой интерфейсных плат, обмен информацией с центральным процессором, контроль за состоянием линий (на физическом и логическом уровнях), генерацию аварийных сигналов и многое другое. Наиболее распространенной для обычных ТКС является комплектация ЦКП интерфейсами V.24/V.28.

Отдельные части ЦКП связаны между собой специализированным ПО, которое в совокупности с ПО управления сетью образует основу гибкой ТС, способной достаточно просто "стыковаться" с различными национальными и корпоративными сетями в условиях жесткой регламентации телекоммуникационных параметров и качества сетевых услуг. Среди последних особо выделим сборку-разборку пакетов переменной длины, облегчающую работу ЦКП с оборудованием, выпускаемым другими фирмами, организацию виртуального вызова и постоянного виртуального канала.

Важная особенность ЦКП PASS и ECOM заключается в сборе и накоплении статистических данных о количестве пере-

данной или принятой информации. Эти данные служат основой для расчетов за пользование сетью и, следовательно, для оценки экономической эффективности функционирования ТКС. Статистическая информация может быть также использована для управления эволюцией сети с целью, например, повышения пропускной способности отдельной линии передачи или целого фрагмента ТКС.

В число статистических параметров, обрабатываемых центральным процессором ЦКП, входят также параметры, характеризующие техническое состояние устройства и работоспособность его ПО. Количественно эти параметры могут быть оценены путем подсчета потока аварийных сигналов различных типов, генерируемых как процессором, так и предпроцессорами ЦКП. С точки зрения управления сетью, такая информация необходима для выявления наименее надежных участков ТКС. Следует заметить, что аварийные сигналы могут генерироваться также в случае получения искаженной пакетной информации, например в случае потери части адресного поля пакета или отрицательного результата при контроле на четность. Подсчет таких сигналов с помощью специальных счетчиков осуществляется в памяти ЦКП, что позволяет разносторонне оценить качество работы устройства на логическом уровне. Примечательно, что аварийные сигналы генерируются процессором ЦКП и в случае попытки несанкционированного доступа к операционным таблицам, а также при попытках вскрытия установленного пароля устройства.

Сборщики-разборщики пакетов необходимы для подключения к ТКС оконечных устройств обработки данных, например терминала или принтера. Наиболее широко распространенными СРП фирмы OST являются устройства типа EUROPAD, которые оснащены интерфейсом V.24/V.28 и поддерживают основные протоколы X.3, X28, X.25, X.29. СРП типа EUROPAD в отличие от ЦКП не содержат предпроцессоров и в силу особенностей работы имеют отличное ПО. Однако большинство функций (сбор статистики, принцип генерации аварийных сигналов и др.), а также команд сходны у ЦКП и СРП.

Устройства, рассмотренные выше, являются полностью совместимыми на физическом и логическом уровнях (соответственно на 1-м и 2-м уровнях в терминологии документации

OST), что позволяет сравнительно просто объединять их в сети различной конфигурации и сложности. При этом укрупнение сети может производиться не только за счет введения в нее новых устройств, но и за счет установки в уже имеющиеся дополнительных плат, позволяющих увеличить число соответствующих каналов СРП и ЦКП. Каждая отдельная дополнительная плата для ЦКП PASS-8/20 содержит 2 порта; для ЦКП ECOM-24 — 4 и для ECOM-72 — 8. Количество асинхронных каналов СРП EUROPAD может быть увеличено. Кроме того, с помощью одного и того же ЦКП (при соответствующей комплектации) возможен выход в такие сети, как ISDN, сеть с коммутацией пакетов и телефонную сеть. Очевидно, еще большие возможности открываются при совместном использовании в сети ЦКП и СРП.

Дальнейшее развитие аппаратных средств OST происходит по пути увеличения скорости коммутации пакетов и совершенствования сервисных и сетевых услуг, обеспечиваемых ПО ЦКП и СРП.

Программное обеспечение ЦКП в процессе работы генерирует достаточно большой поток служебной информации, позволяющей судить не только о работоспособности устройства, но и о его возможности функционирования в сети с пакетной передачей данных. Указанная служебная информация подразделяется на два уровня. Первый уровень включает в себя сведения о состоянии линий передачи, например о наличии электрического контакта с аппаратурой абонента. Информация второго уровня целиком относится к процессу передачи данных по протоколу X.25, поэтому в документации OST этот уровень часто называют логическим в отличие от предыдущего, называемого физическим. В частности, на логическом уровне осуществляется проверка достоверности передаваемой и получаемой информации, подсчет количества полученных и посланных сообщений, контроль за доступом к сети, подсчет времени связи с сопредельными ТС и т.д. Очевидно, что для сбора указанной информации в сети должен быть объект, оснащенный соответствующим ПО, придающим ему административно-командные функции. Таким ПО для сети OST является комплекс программ, объединенных в программный продукт, под названием Net/PC. Данное ПО в совокупности с IBM-совместимой ПЭВМ и специализированной платой образует

центр управления сетью, к основным функциям которого относятся:

- инсталляция сети и управление ее эволюцией;
- отображение состояния сети в реальном масштабе времени;
- обнаружение и идентификация неисправностей в сети;
- администрирование сети;
- реконфигурирование сети;
- контроль загруженности сети и организация эксплуатационных мероприятий.

При объединении ТС в единую глобальную сеть возникает необходимость в создании единого управляющего центра, контролирующего работу отдельных сетей. На базе IBM-совместимого компьютера фирма OST предлагает в качестве упомянутого устройства центр администрирования сетей (НАС), снабженный ПО под названием Supllet. Центр администрирования сетей в иерархическом отношении стоит, естественно выше, чем ЦУС и может выполнять практически все его функции по управлению, сбору, хранению и обработке информации о ТС, находящихся под его контролем. Число таких сетей может достигать 10, а число ЦКП в них — 500. При этом ЦАС может обмениваться служебной информацией, содержащей сведения об отказах в отдельных ЦКП с любым из подконтрольных ЦУС. Программное обеспечение НАС создано на основе продукта Net/PC, что позволяет исключительно легко стыковать средства управления различных уровней. Основное отличие ПО Supllet от ПО Net/PC заключается в меньшем объеме информации о каждой сети, содержащейся в описательной и статистической частях меню.

В ТКС фирмы OST применяются минимально необходимые средства защиты информации. Достаточно большая часть информации, передаваемой транспортной подсистемой по протоколу X.25, является зашифрованной в подсистеме почты. Для повышения степени защищенности передаваемой информации в сетях OST существуют средства ограничения доступа, которые можно разбить на две группы:

- ограничение доступа к управлению ТКС;
- создание фрагментов сети и отдельных линий передачи, защищенных от несанкционированного доступа.

Средства защиты управления устанавливаются администратором сетей, планирующим как условия доступа (создание и периодическое обновление паролей), так и его разграничение между операторами ЦУС и пользователями различных рангов.

В сетях OST система паролей предназначена для защиты следующих объектов и элементов ТКС:

- программного обеспечения управления сетью;
- конфигурационных и маршрутизационных таблиц ЦКП и СРП;
- специализированных списков пользователей;
- статистической информации.

Первые два объекта защиты имеют прямое отношение к живучести сети, а также к проблеме несанкционированного подключения пользователей и дополнительного телекоммуникационного оборудования. Примерно ту же цель преследует и защита специализированных списков пользователей, таких, как списки сетевых идентификаторов пользователей (NUI — аббревиатура от network user identification) и групп закрытых пользователей (ГЗП). Защита списков пользователей важна еще и в экономическом плане, поскольку на основе данных списков ЦУС автоматически начисляет плату за пользование сетью. При наличии такой защиты пользователи могут быть уверены в том, что их идентификатором никто не сможет воспользоваться для передачи данных по ТКС. Статистическая информация также является основанием для начисления платы за пользование сетью, поэтому с экономической точки зрения ее искажение, например сброс счетчиков переданных или полученных пакетов ЦКП, совершенно недопустимо.

В ТКС фирмы OST, как и во многих других, существует два типа паролей: пароль администратора и операторский пароль. Первый из них дает неограниченный доступ к ПО объектов и сети в целом. Этот же пароль дает право регламентации доступа оператора к отдельным разделам и подразделам меню ЦУС, ЦКП и СРП.

Пароль администратора устанавливается первый раз в процессе инсталляции Net/PC. Впоследствии он может быть модифицирован в соответствующем подразделе меню описания сети (ПАРОЛЬ), естественно, недоступного оператору. При конфигурировании ТС администратор может установить собственные пароли, закрывающие оператору или какому-либо абонен-

ту сети доступ к ПС ЦКП или СРП. Следует отметить, что выбор администратором программных средств, доступных оператору, должен обеспечивать последнему возможность не только наблюдения за сетью, но и возможность ее частичного или полного восстановления.

В заводской конфигурации ЦКП пароль задан по умолчанию (в устройствах ECOM и PASS он один и тот же — HELLO). Впоследствии необходимо его изменить таким образом, чтобы доступ к ПО ЦКП и СРП имел оператор ЦУС, но не имели пользователи сети. Более того, с целью гарантированной неприкосновенности ПО объектов сети со стороны пользователей рекомендуется периодически менять пароли с помощью команд подразделов РАСПИСАНИЕ и ПАРОЛЬ.

Таким образом, система паролей является первичным средством, регламентирующим доступ к сетевой информации и модификации ТС. Остальные способы защиты информации, рассмотренные ниже, имеют уровень пользователей транспортной подсистемы и предназначены для защиты их информации.

Их суть заключается в организации проверки процессором ЦКП адреса вызывающего абонента на соответствие адресу, для которого разрешена связь по определенной линии. Список таких адресов хранится в специальной зоне памяти и автоматически загружается в операционные таблицы при включении ЦКП. Такая таблица состоит из двух столбцов, в одном из которых определены адреса вызывающих абонентов, а в другом — номера линий, предназначенных для конфиденциальной связи. Следует отметить, что при конфиденциальном режиме связь может быть как односторонней, так и многосторонней. Конкретная реализация режима осуществляется при конфигурировании линий связи, где выдается разрешение на конфиденциальность, а также при трассировке, во время которой устанавливается соответствие между адресами вызывающих абонентов и разрешенных линий связи. Заметим, что рассмотренный режим может быть использован как самостоятельное, так и дополнительное средство защиты. В последнем случае оно может применяться совместно с идентификацией пользователей и созданием групп закрытых пользователей.

Сетевой идентификатор пользователя (NUI) применяется для реализации в сети двух важных процедур:

- ограничение доступа в ТКС;

- начисление платы за пользование сетью.

Организация ограничения доступа при помощи сетевого идентификатора достигается за счет создания в памяти ЦКП защищенных посредством паролей таблиц. В данных таблицах устанавливается соответствие между идентификаторами, представляющими собой алфавитно-цифровую комбинацию из 1-14 символов, и сетевыми адресами абонентов из 1-15 цифр. Каждый пользователь при передаче сообщений заносит в них свой идентификатор, который, согласно указанной таблице, трансформируется в сетевой адрес пользователя. Таким образом, сообщения с незарегистрированным или отсутствующим идентификатором не могут быть переданы по ТКС.

Начисление платы за пользование сетью также производится в соответствии с упомянутыми таблицами на основе статистической информации, накопленной в памяти ЦКП по каждому отдельному абоненту.

Помимо этого производится организация групп закрытых пользователей. Сеть разбивается на отдельные фрагменты с открытым или ограниченным доступом. Пользователи, чьи терминальные устройства присоединены к последним фрагментам, и образуют данную группу.

В зависимости от степени необходимости обмена информацией с другими аналогичными группами или внутри одной группы каждому члену может быть присвоен какой-либо из следующих видов доступа:

разрешение на связь внутри группы и запрещение на связь вне ее;

передача информации разрешена внутри и за ее пределы, но без права получения информации извне;

обмен сообщениями между членами группы разрешен без права передачи информации внешним абонентам, но с правом ее получения от них;

разрешение на передачу сообщений другим членам группы без права получения от них какой-либо информации;

запрет на передачу информации членам своей группы и разрешение на получения от них сообщений.

Учитывая, что некоторые пользователи как члены нескольких групп могут иметь различные виды доступа, организация защиты информации рассматриваемым способом обладает особой гибкостью.

Для создания коммуникаций между регионами России, включая территории с неразвитой инфраструктурой связи, а также в странах ближнего зарубежья в ЕТКБС используются сегменты спутниковых систем связи. По заданию ЦБ РФ разрабатывается спутниковая система связи (ССС) "Банкир", предназначенная для предоставления абонентам цифровых каналов связи со скоростью от 64 до 256 Кбит/с. Для ССС "Банкир" будут использованы ресурсы космической группировки спутников типа "Купон", а в качестве резервного варианта — ресурсы спутников Eutelsat-F4 или других подобных систем связи. Первый спутник системы "Банкир" был запущен в ноябре 1997 г.

Банковские информационные стандарты выдвигают повышенные требования к быстродействию и надежности технических и программных средств. В ЕТКБС выполнение заданных требований достигается использованием высокопроизводительного отказоустойчивого оборудования и соответствующего программного обеспечения, резервированием узлов, применением специализированных средств сохранения целостности данных и самодиагностики, оперативным устранением отказов.

Для поддержки синхронной работы расчетных и информационных центров внедряются высокоскоростные магистральные каналы связи и средства автоматического копирования общесистемной и прикладной информации в удаленных резервных центрах и на внешних носителях.

Применяются архитектурные решения по реализации надежных серверов в кластерной системе с горизонтальной и вертикальной интеграцией процессов обработки и передачи информации, обеспечивающие высокие показатели надежности, безопасности информационного взаимодействия служб ЦБ РФ и своевременности доставки платежных документов.

Все перечисленные механизмы, согласно международному стандарту ISO 7498-2 [19], реализуются на прикладном уровне, т.е. встраиваются непосредственно в банковские приложения внутри абонентской системы или в систему электронного документооборота, в результате чего защита информации обеспечивается независимо от телекоммуникационной системы.

1.2. ЭЛЕКТРОННЫЙ ДОКУМЕНТООБОРОТ

Документооборот банковской системы состоит из двух основных потоков:

⇒ документы управления, циркулирующие между различными структурными подразделениями ЦБ РФ;

⇒ платежные документы, перемещаемые как между соответствующими функциональными подразделениями ЦБ РФ, так и между коммерческими банками и другими финансовыми учреждениями.

К основным документам, образующим документооборот между различными банковскими структурами (подразделения ЦБ РФ, коммерческие банки), относятся:

- платежное поручение;
- чек;
- аккредитив;
- оборотносальдовая ведомость;
- консолидированный ежемесячный баланс;
- расчет нормативов;
- справка по внебалансовым счетам;
- отчет о доходах и расходах банка и т.д.

К вспомогательным относятся те документы, которые обеспечивают дополнительный сервис и полноту обслуживания как клиентов автоматизированной банковской системы, так и служб эксплуатации, контроля, анализа и т.д. К ним относятся, например, ведомости по заработной плате, выплате пенсий, начислению дивидендов, а также справочная, отчетная и нормативная информация, оформленная в виде больших массивов. Вспомогательная информация является существенной частью документооборота современных банковских систем.

Перечисленные документы в электронной типовой форме являются основой электронного документооборота различных автоматизированных банковских систем (АБС), в том числе и АСБР.

В свою очередь, электронные платежные документы (ЭПД) представляют собой наиболее массовые и важные информационные ресурсы АБС с позиций безопасности информации [5, 6]. В соответствии с этим Банк России выработал требования к технологиям, системам и средствам обработки, передачи и хранения электронных платежных (несекретных) документов. Тре-

бования разработаны в соответствии с положениями федеральных законов, нормативных и иных актов Банка России, Государственной технической комиссии при Президенте Российской Федерации (Гостехкомиссии России), Федерального агентства правительственной связи и информации при Президенте Российской Федерации (ФАПСИ).

Важность вышеизложенного подчеркивается и обусловлена утверждением за информацией статуса материального ресурса [10]. *Информационные ресурсы* — отдельные документы или их массивы на материальных носителях с необходимыми реквизитами в информационных системах. В свою очередь, *документированная информация* (документ) — зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать. Содержащиеся в ЭВМ сведения об активах (стоимость кредита, результаты подсчета баланса, счета-квитанции, остатки на счетах и т.п.) представлены в виде цифровой информации или данных на машинных носителях.

Для успешного внедрения системы электронных платежей необходима унификация структуры и единые правила заполнения банковских документов во всех автоматизированных рабочих местах (АРМ).

Для каждого банковского документа необходимо разработать его типовой электронный образ, методы контроля правильности и полноты заполнения.

Для организации взаимодействия между различными отечественными и международными банковскими системами структуры банковских документов должны удовлетворять стандартам, разработанным в рамках рекомендаций EDIFACT [20].

В настоящее время коммерческие банки, предоставляющие крупным клиентам услуги по организации рабочих мест для удаленного ввода платежных документов на базе ПЭВМ, также внедряют новейшие информационные технологии.

Система организации документооборота (СОД) предоставляет возможность подготовки документов, входного и выходного контроля, учета прохождения документов, ведения архивов и преобразования форматов.

Структура электронной СОД и ее место в системе обработки информации ЕТКБС (рис.2) определяется набором функций, обеспечивающих обмен документами межбанковских расчетов, и другими формализованными документами с использованием

транспортной среды электронной почты. В эти функции входят:

- учет входящей и исходящей документации;
- преобразование форматов представления документов;
- внутренняя и внешняя рассылка документов;
- ведение архивов и т.п.

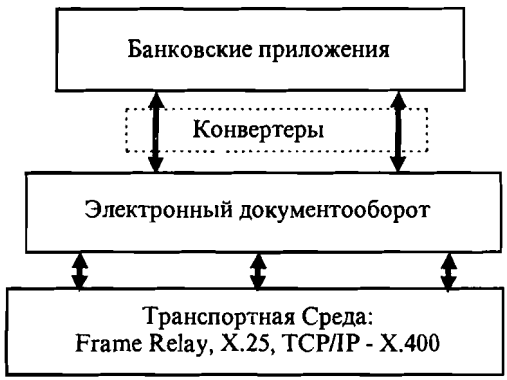

Рис.2. Взаимодействие СОД в системе обработки информации

Система организации документооборота (рис.3) состоит из следующих компонентов:

центр управления организацией документооборота (ЦОД);

локальные центры и системы организации документооборота;

локальные и удаленные рабочие места.

Система организации документооборота производит маршрутизацию и распределение документов по различным прикладным системам с организацией "очередей" обработки и преобразования форматов. При этом ЦОД осуществляет управление средствами почтовой системы и обеспечивает:

- проведение процесса аутентификации пользователей;
- прием и передачу сообщений;
- обработку информации криптографическими средствами;
- регистрацию данных и архивацию сообщений;
- определение маршрутов продвижения документов;
- построение очередей на передачу;
- взаимодействие с локальными рабочими местами;

■ преобразование документов в унифицированные форматы электронных банковских сообщений;
■ обмен информацией с расчетной банковской системой.

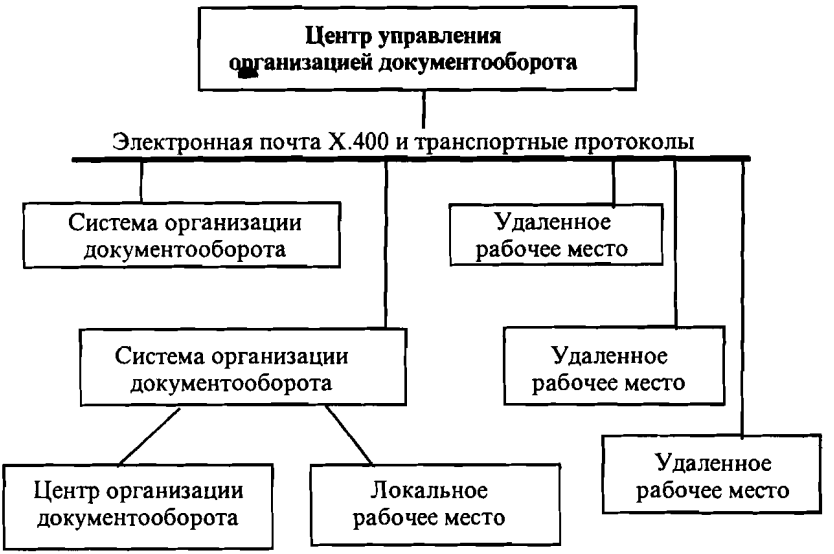

Рис.3. Общая структура СОД

В ЦБ РФ основными форматами электронных платежей и расчетов в соответствии с утвержденным положением "Временные форматы электронных сообщений" приняты унифицированные SWIFT-ориентированные форматы.

Часть межбанковских расчетов, а именно расчетов многофилиальных банков, в том числе по перераспределению кредитных ресурсов, осуществляется между головным банком и его филиалами и между филиалами банков с отражением на их балансовых счетах. Внутрибанковские расчеты динамично развиваются.

Межбанковские расчеты осуществляются также через корреспондентские счета, открываемые в других банках. Порядок открытия и режим функционирования корреспондентского счета одного банка в другом определяется по соглашению между ними.

Операции, проводимые по корреспондентским счетам банков-корреспондентов, делятся, главным образом, на два вида:

операции, основывающиеся на обслуживании клиентов, и собственные межбанковские операции. К первым относятся операции по коммерческим сделкам клиентов; вторые включают кредитные операции, операции по покупке и продаже валют, по торговле ресурсами на денежном рынке и др. Банки, имеющие развитую корреспондентскую сеть, способны осуществлять расчеты с максимальной скоростью и образуют собственные расчетные системы.

Развитие корреспондентских отношений зависит от различных факторов: взаимных потоков платежей, цены и спроса на рынке кредитных ресурсов, возможности участия в торгах на региональных валютных биржах и других.

Расчеты между банками-корреспондентами составляют значительную часть всего платежного оборота России. Таким способом совершается большая часть расчетов с банками стран СНГ и зарубежными банками.

Еще одним способом межбанковских расчетов являются расчеты через клиринговые палаты, как негосударственные, так и действующие на базе расчетно-кассовых центров Банка России.

В основу принципов проведения клиринговых операций положены две возможные модели. Первая — без предварительного депонирования средств на счетах банков-участников расчетов в клиринговом учреждении. Окончательный расчет в этом случае осуществляет Центральный банк Российской Федерации. Вторая модель — с предварительным депонированием средств на счетах банков-участников в клиринговом учреждении. Расчетным агентом по такой схеме является само клиринговое учреждение.

По первой модели в 1997 г. в Москве начала работать Клиринговая палата Межбанковского финансового дома (МФД). По второй модели, по данным на конец 1996 г., действовали шесть клиринговых учреждений, расчеты через них осуществляли 143 кредитные организации и филиала. Удельный вес расчетов, осуществляемых через них, в настоящее время невелик. Банк России играет определяющую роль в разработке принципов организации клиринговых операций и контролирует их соблюдение.

В 1996 г. была разработана "Стратегия развития платежной системы России", которая содержит основные долгосрочные и

среднесрочные мероприятия. Они включают создание системы расчетов в режиме реального времени, т.е. переход на качественно новый уровень передачи банковской информации, развитие негосударственных расчетных и клиринговых систем с соответствующим регламентированием и надзором за их деятельностью, разработку систем стандартизации и сертификации банковских технологий, создание в России условий для внедрения расчетов платежными(пластиковыми) картами.

1.3. АВТОМАТИЗИРОВАННАЯ СИСТЕМА БАНКОВСКИХ РАСЧЕТОВ

1.3.1. Общие положения

Современные системы электронного документооборота все больше применяются во всех областях экономики [38]. Их преимуществом является высокая скорость прохождения и обработки документов. На любом предприятии или в любом учреждении внедрение системы электронного документооборота может значительно повысить эффективность работы в целом и качество обработки документов. Одной из таких систем электронного документооборота является система банковских расчетов или клиринговая система. В странах Западной Европы и Северной Америки применение автоматизированных клиринговых центров (КЦ) приняло настолько широкие масштабы, что трудно себе представить, как без них функционировали бы банковские системы. Главными целями каждой клиринговой системы являются:

- обеспечение рационального платежного оборота путем балансирования платежных требований и обязательств, минимизирующего перемещения денежной массы;
- обеспечение согласованного по срокам беспрепятственного платежного оборота.

Кроме осуществления главных функций с помощью клиринговой системы решаются следующие основные задачи:

- проблема срочных платежей и взаиморасчетов, а также перевода больших сумм денег;
- гарантия платежей и расчетов, сведение к минимуму банковского риска ;

- сокращение расходов и увеличение доходов банка (за счет расширения услуг);
- обеспечение конкурентоспособности банковских сетей и систем;
- сокращение до минимума доли ручного труда и использования бумажных носителей информации;
- обеспечение высокой степени сохранности и защищенности банковской информации;
- сокращение до разумных пределов доли расчетов с наличными;
- расширение спектра услуг, оказываемых клиентам;
- унификация и стандартизация;
- разумное сочетание временных и финансовых затрат банков с расширением услуг;
- интеграция различных систем.

Клиринговая система должна обеспечивать наряду со своей основной функцией — технологически правильной процедурой клиринга — и другие функции, невозможность выполнения которых ставит под сомнение вопрос о ее пригодности. Суть этих функций сводится к необходимости обработки достоверных данных к нужному сроку при обеспечении требуемого уровня достоверности обработки информации, а охарактеризовать их можно как оперативность, достоверность, надежность и безопасность.

Оперативность обработки банковской информации, поступающей в клиринговый центр, зависит от производительности центра как системы вкупе с надежностью всей используемой технологии.

Достоверность полученных результатов подразумевает обеспечение требуемого уровня достоверности обработки информации.

Для безопасности банковской информации на всех этапах ее обработки должны применяться методы, обеспечивающие требуемый уровень защищенности данных от утечки, несанкционированного изменения и нарушения процесса их обработки [2, 4, 11, 12, 20, 27].

С точки зрения информационной технологии современный расчетно-клиринговый центр, независимо от типа, в своем большинстве представляет собой распределенную систему обработки данных, построенную по технологии передачи данных

в соответствии с архитектурой открытых систем и международных стандартов (рис.4).

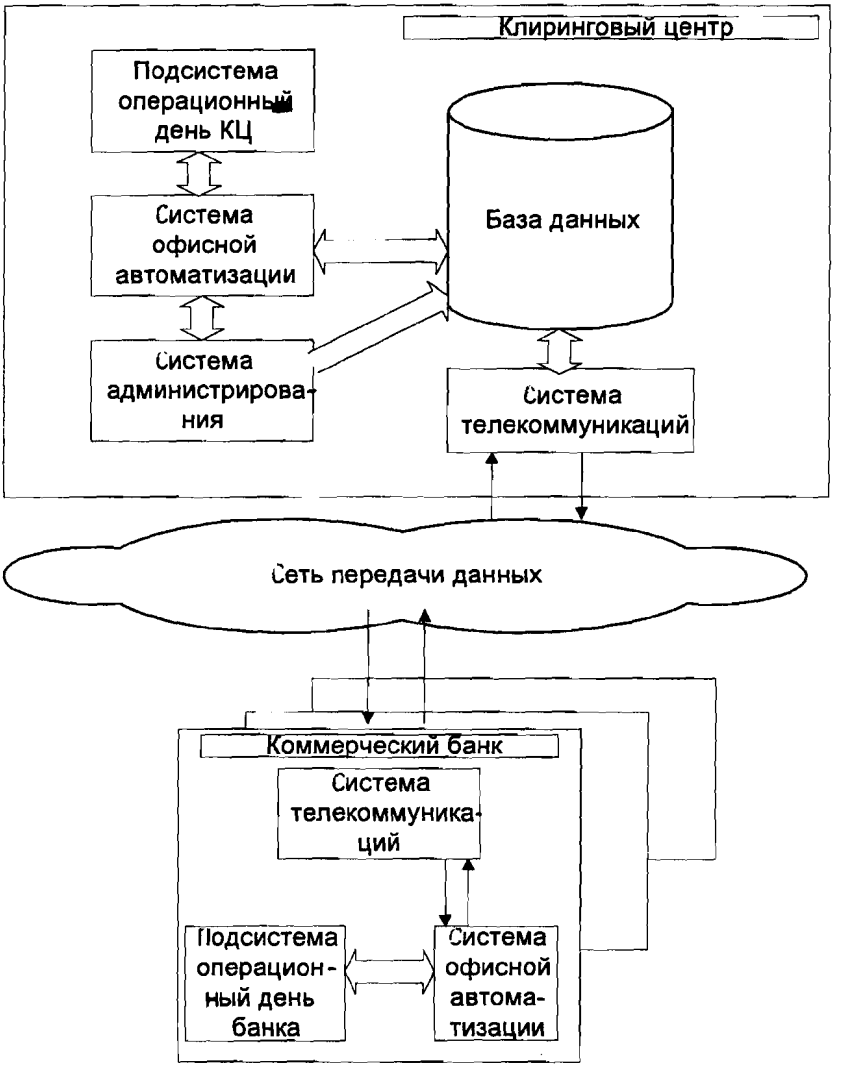

Рис.4. Общая структура клирингового центра

Его структура представляет собой совокупность функциональных подсистем, которые обеспечивают следующие основные процессы [38]:

- прикладная подсистема "операционный день" клирингового центра непосредственно выполняет функцию межбанковских расчетов;
- подсистема офисной автоматизации предназначена для организации электронного документооборота в клиринговом центре;
- подсистема администрирования поддерживает настройку и управление функционированием всех систем;
- телекоммуникационная система позволяет обеспечить взаимодействие между клиринговым центром и коммерческими банками (клиентами клирингового центра).

Однако кроме очевидных преимуществ в сравнении с обычными способами расчетов: существенного повышения скорости межбанковских расчетов, снижение затрат, связанных с транспортировкой наличных денег и т.д., внедрение систем электронных расчетов может повлечь за собой и ощутимые потери, если своевременно не будут приняты адекватные меры безопасности.

Упрощенная схема электронных клиринговых расчетов в наиболее общем случае представлена на рис.5.

В случае с предварительным депонированием средств банки открывают корреспондентские счета в клиринговом центре (КЦ). В КЦ находятся определенные суммы денег обоих банков. Затем, когда один из банков хочет сделать платеж другому банку, он дает распоряжение КЦ перевести на счет другого банка необходимую сумму денег. КЦ это делает путем уменьшения части средств банка 1 на указанную сумму и добавления их на счет банка 2. После данной операции сумма на счету другого банка увеличится, а у банка, делавшего платеж, уменьшится на сумму платежа. Точно так же происходит платеж в обратном направлении. Следует отметить, что сумма платежа не может превышать сумму, находящуюся в данный момент на счету банка. Таким образом получается система взаимозачетов между банками, которая исключает необходимость использования наличных средств. Между банками и КЦ циркулируют только формализованные документы, называемые платежными поручениями.

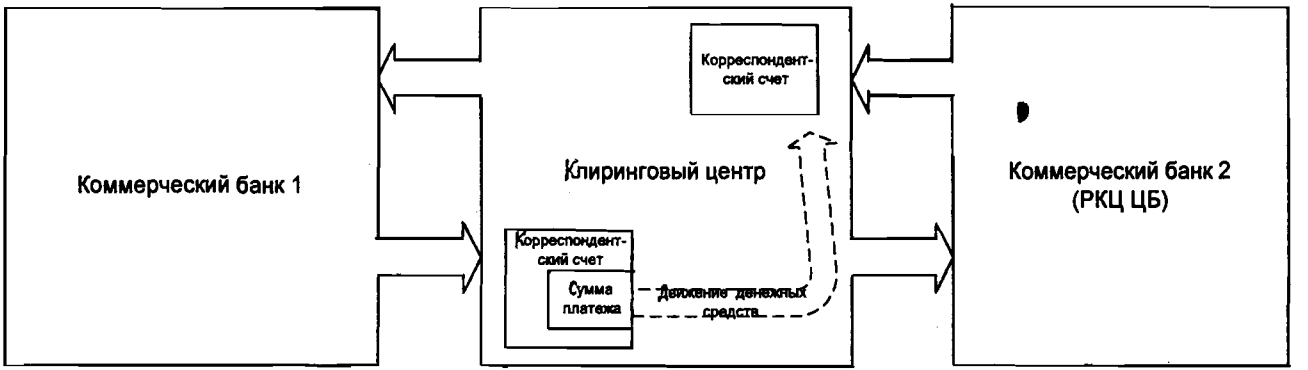

Рис.5. Упрощенная структурная схема расчетной системы

1.3.2. Расчеты в системе ЦБ РФ

Платежная система ЦБ с ее расчетной основой строится по указанным выше принципам, является распределенной системой обработки информации и обладает определенными особенностями.

Как указано в [36], условно эти особенности платежной системы можно разбить на три группы: системные, информационные и "конкретно-исторические".

К *системным особенностям*, присущим, по-видимому, для любой платежной системы и ее важнейшей расчетной части, можно отнести следующие:

1. Жесткие требования системы на надежность и оперативность перевода денежных средств (платежей) между участниками расчетов. Экономическая (финансовая, материальная) ответственность Центрального банка перед коммерческими банками и коммерческих банков перед своими клиентами за нарушение сроков и правильности проводки платежей (см. разд.1). Эта ответственность закрепляется в соответствующих договорах и при необходимости должна регулироваться в арбитражных судах.

2. Обязательное наличие арбитров (третейских судов) для разбирательства возможных споров между участниками расчетов в платежной системе.

3. Подверженность платежной системы нападениям злоумышленников с целью хищения денежных средств путем создания фальшивых или искаженных платежных документов, а также использование информации, циркулирующей в платежных системах в преступных целях. Нарушителями при этом могут быть как легальные пользователи, так и посторонние лица.

4. Возможность оценить ущерб (в денежном выражении) от тех или иных угроз платежной системе и, как следствие, сопоставить затраты на реализацию конкретных мер защиты с возможными потерями от ее отсутствия.

К *информационным особенностям* платежной системы относятся:

1. Информация, обрабатываемая в платежной системе, не составляет государственную тайну.

2. Владельцами информации, циркулирующей в платежной системе, являются в основном коммерческие банки или их клиенты.

3. Большое количество платежных документов, обрабатываемых в платежной системе в течение суток.

4. Согласно нормативным документам ЦБ РФ сроки хранения платежных документов составляют 5 лет.

К *"конкретно-историческим" особенностям*, присущим платежной системе России, можно отнести:

1. Значительные расстояния между участниками платежной системы (протяженность страны охватывает 11 часовых поясов).

2. Большое количество участников платежной системы (корреспондентов сети). В настоящее время в число участников платежной системы входят более тысячи расчетно-кассовых центров и свыше трех тысяч коммерческих банков и их филиалов (см. раздел 1).

3. Неразвитость телекоммуникационной системы страны, отсутствие качественных каналов связи со многими участниками платежной системы.

4. "Региональная" структура потоков платежных документов (свыше 75% платежей производятся внутри региона).

5. Наличие центров обработки платежной информации в регионах, в которых скапливаются большие массивы данных (звездообразные структуры организации региональных сетей) и, как следствие, высокие требования по производительности средств обработки банковской информации в таких центрах.

6. Использование в различных регионах различных систем обработки информации (on-line, off-line), наличие большого количества программно-технических платформ (в основном иностранного производства), на которых реализуется доставка и обработка платежных документов, использование различных по своим техническим характеристикам ПЭВМ.

7. Недостаточное количество квалифицированных кадров в области безопасных информационных технологий.

8. Необходимость размещения средств криптографической защиты на различных участках технологической цепочки обработки электронных платежных документов — средства шифрования размещаются на участке транспортирования документов и, возможно, их хранения. Средства электронной

цифровой подписи (ЭЦП) — на участках ввода и контроля документов.

9. Недостаточная приспособленность помещений участников платежной системы для реализации жестких технических и организационных мер безопасности, особенно с учетом того, что банковская система предполагает присутствие значительного количества посторонних лиц на банковских объектах.

Начальная стадия реформы банков в России характеризовалась почти полным отсутствием телекоммуникаций и современных технологий автоматизации банковской деятельности. В этот период важную роль в становлении современной расчетной системы страны сыграли расчетно-кассовые центры (РКЦ) ЦБ РФ, являющиеся технологической основой платежной системы страны. В настоящее время проявляется тенденция сокращения их числа и постепенной потери ими своей значимости. Это связано с централизацией капитала вокруг крупных банков и сокращением числа мелких банков, а также рядом других явлений, происходящих в банковском секторе экономики. Однако представляется, что РКЦ будут существовать еще достаточно длительный период (на это указывает и то, что процесс создания новых РКЦ, определяемый конкретными потребностями регионов, до настоящего времени еще не закончен), и это не будут "застывшие" в технологическом отношении структуры. Они все шире будут внедрять современные информационные технологии, в том числе телекоммуникационные, обеспечивающие на региональном уровне возможность динамичной перестройки структур ЦБ РФ в соответствии с местными условиями с учетом общих процессов, происходящих в банковской сфере экономики.

Одним из важнейших требований к системам автоматизации межбанковских расчетов является их адаптивность, т.е. возможность приспосабливать их к условиям внешней среды (изменяемой совокупности обслуживаемых банковских учреждений и правил, по которым производится взаимодействие с этими учреждениями), которая в общем случае может довольно интенсивно изменяться с течением времени.

Существуют три модели расчетно-аналитических систем. Централизованная модель предполагает обработку информации (документов) по банковским расчетам между всеми учреждениями ЦБ РФ, действующими в регионе, в специализирован-

ном центре обработки информации. Ввод информации, предварительный ее контроль и получение экранных и печатных форм при этом осуществляются на объектах автоматизации, т.е. в РКЦ. На местах может осуществляться и предварительный контроль платежных документов.

В распределенной модели все операции, кроме расчетов с другими государствами, осуществляются на объектах автоматизации. При этом на вычислительном комплексе центра обработки информации выполняются функции управления региональными документопотоками: межбанковские электронные расчеты, составление сводных форм по региону, контроль МФО, межгосударственные расчеты.

Смешанная обработка предполагает централизованное обслуживание части РКЦ, в то время, как другая их часть работает по распределенной схеме. При этом вычислительный комплекс центра обработки информации выполняет функции управления документопотоками для первых и функции обработки информации для вторых.

В настоящее время превалирует создание региональных систем банковских расчетов и взаимодействующих с ними аналитических систем, базирующихся на централизованной модели. Использование централизованной модели обеспечивает возможность реализации расчетно-аналитической системы любого из указанных выше типов и допускает плавный переход от использования одной технологии к другой. Проблема перехода к централизованной модели сегодня актуальна для многих регионов, в которых в настоящее время используются распределенные модели, а изменение структуры расчетной системы ЦБ РФ должно выполняться максимально безболезненно. Многообразие конкретных ситуаций, складывающихся в краях, республиках и областях Российской Федерации вызывает необходимость построения расчетно-аналитических систем с возможностью учета особенностей каждого конкретного региона при использовании типовых главных организационно-технических решений.

Наряду с автоматизацией учетно-операционных и кредитных работ, выполняемых в банковских учреждениях ЦБ РФ, автоматизированная система межбанковских расчетов должна обеспечивать или не препятствовать всем возможным способам осуществления расчетов (почтовое и телеграфное авизование, банковские платежи по 871-му счету, электронные платежи на

валовой основе, электронные платежи на чистой основе) при любой — централизованной, распределенной или смешанной — схеме обработки информации в регионе. Задача создания и эксплуатации подобной системы должна сводиться, с одной стороны, к обеспечению полной централизации расчетов в рамках региона и единообразия в организации межрегиональных взаимосвязей, независимо от используемой в регионе схемы обработки банковской информации, а с другой — к созданию возможностей автономной от специализированного центра обработки информации работы отдельных банковских учреждений.

Для обеспечения высокой надежности и безопасности расчетных центров, в системе ЦБ РФ, применяются кластерные конфигурации. Типовая региональная АСБР была создана группой отечественных организаций во главе с ГУ ЦБ РФ по Рязанской области и внедрена в рабочую эксплуатацию более чем в десятке российских регионов. Она позволяет обеспечить:

- повышение скорости осуществления банковских расчетов;
- высокую безопасность обработки и хранения информации;
- повышение надежности банковских операций;
- минимизацию средств, затрачиваемых на поддержку локальных сетей;
- высокую производительность вычислительного комплекса;
- полную отказоустойчивость программно-технического комплекса, обеспеченную за счет использования двухмашинного комплекса компьютеров;
- управление комплекса из единого центра.

АСБР работает на надежных, высокопроизводительных серверах корпорации Digital Equipment Corporation (DEC), использующих процессор Alpha и операционную систему Open VMS и ПЭВМ под управлением MS DOS и MS Windows. Для закрытия криптографическими методами каналов связи на участках от банков-участников расчетов до серверов используется сертифицированное СКЗИ "Янтарь АСБР". (Это средство криптографической защиты более подробно рассматривается в следующих разделах.) Оно встраивается в автоматизированные системы банковских расчетов и предназначено для:

- повышения безопасности процессов электронных расчетов в регионах;

♦ создания защищенной от несанкционированных воздействий компьютеризованной информационной среды, отражающей актуальные потребности банков и других финансовых учреждений;

♦ обеспечения качественного мониторинга за функционированием средств и систем защиты;

♦ внедрения стандартизированных типовых технологий защиты информации на современной программно-аппаратной базе.

Юридические лица, участвующие в проведении электронных расчетов АСБР, называются "абонентами сети". Под этим термином следует понимать конкретного участника расчетов. Абонентами сети АСБР являются:

- главный расчетно-кассовый центр (ГРКЦ);
- расчетно-кассовые центры (РКЦ);
- коммерческие банки (КБ).

Далее по тексту между абонентами типа ГРКЦ, РКЦ и КБ там, где это возможно, не делается различий и используется единое обозначение абонент КБ (оператор КБ).

Рассматриваемая автоматизированная система банковских расчетов АСБР активно вводится в региональных управлениях ЦБ РФ в качестве типовой. Для АСБР коммерческие банки и РКЦ являются равноправными участниками расчетов. Роль локального клирингового центра играет автоматизированная база данных АСБР, работающая, как отмечалось, на высокопроизводительных серверах корпорации DEC (рис.6).

Для обеспечения бесперебойной работы в данной системе используется многомашинный комплекс, состоящий из серверов DEC Alpha, включенных таким образом, что при выходе из строя одного из них другой (другие) сервер продолжает поддерживать систему расчетов в рабочем состоянии (в дальнейшем, для удобства изложения материала, на схемах будет показываться только один сервер). Однако следует иметь в виду, что серверов, как минимум, два. Также подразумевается, что подсистемы "операционный день", "офисная автоматизация", администрирования реализованы в серверах и входят в состав базы данных (БД). В системе использована подсистема безопасности, основанная на встроенных функциях администрирования системы DEC AXP OPEN VMS и на созданной в базе данных подсистеме безопасности и разграничения прав пользователей БД.

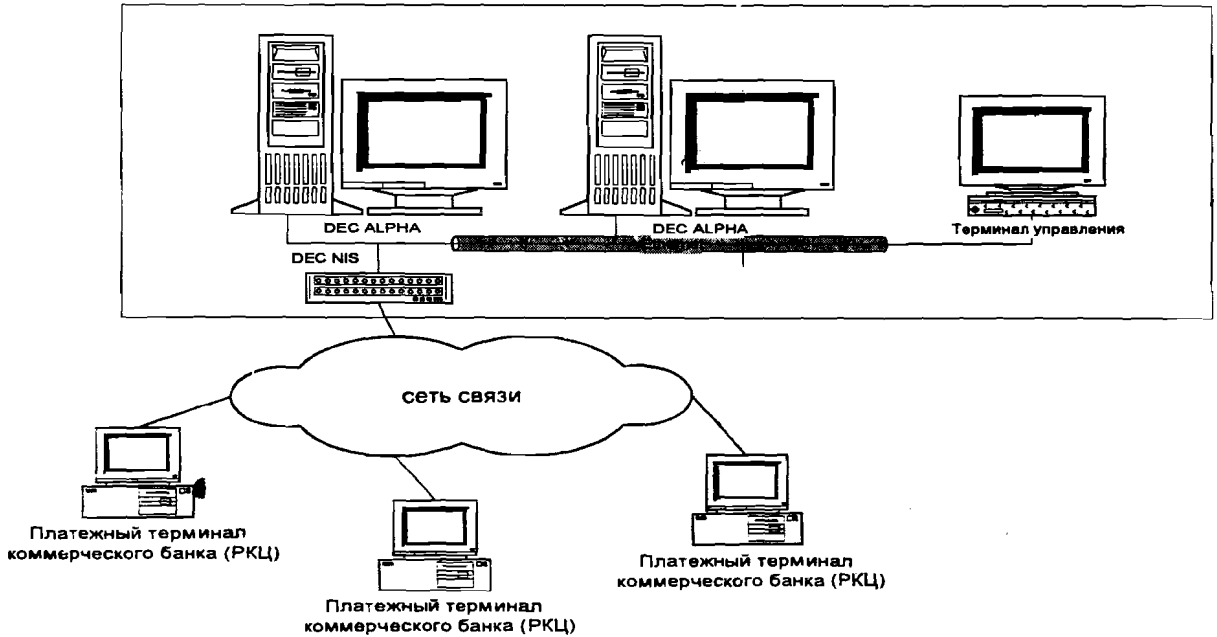

Рис.6. Упрощенная структура АСБР

Вычислительным ядром системы служит региональный вычислительный комплекс автоматизированной системы банковских расчетов (ВК АС БР). Он представляет из себя интегрированный комплекс аппаратных средств и программного обеспечения, производящий обработку банковской информации в регионе на основе автоматизированной системы банковских расчетов. В состав комплекса входит несколько центров обработки данных, располагающихся в региональном ГРКЦ и в районных расчетно-кассовых центрах. Центры обработки данных строятся на основе структурированной кабельной сети, включающей в себя оптоволоконное кольцо FDDI, проложенное по всему зданию, концентраторы, устройства подключения к сети X.25 и другие активные компоненты, а также кабельную разводку на витой паре непосредственно по рабочим местам. Локальные сети объединены в единое информационное пространство с помощью сети пакетной коммутации X.25. Все компоненты структурированной кабельной сети сертифицированы по 5-й категории в соответствии со стандартами TIA/EIA-40, TIA/EIA-36, TIA/EIA-568 и ISO/IEC 11801. Локальные сети центров обработки данных насчитывают от 50 до 250 рабочих мест.

Серверы ВК АС БР реализованы на двухмашинных комплексах компьютеров AlphaServer под управлением операционной системы OpenVMS. В центре обработки данных ГРКЦ установлены наиболее мощные компьютеры семейства AlphaServer, в районных РКЦ — AlphaServer младшего и среднего класса. Работа компьютеров в составе кластера предполагает, что несколько машин работают совместно, под управлением одной операционной системы и контролируют исправность друг друга через высокоскоростной канал обмена информацией. Компьютеры комплекса имеют общее дисковое пространство, через которое при необходимости обмениваются данными прикладные задачи. При исправности всех компьютеров, входящих в комплекс под управлением ОС OpenVMS, прикладные задачи работают параллельно на нескольких машинах. Таким образом обеспечивается увеличение быстродействия комплекса в два и более раз. При отказе одного из компьютеров, входящих в комплекс, его задачи могут быть перераспределены между исправными ЭВМ, которые считывают

данные с дисков и продолжают процессы, прерванные из-за отказа. Работа всего вычислительного комплекса не будет прервана, хотя его быстродействие на время устранения неисправности несколько снизится. Применяемый в составе комплекса дисковый массив позволяет продолжать работу при отказе любого диска или другого элемента и проводить его замену, не прерывая работы системы. Сочетание двухмашинного комплекса на базе компьютеров AlphaServer и одной из самых надежных операционных систем OpenVMS обеспечивает требуемую для банковского учреждения надежность системы (круглосуточное безостановочное функционирование комплекса при отказе любого элемента) и высокую производительность вычислительного комплекса.

Для управления вычислительным комплексом АСБР в сети ГРКЦ предусмотрен центр управления. Программно-аппаратные средства центра управления позволяют проводить мониторинг сети, осуществлять управление отдельными узлами и реконфигурацию сети, не прерывая работы ВК АСБР. С помощью сети X.25 к региональной АСБР может быть подключено большое число пользователей в различных финансовых учреждениях региона (области). На рис.7 приведен пример внедрения ВК АСБР в г. Владимире, где использована оптоволоконная линия передачи данных FDDI.

В общем случае весьма важная подсистема защиты банковской информации в АСБР, как и подсистема защиты любой другой информации, должна обеспечивать достижение трех целей: конфиденциальности, целостности и доступности информации, так как перерывы в функционировании банковской системы приводят к самым значительным потерям для всех ее участников [35]. Первым по важности является обеспечение целостности информации, так как ее нарушение может привести к значительным убыткам отдельных участников расчетной системы, хищениям денежных средств по фальшивым платежным документам. Обеспечение конфиденциальности является третьей по значимости целью защиты информации в расчетной системе, так как ее нарушение не ведет к прямым убыткам участников расчетов и, как правило, не носит катастрофических последствий.

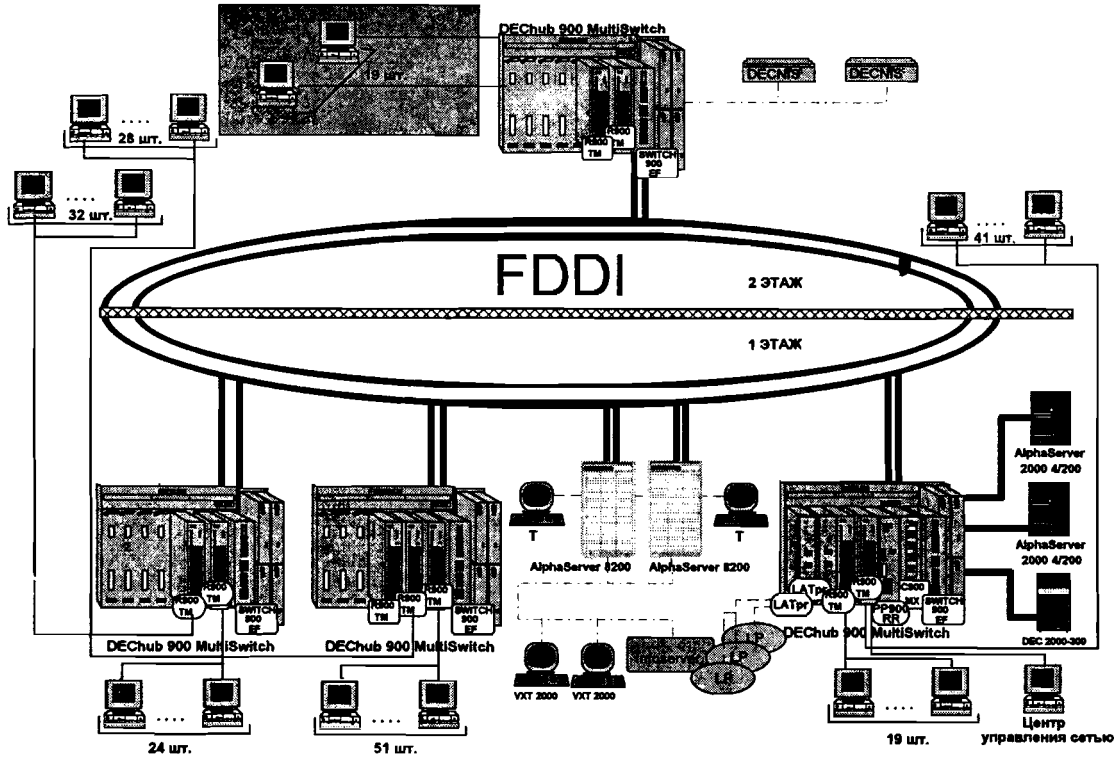

Рис.7. Пример внедрения ВК АС БР (г. Владимир)

Исключительно важным элементом для расчетной системы является защита юридической силы или значимости платежных документов для справедливого разрешения споров и определения виновных в нанесенном ущербе, так как только юридическая защищенность создает доверие к системе расчетов у ее участников и повышает их дисциплинированность при совершении расчетов. Поэтому для банковской системы приоритетными являются криптографические средства обеспечения подлинности и целостности платежных документов, а также средства обеспечения юридической силы электронных платежных документов, что во многом отличает банковскую систему от других информационных систем, содержащих информацию, составляющую государственную тайну.

Изложенные положения нашли отражение при создании и эксплуатации программно-аппаратного средства криптографической защиты информации "Янтарь АСБР" (см. разд.3).

2. ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ БАНКОВСКИХ РАСЧЕТОВ

2.1. ОСНОВНЫЕ ПОЛОЖЕНИЯ

Рассмотрим расширительную формулировку понятия "безопасность информации", учитывающую специфику АСБР как разновидности и составной части АБС, изложенную в аналогичных отечественных работах [27]. Таким образом, *безопасность информации* — состояние устойчивости информации к случайным или преднамеренным нерегламентированным воздействиям, исключающее недопустимые риски ее уничтожения, искажения и раскрытия, которые приводят к материальному ущербу владельца или пользователя информации. Это определение наиболее полно учитывает главное назначение любой информационной АБС — исключение финансовых потерь, получение прибыли владельцем в условиях реальных рисков — и включает минимизацию типично банковских рисков (например, потери за счет ошибочных направлений платежей, фальсификация платежных документов и т.д.) посредством обеспечения безопасности информации, которая подвергается воздействию случайных и преднамеренных угроз. Здесь под *угрозой безопасности информации* понимается потенциальная возможность нарушения основных качеств или свойств информации при ее обработке техническими средствами: конфиденциальности, целостности, доступности и юридической силы (значимости). Эти свойства информации будут определены далее. Перечень используемых терминов и определений приводится в приложении 1.

В настоящее время в России идет активное освоение практики ведения дел в рыночных условиях. Участники экономической деятельности испытывают в связи с этим острую потребность квалифицированно оценивать риски в процессе управления ресурсами и эффективно исправлять их последствия [4].

Риск — стоимостная оценка вероятностного события, ведущего к потерям. Риск позволяет оценить вероятность того, что

некоторая величина финансового ущерба будет находиться в определенных количественных пределах. Это, по сути дела, оборотная сторона свободы предпринимательства. С расширением географии деятельности банка, его АБС, развитием сети отделений и филиалов, осуществлением совместных работ с другими экономическими структурами возрастает риск или вероятность финансовых потерь. Это связано с угрозой появления убытков для банка (предприятия) в целом со стороны одного из его филиалов или одного из участников холдинга вследствие неэффективности его деятельности, либо непрофессионализма персонала или его мошенничества.

Финансовые риски составляют особую группу. Их можно подразделить на несколько основных подгрупп:

♦ кредитный риск, или риск потерь, связан с невыполнением условий кредитного соглашения контрагентом;

♦ рыночный риск связан с неблагоприятными колебаниями обменных курсов валют и процентных ставок. В числе примеров рыночного риска можно назвать процентный, валютный и фондовый риски;

♦ риск ликвидности заключается в возможном невыполнении компанией своих текущих обязательств по платежам;

♦ риск контроля связан с техникой отчетов, внешним аудитом, надежностью автоматических платежей и т.п

♦ операционный риск — риск того, что потери могут возникнуть из-за ошибок или пропусков в обработке документов и расчетах. Этот риск включает риск возможного мошенничества, коммуникационный и организационный риски;

♦ риск потери репутации банка, который возникает из операционных сбоев, неспособности действовать в соответствии с определенными законами и инструкциями либо другими источниками права [5].

Два последних, типично банковских вида риска, наиболее важных для рассматриваемой в данной книге темы, анализируются в следующем разделе.

По мере развития конкуренции, освоения отечественными банками новых сфер деятельности и рыночных инструментов, расширения и углубления внешнеэкономических связей риски в бизнесе будут возрастать, появятся новые виды рисков. Между тем российская хозяйственная практика последних лет дает немало примеров негативных последствий, обусловленных не-

вниманием к этой стороне деятельности, непониманием ее значения (банкротства, крупные финансовые потери на внутреннем и внешних рынках, упущенная выгода и пр.). Управление рисками как область знаний находится на стыке различных отраслей знаний, требует использования методов математического моделирования, прогнозирования, применения элементов финансового и стратегического планирования.

Управление рисками обычно включает следующие направления деятельности:

- идентификацию угроз, анализ и оценку рисков;
- кризисное управление (ликвидация последствий возникающих убытков, выработка механизмов выживания);
- систему страховых превентивных мероприятий (минимизация и предупреждение риска). Эти мероприятия детально отработаны в зарубежных банках [7, 8].

Например, анализ риска предполагает выявление его источников (собственно хозяйственный риск; риск, связанный с личностью человека; риск, обусловленный природными факторами; системный риск) и его причин (риски, связанные с неопределенностью будущего, непредсказуемостью поведения партнеров, недостатками информации и пр.), прогнозирование уровня потерь. Неоднородность сферы деятельности банка и его предприятий делает объективно необходимым конкретизацию стратегий кризисного управления, побуждает разрабатывать различные концепции информационной безопасности в зависимости от размеров организации (малый, средний, крупный бизнес), сфер деятельности (финансовая, банковская, производственная, внешнеторговая и пр.), национальных и региональных особенностей. Таким образом, *анализ риска* — это процесс получения количественной оценки ущерба, который может произойти в случае реализации угрозы безопасности.

Анализ рисков включает определение того, что нужно защищать, от чего защищаться и как защищаться. Для этого надо определить все, чем оцениваются риски, и ранжировать их по уровню важности. Этот процесс включает принятие экономичных решений о необходимых методах и средствах защиты, так как средства, выделяемые на защиту, не должны превышать стоимости защищаемого объекта. Полное рассмотрение анализа риска находится за пределами данной работы. Тем не менее следует рассмотреть два важных элемента анализа риска:

⇒ определение ценности или классификация информационных ресурсов;

⇒ выявление угроз информации.

Определение ценности или классификация информационных ресурсов может проводиться только в условиях конкретной автоматизированной информационной системы с применением стоимостного критерия. При этом помимо ценности и важности информации целесообразно рассматривать необходимое время существования ее выбранной категории (грифа) ограничения доступности. Общее выявление угроз информации в автоматизированных банковских системах будет кратко рассмотрено в следующем разделе. Подробный анализ рисков для различных автоматизированных информационных систем и их средств приведен в работах [4, 7, 8, 13, 14].

2.2. АНАЛИЗ УГРОЗ

Прежде всего целесообразно уточнить основные качества или свойства информации, которые подвергаются воздействию угроз. При достижении безопасности информации базовыми задачами являются обеспечение ее доступности, конфиденциальности, целостности и юридической силы (значимости). Каждая угроза должна рассматриваться с точки зрения того, как она может затронуть эти четыре свойства или качества безопасной информации.

Конфиденциальность означает, что информация ограниченного доступа должна быть досягаема только тому, кому она предназначена. Под целостностью информации понимается ее свойство существования в неискаженном виде. Доступность информации определяется способностью системы обеспечивать своевременный беспрепятственный доступ к информации субъектов, имеющих на это надлежащие полномочия.

Юридическая сила или значимость информации приобретает важность в последнее время, вместе с созданием нормативно-правовой базы безопасности информации в нашей стране [3, 10-12]. Последнее, например, актуально при необходимости обеспечения строгого учета любых информационных услуг, который является экономической основой работы всякой информационной системы и служит для соблюдения жесткой регламентации и регистрации доступа к информации при пользова-

нии информационными ресурсами системы. Помимо этого часто должна обеспечиваться строгая нотаризация (юридически значимая регистрация) информации, которая необходима при разборе любых конфликтов между заказчиками и исполнителями работ по информационному обслуживанию.

Для определенности рассмотрим конкретные примеры угроз [28]. Можно выделить следующие группы потенциально вероятных угроз для банковских автоматизированных комплексов или ТКС финансово-кредитной сферы, обрабатывающих конфиденциальную информацию, которая не является государственной тайной (табл.1).

Таблица 1

Природные	Технические	Непосредственно созданные людьми
Стихийные бедствия Магнитные бури Радиоактивное воздействие	Пропажа или колебания электропитания и других средств обеспечения функционирования Отказы и сбои аппаратно-программных средств Электромагнитные излучения и наводки Утечки через каналы связи (оптические, электрические, звуковые) и т.п.	*Непреднамеренные действия:* обслуживающего персонала управленческого персонала программистов пользователей АС архивной службы службы безопасности *Преднамеренные действия:* обслуживающего персонала управленческого персонала программистов пользователей АС архивной службы службы безопасности несанкционированных пользователей (коммерческий шпионаж, диверсии)

Мировой опыт и статистический анализ случаев компьютерных преступлений в банковской сфере показывает, что [28]:

кража денег — 36%;

кража услуг — 34%;

кража информации — 12%;
подделка данных — 8%;
вымогательство — 4%;
нанесение ущерба программам — 2%;
нанесение ущерба оборудованию — 2%;
помехи нормальной работе — 2%.

Компьютерные преступления — это один из видов реализации угроз безопасности информации.

В работах [4, 13, 14] подробно анализируются угрозы и финансовый ущерб от их воздействия на различные автоматизированные системы современных информационных технологий. Часть этих материалов изображена на рис.8-10.

Обобщая данные анализа, можно констатировать превалирование вероятности реализации случайных угроз над преднамеренными. При этом финансовый ущерб реализации преднамеренных угроз превышает потери от реализации случайных угроз, поэтому сосредоточим свое внимание на первых.

На основании рекомендаций Международной организации стандартизации (ISO) для банковских систем классификацию угроз предлагается произвести по следующим критериям: цели реализации угроз и способу их воздействия. Данные критерии в конечном итоге позволяют определить механизмы угроз для каждого технического средства банковской системы и реализовать необходимые меры защиты.

Угрозы по цели реализации включают в себя:

• нарушение конфиденциальности информации (информация, хранимая и обрабатываемая в системе имеет большую ценность и ее несанкционированное использование может нанести значительный ущерб);

• нарушение целостности информации (информация может быть утрачена вследствие ее несанкционированного удаления либо модификации);

• нарушение работоспособности системы (несанкционированное и некорректное изменение режимов работы компонентов системы, их модификация либо ложная подмена могут привести к получению неверных результатов, отказу системы от обработки потока информации или значительным задержкам ее доставки, а также отказам в обслуживании).

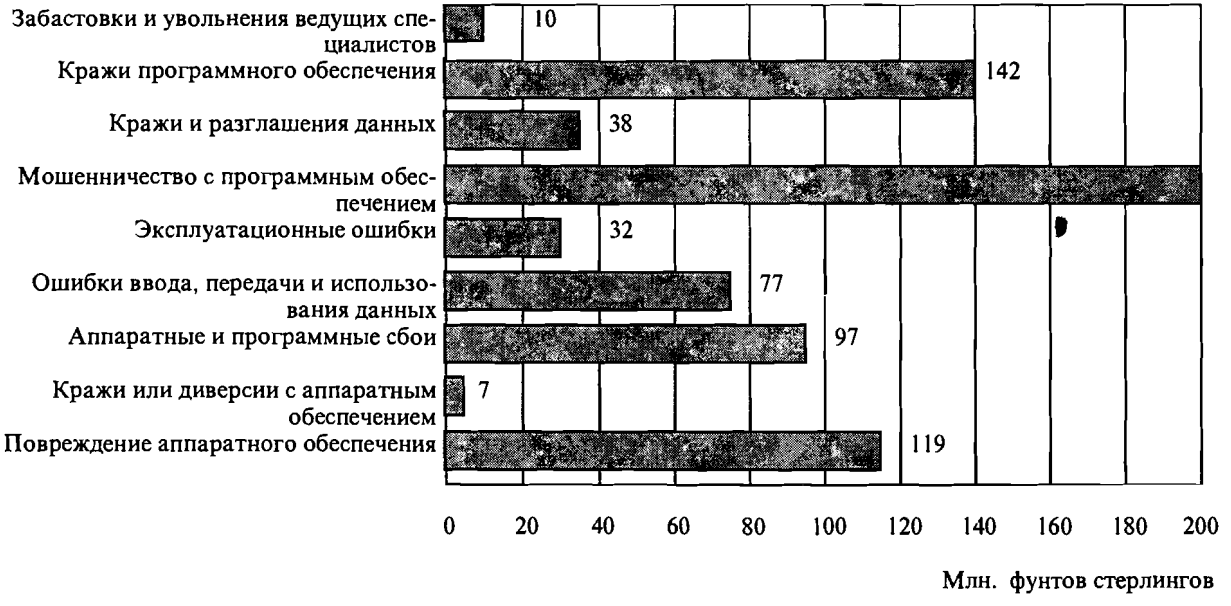

Рис.8. Потери Франции из-за инцидентов с информационной технологией (по данным фирмы Coopers & Lybrand)

Рис.9. Основные причины убытков североамериканских компаний, пренебрегающих защитой данных (Ernst&Young)

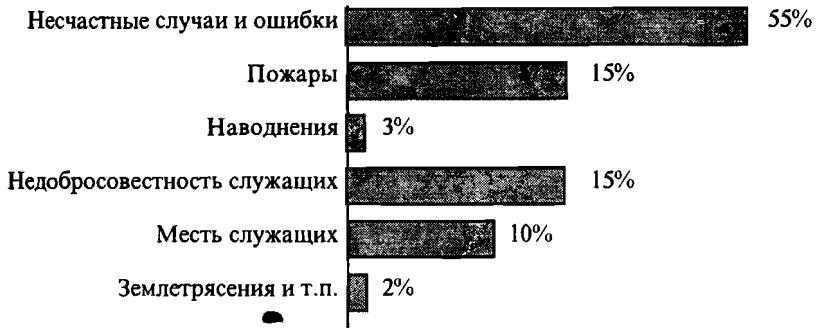

Рис.10. Вероятности угроз безопасности информационным технологиям (по данным фирмы Executive Information Network)

По способу воздействия на объект угрозы включают:

непосредственное воздействие на объект атаки, например, непосредственный доступ к набору данных, программе, как в результате ошибки, так и преднамеренно;

воздействие на систему разграничения полномочий и разрешений (в том числе захват привилегий). При этом способе несанкционированные действия выполняются относительно прав пользователей, а сам доступ к объекту осуществляется впоследствии законным путем;

опосредованное воздействие (через других пользователей);

"маскарад", когда пользователь присваивает себе каким-либо образом полномочия другого пользователя;

"использование вслепую", когда один пользователь заставляет другого выполнить необходимые действия, причем последний о них может и не подозревать. Для реализации этой угрозы может использоваться "компьютерный вирус" либо "программная закладка".

По отмеченным критериям относительно банковской системы Российской Федерации в зависимости от используемых технических средств угрозы могут иметь различные формы проявления.

По используемым в банковской системе техническим средствам угрозы могут быть систематизированы в отношении:

оборудования пользователя (должностных лиц, операторов), на котором производится "ручное" формирование (подготовка) электронных платежных документов (ЭПД) и их обработка;

оборудования локальных вычислительных сетей и технических средств, выполняющих централизованную автоматизированную обработку ЭПД, поступающих с рабочих мест пользователей;

оборудования транспортной сети, обеспечивающего передачу ЭПД по каналам связи.

Угрозы, связанные непосредственно с оборудованием пользователя (ПЭВМ, АРМ, терминалами), их программным обеспечением, могут включать в себя:

чтение информации с экрана посторонним лицом (во время отображения информации на экране законным пользователем или при отсутствии законного пользователя на рабочем месте);

чтение информации из оставленных без присмотра распечаток либо черновых бумаг;

хищение носителей информации (магнитных дисков, магнитных лент, дискет, карт);

подключение к устройствам ПЭВМ либо к ее составным частям (платам, блокам) специально разработанных аппаратных средств, копирующих информацию или программное обеспечение, с последующим снятием;

использование специальных технических средств для перехвата электромагнитных излучений от ПЭВМ, терминалов, АРМ;

несанкционированный доступ к ПЭВМ, ее операционной системе и программному обеспечению, к терминалу;

копирование информации из электронной памяти посторонним лицом;

нарушение конфиденциальности информации при ее хранении;

нарушение целостности информации посторонним лицом;

несанкционированное стирание информации из архива до истечения срока ее хранения;

несанкционированное копирование, модификация, уничтожение программного обеспечения;

хищение носителей ключевой и парольной информации либо их несанкционированное копирование;

несанкционированное копирование ключевой и парольной информации из оперативной памяти ЭВМ;

несанкционированное обращение к базам данных.

В пределах вычислительной сети комплекс угроз затрагивает оборудование "общей шины", центральный процессор, сервер и может включать в себя следующие механизмы:

- в рамках общей доступности ПЭВМ возможно нарушение конфиденциальности информации, т.е. ее передача без шифрования либо переадресация;
- перехват информации при ее передаче по соединительным линиям либо общей шине;
- извлечение открытой, либо зашифрованной информации при ее промежуточном хранении в технических средствах обработки и коммутации (файл-сервере, центральном сервере, центральной вычислительной машине и т.д.);
- уничтожение (стирание) открытой, зашифрованной информации при долговременном хранении в центрах обработки;
- копирование информационного обеспечения, в том числе маршрутно-адресных таблиц, средств коммутации;
- несанкционированный доступ к СУБД;
- модификация маршрутно-адресной информации.

Данный комплекс угроз требует трансформации программного обеспечения (включения программных закладок) либо применения специальной аппаратуры.

Следует отметить, что приведенный комплекс угроз в отношении оборудования пользователя и вычислительной сети, за исключением угроз, связанных с электромагнитным излучением, возможен лишь со стороны работников банковских учреждений при их несанкционированных действиях, либо со стороны разработчиков программно-технических средств, преднамеренно использующих программно-аппаратные закладки.

Механизмы угроз в транспортной сети возникают ввиду наличия внешних и внутренних угроз к сообщениям, а при хранении информации на центрах переприема — угроз к хранилищу данных.

Внешние угрозы сообщениям исходят от несанкционированных пользователей со стороны канала связи и могут проявляться следующим образом:

- перехватом сообщений;
- модификацией сообщений;
- повторным воспроизведением сообщений;
- уничтожением сообщений;
- формированием ложных сообщений;

■ переадресацией сообщений;

■ анализом трафика, с целью раскрытия характера и объема передаваемых данных, частоты передачи и т.п.

Целью комплекса внешних угроз является дезорганизация работы сети, включая навязывание ложной информации пользователю при приеме или создание эффекта "затруднения" связи.

Механизмы внутренних угроз сообщениям исходят от самих абонентов конфиденциальной связи и могут проявляться следующими способами:

♦ отрицание сообщений — один из абонентов может отрицать свое участие в обмене;

♦ нарушение уровня защиты (при условии, что в системе используются различные уровни секретности).

Внутренние угрозы приводят к возникновению конфликтов, причинами которых являются неполучение, сокрытие информации от другого корреспондента, передача ее самому себе.

Угрозы к хранилищу данных возникают в оборудовании транспортной сети (в центрах коммутации пакетов/сообщений) при реализации режима отложенной доставки информации пользователю и включают в себя:

• модификацию маршрутизации информации, когда несанкционированные изменения содержимого справочника могут привести к неправильной маршрутизации сообщений или их потере;

• модификацию адресной части хранимого сообщения, которая приводит к упомянутым выше последствиям;

• несанкционированный доступ к сообщениям;

• преждевременное воспроизведение, когда несанкционированный пользователь создает копию сообщения задержанной доставки и посылает эту копию заданному получателю, пока оригинал еще удерживается для доставки. Преждевременное получение сообщения либо его двукратное получение может запутать получателя.

Рассмотренный комплекс угроз к хранилищу данных требует защиты от несанкционированной модификации сетевого и системного программного обеспечения в транспортной ПЭВМ, а также защиты от НСД к хранящимся сообщениям. Из этого следует, что в комплексе угроз при подготовке, формировании, обработке и передаче электронных платежных документов

весьма значительную часть составляют угрозы, связанные с несанкционированным изменением и использованием программного обеспечения. Для реализации данного комплекса угроз могут быть использованы следующие основные механизмы взлома программного обеспечения, основанные на применении "вредоносных программ" типа: "троянский конь", "червь", вирус "жадная" программа, захватчик паролей.

Краткие характеристики вредоносных программ следующие:

"троянский конь" выполняет совместно с основными дополнительные, но не указанные в документации, действия;

"вирус" может "заражать" другие программы путем включений в них своей, возможно модифицированной копии, причем последняя сохраняет способность к дальнейшему размножению;

"червь" распространяется через сеть с целью дезорганизации работы узлов связи и не оставляет своих копий на магнитном носителе;

"жадные" программы стремятся монополизировать какой-либо ресурс системы, не давая другим программам возможности реализации;

"захватчики паролей" предназначены для воровства паролей. Они делают пустым экран терминала, что бывает после НСД, либо останова системы, либо окончания сеанса работы. При попытке входа имитируется ввод имени и пароля, которые пересылаются к владельцу программы-захватчика, после чего выводится сообщение об ошибке ввода и управление возвращается операционной системе. Пользователь, думающий, что допустил ошибку при наборе пароля, повторяет вход и получает доступ к системе. Однако его имя и пароль уже известны владельцу программы-захватчика.

Из приведенного обобщенного перечня угроз, которые могут иметь место в банковских системах, видно их многообразие, разные места и способы воздействия. На данном перечне угроз основаны требования к защите банковской информации.

Одними из основных и основополагающих документов в части требований защиты информации являются Рекомендации ISO 7498-2-89 и Стандарты МККТТ/ISO для безопасной обработки сообщений (Рекомендации серий X.400, X.500 МККТТ). Стандарты и рекомендации для безопасной передачи, приема и

обработки сообщений в системе определяют следующие принципы защиты информации:

конфиденциальность содержания (позволяет отправителю быть уверенным, что никто не прочитает сообщения, кроме определенного получателя);

целостность содержания (позволяет получателю убедиться, что содержание сообщения не модифицировано);

целостность последовательности сообщений (позволяет получателю убедиться в том, что последовательность сообщений не изменена);

аутентификация источника сообщений (отправитель получает возможность аутентифицироваться у получателя как источник сообщения, а также у любого устройства передачи сообщений, через которое они проходят);

доказательство доставки (отправитель может убедиться в том, что сообщение доставлено неискаженным нужному получателю);

доказательство подачи (отправитель может убедиться в идентичности устройства передачи сообщения, на которое оно было подано);

безотказность источника (позволяет отправителю доказать получателю, что переданное сообщение принадлежит ему);

безотказность поступления (позволяет отправителю сообщения получить от устройства передачи сообщения, на которое оно поступило, доказательство того, что сообщение поступило на это устройство для доставки определенному получателю);

безотказность доставки (позволяет отправителю получить от получателя доказательство получения им сообщения);

управление контролем доступа (позволяет двум компонентам системы обработки сообщений установить безопасные соединения);

защиту от попыток расширения своих законных полномочий (на доступ, формирование, распределение и т.д.), а также изменения (без санкции на то) полномочий других пользователей;

защиту от модификация программного обеспечения путем добавления новых функций.

Исходя из статистических материалов, приведенных в начале раздела, можно сделать вывод, что максимальную угрозу для АСБР, как разновидности АБС, представляют непреднаме-

ренные и преднамеренные действия персонала банка. Причинами таких действий являются халатность, некомпетентность, самоутверждение и корыстные цели. Первые три причины на практике часто переплетаются и трудно разделимы. По различным данным большую часть всех нарушений представляют неумышленные ошибки персонала. Злонамеренные воздействия случаются реже, но несут больший финансовый ущерб. Статистика компьютерных преступлений в банковской сфере указывает на преимущественное участие в осуществлении НСД к информации в АБС (от 75 до 90% случаев) самих работников банков [16]. Естественно, что максимальный ущерб могут нанести высококвалифицированные специалисты, имеющие непосредственный доступ, с наибольшими полномочиями, к средствам АСБР. Перечисленные факторы обычно учитывают при разработке модели потенциального нарушителя и оценки степени риска. Разработка модели нарушителя — это определение субъекта, потенциально совершающего несанкционированные действия.

При обосновании модели нарушителя обычно определяют:

- категории лиц, в числе которых может оказаться нарушитель;
- возможные цели нарушителя и их градация по степени предполагаемого ущерба;
- оценку квалификации и технической вооруженности нарушителя;
- ограничение и предположения о характере действий нарушителя.

Для рассматриваемых систем обычно нарушители делятся на следующие категории:

- зарегистрированные пользователи системы;
- сопровождающий и обслуживающий персонал (инженеры, подсобные рабочие, уборщицы и т.д.);
- посторонние лица (не принадлежащие к указанным категориям).

Во всех технологически сложных системах (АСБР безусловно, относятся к таким) время от времени возникают нештатные ситуации, связанные со сбоями или отказами технических средств. Поэтому потенциально существуют угрозы того, что злоумышленники могут воспользоваться побочными результа-

тами этих нештатных ситуаций (например, потерями или искажениями файлов, раскрытием секретных кодов и т.п.).

2.3. ТРЕБОВАНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Успешному решению проблем обеспечения информационной безопасности в автоматизированных системах кредитно-финансовых учреждений (банков), к которым относится любая АСБР, предшествует точная постановка цели и задач ее достижения [27].

Как отмечалось ранее, информационная безопасность АСБР не является самоцелью и ее обеспечение необходимо для снижения рисков и экономических потерь, связанных с всевозможными угрозами информационным ресурсам автоматизированной системы.

В кредитно-финансовой сфере для обеспечения информационной безопасности автоматизированной системы необходимо поддерживать главные свойства или качества безопасной информации: доступность, конфиденциальность, целостность и юридическую значимость. Определения этих понятий изложены в приложении 1. Практическая реализация последнего качества осложнена незавершенностью становления отечественной нормативно-правовой базы по защите информации. Например, 01.01.97 вступили в силу статьи нового Уголовного кодекса, предусматривающие ответственность за компьютерные преступления. Только в 1996 г. вступил в действие ГОСТ Р 50739-95, с учетом которого следует проводить анализ и выбор средств зашиты информации [21].

Также необходимо выполнять положения нормативно-методических документов двух государственных организаций — ГОСТЕХКОМИССИИ и ФАПСИ, которые организуют в нашей стране деятельность по защите информации. Поэтому выбор и эксплуатацию средств защиты информации для кредитно-финансовой сферы целесообразно проводить на основе сертификатов продукции и лицензий на вид деятельности, которые определены Положением о лицензировании деятельности в области защиты информации [34]. В любом случае комплексное обеспечение информационной безопасности АСБР начинается с учета положений ряда документов упомянутых

государственных организаций [21-26, 30-32]. Эти документы определяют общие требования по защите информации. Конкретную практическую реализацию системы защиты информации от несанкционированного доступа целесообразно проводить, руководствуясь требованиями документа "ВРЕМЕННЫЕ ТРЕБОВАНИЯ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ТЕХНОЛОГИЙ ОБРАБОТКИ ЭЛЕКТРОННЫХ ПЛАТЕЖНЫХ ДОКУМЕНТОВ В СИСТЕМЕ ЦЕНТРАЛЬНОГО БАНКА РОССИЙСКОЙ ФЕДЕРАЦИИ", который был введен приказом [6].

В настоящее время данный документ является единственным в своем роде кратким сводом основных требований по практическому построению комплексной системы информационной безопасности отечественного автоматизированного банка. При этом следует отметить, что этот документ предназначен для весьма специфического государственного банка и его положения могут использоваться в других автоматизированных банках с учетом их особенностей. Аналогичным по детализации и практической направленности является ведомственный документ «Требования к заявителю на право установки (инсталляции), эксплуатации сертифицированных ФАПСИ шифровальных средств и предоставления услуг по шифрованию информации при защите информации по уровню "С". 1996», который предназначен для потребителей криптографических средств защиты информации [26].

Опираясь на требования упомянутого документа ЦБ РФ, которые разработаны в соответствии с положениями федеральных законов, нормативных и иных актов Банка России, Гостехкомиссии и ФАПСИ, целесообразно кратко выделить его основные положения. В первом разделе общую важность представляют организационные требования. Например, привлекаемые для разработки, установки и ремонта средств и систем защиты электронных платежных документов на договорной основе специализированные организации должны иметь государственные лицензии от Гостехкомиссии, ФАПСИ и других государственных органов в соответствии с российским законодательством.

Используемые при этом средства защиты информации от несанкционированного доступа (НСД) должны иметь сертификат Гостехкомиссии. Криптографическая защита электронных пла-

тежных документов обеспечивается на основе использования средств криптографической защиты информации (СКЗИ), имеющих сертификат или временное разрешение ФАПСИ.

Следует специально отметить, что основное внимание в указанных временных требованиях ЦБ РФ уделяется защите электронных платежных документов, которые выделены в названии из всего документооборота банка [6].

Обязанности по администрированию программно-технических средств защиты электронных платежных документов для каждого технологического участка прохождения этих документов возлагаются приказом по участнику электронных платежей на сотрудников (сотрудника), задействованных на данном технологическом участке (администраторов информационной безопасности), с внесением соответствующих изменений в их должностные обязанности.

Второй раздел упомянутых требований посвящен обеспечению информационной безопасности при внедрении и эксплуатации систем обработки электронных платежей и начинается с требований к технологическим мерам защиты:

процесс обмена электронными платежными документами между участниками электронных платежей и кредитными организациями (клиентами) должен быть регламентирован и осуществляется в соответствии с заключенными договорами;

основанием для ввода электронного платежного документа (не подтверждаемого первичным документом на бумажном носителе) в систему электронных платежей является наличие под документом действующей и зарегистрированной (в соответствии с условиями договора) ЭЦП кредитной организации (клиента) — отправителя документа — и положительный результат ее проверки;

все поступающие от кредитных организаций электронные платежные документы с ЭЦП помещаются в архив и хранятся не менее пяти лет;

поступающие от кредитных организаций (клиентов) магнитные носители с электронными платежными документами до ввода в систему электронных платежей подвергаются антивирусному контролю на выделенной для этого автономной персональной электронно-вычислительной машине (ПЭВМ);

ввод платежных документов в систему электронных платежей должен сопровождаться формированием эталонной базы,

содержащей входящие электронные платежные документы с ЭЦП, для осуществления контроля выходных документов.

Далее идут сугубо специализированные правила прохождения электронных платежных документов по системе Банка России, которые касаются, например, кода аутентификации, представляющего собой защитный код, проставляемый при создании файла электронных платежных документов в целях осуществления контроля его целостности и авторизации на последующих технологических участках обработки. Также должен быть реализован полный пореквизитный контроль на совпадение выходных электронных платежных документов с документами, содержащимися в эталонной базе входящих электронных платежных документов, и их сверка с реквизитами соответствующих документов, отраженных по балансу. Указанный контроль выходных электронных платежных документов должен быть организован как параллельный независимый процесс по отношению к процессу обработки электронных платежных документов и осуществляться на автоматизированном рабочем месте контроля.

Помимо этого особое внимание уделено регламентации технологических процессов подготовки, ввода и обработки электронных платежных документов, а также установке, настройке, эксплуатации и восстановлению средств обработки, в том числе программного обеспечения и его контролю целостности. При этом порядок действий администраторов информационной безопасности и персонала, занятых в системах обработки и передачи электронных платежных документов, должен быть регламентирован.

Особо выделены вопросы формирования уникальных идентификаторов, организации парольной защиты, установления и изменение полномочий, а также контроль доступа пользователей ЭВМ и/или ЛВС к электронным платежным документам и информации о них. Для примера в приложении 3 приводится выдержка из рассматриваемых временных требований ЦБ РФ, которая посвящена организации парольной защиты. Заканчивается раздел требованиями по регистрации действий пользователя в специальном электронном журнале, доступном только администратору информационной безопасности. Копия журнала должна храниться не менее пяти лет. Перечень необходимых параметров регистрации должен включать в себя:

- время входа (выхода) в систему и идентификатор пользователя;
- факт обращения к ПО обработки электронных платежных документов;
- факты попыток НСД;
- информацию о сбоях и других нештатных ситуациях.

Сходные требования, соответствующие заглавиям, изложены в разделах "Обеспечение информационной безопасности при передаче электронных платежных документов", "Обеспечение защиты помещений и технических средств" и "Обеспечение информационной безопасности при использовании криптографических средств защиты". Они аналогичны требованиям ФАПСИ, представленным в приложении 2.

Завершается документ разделом "Контроль за обеспечением безопасности технологии обработки электронных платежных документов", в котором определено, что контроль должен осуществляться в рамках всего комплекса технологических, организационных, технических и программных мер и средств защиты на этапах подготовки, обработки передачи и хранения электронных платежных документов.

В приложении к требованиям представлены типовые формы следующих документов:

"Примерное положение об администраторе информационной безопасности";

"Примерное положение об администраторе информационной безопасности расчетно-кассового центра";

"Типовой паспорт программного обеспечения автоматизированного рабочего места";

"Требования к организации парольной защиты автоматизированной системы участника электронных платежей".

В любом случае большое внимание необходимо уделять подробному и всестороннему документированному описанию конкретных требований информационной безопасности, изложенных в эксплуатационной документации на средства защиты. Необходимо, в соответствии с ГОСТ Р 50739-95: "ГОСУДАРСТВЕННЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования", руководствоваться положениями рабочей документации, включающей в себя:

- руководство пользователя;
- руководство по комплексу средств защиты;
- тестовую документацию;
- конструкторскую (проектную) документацию.

В упомянутых эксплуатационных документах приводятся минимально необходимые требования по защите для конкретного средства защиты информации, что предполагает наличие дополнительных или специфических требований для каждого объекта информатики. Как правило, комплексная защита АСБР строится на основе средств криптографической защиты информации (СКЗИ). Для совместимости и унификации в системе обычно используются одни и те же СКЗИ.

В любом случае практической реализации перечисленных требований необходимо соблюдать ОСНОВНЫЕ ПРИНЦИПЫ комплексной ЗАЩИТЫ информации в автоматизированных системах (АС), которые изложены в документе [22] и включают следующие положения:

- защита информации в средствах вычислительной техники (СВТ) и АС основывается на положениях и требованиях существующих законов, стандартов и нормативно-методических документов по защите от несанкционированного доступа (НСД) к информации;
- защита СВТ обеспечивается комплексом программно-технических средств;
- защита АС обеспечивается комплексом программно-технических средств и поддерживающих их организационных мер;
- защита АС должна обеспечиваться на всех технологических этапах обработки информации и во всех режимах функционирования, в том числе при проведении ремонтных и регламентных работ;
- программно-технические средства защиты не должны существенно ухудшать основные функциональные характеристики АС (надежность, быстродействие, возможность изменения конфигурации АС);
- неотъемлемой частью работ по защите является оценка эффективности средств защиты, осуществляемая по методике, учитывающей всю совокупность технических характеристик оцениваемого объекта, включая технические решения и практическую реализацию средств защиты;

• защита АС должна предусматривать контроль эффективности средств защиты от НСД. Этот контроль может быть либо периодическим, либо инициироваться по мере необходимости пользователем АС или контролирующими органами.

Перечисленные мероприятия направлены в основном на компенсацию воздействия преднамеренных угроз безопасности информации, которые наносят максимальный финансовый ущерб АС финансово-кредитной сферы (см. предыдущий раздел). При этом следует помнить, что максимальная вероятность проявления непреднамеренных (случайных) угроз безопасности информации. Подтверждением этого являются материалы фирмы DEC для автоматизированных банков [4, 27].

Фирма DEC оснастила и обслуживает около 70% всех электронных банков в мире, предлагая комплексные услуги по разработке, поставке и техническому сопровождению АБС. Обобщая большой и разнообразный опыт создания и эксплуатации АБС, фирма DEC обращает значительное внимание на среду или условия функционирования СВТ, как составной части комплексного обеспечения безопасности информации. В материалах этой фирмы, помимо проблем защиты от несанкционированного доступа, упомянуты проблемы внешних воздействий среды функционирования АБС.

Физические факторы среды функционирования включают:

• расположение или размещение АБС;

• климатические воздействия на систему и ее элементы (температура, влажность и загрязнение воздушной массы);

• механические воздействия на технические средства (удары и вибронагрузка).

Электрические факторы среды функционирования включают:

• качество и надежность электропитания системы;

• заземление оборудования;

• электромагнитные помехи.

Целесообразно более подробно остановиться на электрических факторах среды функционирования АБС и ее элементов, так как они представляют несомненную угрозу безопасности информации при несоблюдении определенных стандартизированных правил и условий (см. следующие разделы). Соблюдение этих правил и условий позволяет одновременно решать проблемы раскрытия информации из-за утечки по каналам

электромагнитных излучений и наводок и обеспечивает безотказное функционирование АБС при различных флуктуациях в сети электропитания. Одновременное решение различных проблем с помощью единых средств существенно снижает затраты по защите информации. В материалах фирмы DEC уделено внимание правильной установке и обслуживанию СВТ системы, хранению и использованию носителей информации. Рассматриваются меры по защите АБС от стихийных бедствий и мероприятия по физической безопасности системы.

Рассмотрим эти положения на конкретных примерах. С развитием мобильных средств электросвязи (радиотелефон) повсеместно в развитых странах стали отмечаться случаи негативного воздействия мощных электромагнитных полей связных передатчиков на близко расположенную вычислительную технику, которые выражались в сбоях или неустойчивой работе ЭВМ. В результате Международная электротехническая комиссия (МЭК) выпустила стандарт МЭК 801/1000-4, распространяющий свои требования на радиоэлектронные и электронные изделия, которые могут в условиях эксплуатации подвергаться воздействию радиочастотных электромагнитных полей. Отечественным аналогом этого стандарта является ГОСТ Р50008-92 "Совместимость технических средств электромагнитная. Устойчивость к радиочастотным электромагнитным полям в полосе 26-1000 МГц. Технические требования и методы испытаний". Основным средством защиты от подобных воздействий или электромагнитных помех служит электромагнитное экранирование, одновременно решающее проблемы защиты информации, которая распространяется или раскрывается за счет электромагнитных излучений на экране монитора.

Знание требований документа РД 50 714-92 "Уровни электромагнитной совместимости в низковольтных системах электроснабжения общего назначения в части низкочастотных кондуктивных помех и сигналов, передаваемых по силовым линиям" позволяет квалифицированно эксплуатировать СВТ электронной банковской системы, устойчиво работающее при электропитании от отечественных силовых электросетей.

Исследование нескольких отечественных питающих сетей показали, что относительное время аварийной работы сетей электропитания составляет до 10%. По видам нарушений картина следующая: падение напряжения за пределы допустимых

значений — 50%, повышение напряжения — 10%, отключение питания — 20%, броски напряжения — 5%. Самыми опасными являются кратковременные высоковольтные броски напряжения, обычно возникающие из-за отключения индуктивной нагрузки. Учитывая указанные обстоятельства, для всех отечественных АБС целесообразно использовать источники бесперебойного питания или Uninterruptable power supply (UPS), которые обеспечивают защиту от данных нарушений. Это весьма важно для оборудования АСБР. Следует учесть, что при авариях в электросетях UPS обеспечивают качественное электропитание в течение нескольких минут, необходимых для успешного завершения вычислительного процесса и создания условий для его последующего восстановления. Для компенсации негативных последствий более длительных аварий необходимо применять более радикальные средства, например, дизель-генераторы.

Обычно не вызывает сомнений необходимость качественного заземления технических средств АБС или АСБР, что является не простой проблемой.

В материалах фирмы DEC также уделено внимание правильной установке и обслуживанию СВТ системы, хранению и использованию носителей информации. Рассматриваются меры по защите АБС от стихийных бедствий и мероприятия по физической безопасности системы. Выделяя главные угрозы безопасности информации АБС при случайных воздействиях, следует рассмотреть ряд технических решений, которые часто применяются для повышения безотказности функционирования сложных систем.

Основным условием устойчивой работы оборудования АБС любого класса является обеспечение гарантированного электропитания. Особенно важно это для регионов с неустойчивым электроснабжением и регионов с большими рисками финансового ущерба при реализации этих угроз (см. разд.1).

На сегодняшний день существуют два основных подхода к построению системы защиты от сбоев в электропитании. Первый предполагает установку отдельных блоков гарантированного питания для каждого компьютера системы или хотя бы только для сервера. Преимущества этого подхода заключаются в возможности постепенного наращивания количества таких блоков, простоте обслуживания и ремонта, а также в сохране-

нии работоспособности всей сети при выходе из строя одного из блоков. Второй подход состоит в установке центрального блока электропитания. При этом для его размещения можно выбрать самое удобное и защищенное место, управление им поддерживается по специальному протоколу. К недостаткам данного подхода можно отнести необходимость прокладки отдельной сети питания внутри зданий, а само устройство должно обладать запасом мощности для подключения компьютеров на случай расширения сети. Кроме того, выход из строя блока гарантированного питания приводит к остановке всех компьютеров сети.

Другой серьезной угрозой является остановка сервера. Сервер является ответственным элементом любой вычислительной сети. Одна из важнейших функций сервера — хранение информации и обеспечение доступа к ней пользователей сети. Поэтому в современных серверах и операционных системах предусматриваются возможности программного или аппаратного дублирования накопителей на жестких магнитных дисках.

Аппаратное дублирование заключается в использовании специальных контроллеров для построения массивов недорогих резервных дисков (Redundant Array of Independent Disks — RAID). С помощью таких контроллеров также можно строить массивы, в которых есть два симметричных (дублирующих) набора.

Аппаратура RAID-контроллера и архитектура большинства серверов позволяют заменять диски, не выключая сервер, а алгоритмы обеспечивают восстановление информации на ходу: сервер продолжает работать, а контроллер восстанавливает информацию на диске, установленном вместо вышедшего из строя.

Даже при наличии средств обеспечения доступности оперативной информации, которая хранится на жестких дисках сервера, рекомендуется сделать ее резервную копию на сменных носителях. Сегодня технология создания резервных копий предлагает множество вариантов. Простейший из них состоит в сохранении полной копии рабочих дисков сервера на магнитных лентах (современные накопители такого типа позволяют хранить до 20 Гбайт информации на одной кассете).

Повышенные требования к устойчивости работы АСБР определяются постоянным режимом его функционирования

(часто круглосуточная и безостановочная работа). Поэтому возникает проблема построения систем, самостоятельно распределяющих нагрузку внутри себя, в том числе при отказе одного из серверов. Такие системы существуют, правда, при этом приходится платить временем, которое система затрачивает на свою внутреннюю реконфигурацию. Основными признаками таких систем являются:

- ♦ единство системы (с точки зрения пользователя);
- ♦ многомашинный комплекс;
- ♦ высокая надежность;
- ♦ общая файловая система;
- ♦ наращиваемость;
- ♦ гибкость конфигурирования;
- ♦ единое управление (администрирование).

Наиболее полно этим требованиям отвечает, например, комплекс, управляемый сертифицированными операционными системами VMS или Open VMS фирмы Digital.

Перечисленные свойства позволяют строить многомашинные комплексы, в которых при нормальном режиме работы производительность каждого сервера суммируется с остальными. Однако в случае отказа одного из серверов его функции автоматически перераспределяются между работоспособными компьютерами (время задержки составляет доли секунды). Именно благодаря комплексу VMS крупнейшие банки Сан-Франциско смогли продолжить свою работу после сильнейшего землетрясения.

Вышеизложенное позволяет с достаточной степенью детализации рассмотреть практические вопросы построения и эксплуатации системы защиты информации на примере программно-аппаратного СКЗИ "Янтарь АСБР". Ранее отмечалось, что криптографические средства обеспечения безопасности информации являются основой создания подсистем защиты данных автоматизированных банковских систем.

3. СРЕДСТВО КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ "ЯНТАРЬ АСБР"

3.1. НАЗНАЧЕНИЕ

Программно-аппаратное средство криптографической защиты информации "Янтарь АСБР", построенное на основе комплекса криптографических средств защиты информации "Янтарь" и предназначенное для защиты передачи конфиденциальной информации в АСБР, имеет сертификат ФАПСИ № СФ/124-0187 по уровню безопасности информации "С". Указанный уровень безопасности используется для обеспечения защиты информации, не содержащей сведений, составляющих государственную тайну. При этом обеспечение безопасности информации по уровню "С" означает криптографическую защиту на уровне потребителя. Информационно-телекоммуникационные системы создаются предприятием самостоятельно на основе сертифицированных СКЗИ, встраивание которых в прикладные системы должно происходить с выполнением интерфейсных и криптографических протоколов, определенных технической документацией на СКЗИ (см. приложение 2).

СКЗИ "Янтарь АСБР", как было показано в разд.1.3.2, встраивается в автоматизированные системы банковских платежей, работающих на надежных, высокопроизводительных серверах корпорации Digital, использующих процессор Alpha и операционную систему Open VMS и ПЭВМ под управлением MS DOS и MS Windows. СКЗИ "Янтарь АСБР" используется для закрытия криптографическими методами каналов связи на участках от банков-участников расчетов до серверов и предназначено конкретно для:

⇒ повышения безопасности процессов электронных денежных расчетов в регионах;

⇒ создания защищенной от несанкционированных воздействий компьютеризованной информационной среды, отражающей актуальные потребности банков и финансовых учреждений;

⇒ обеспечения качественного мониторинга за функционированием средств и систем защиты;

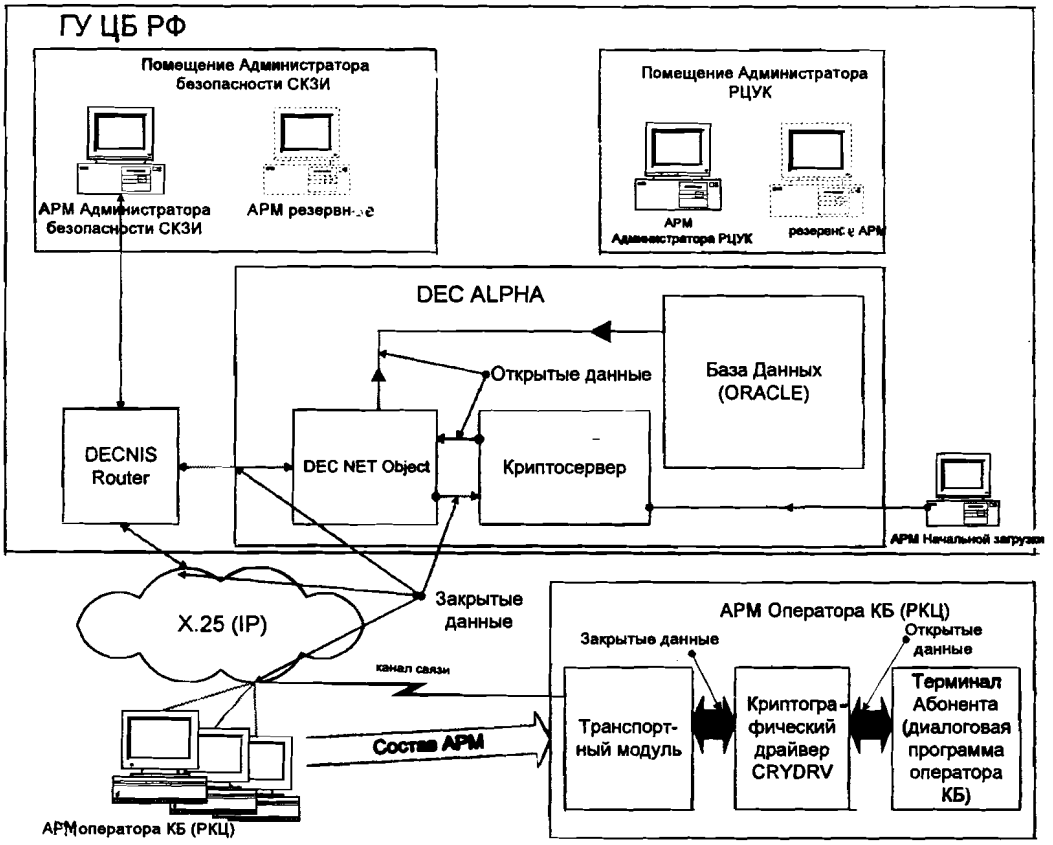

Рис.11. Обобщенная схема функционирования СКЗИ "Янтарь АСБР"

⇒ внедрения стандартизированных типовых технологий защиты информации на современной программно-аппаратной базе.

СКЗИ "Янтарь АСБР" является весьма быстродействующим, проверка значения электронной цифровой подписи занимает всего 0.03 с и тем самым не оказывает заметного влияния на скорость проведения электронных расчетов.

СКЗИ "Янтарь АСБР" обеспечивает:

конфиденциальность и контроль целостности хранимой и передаваемой информации посредством применения шифрования информации в соответствии с ГОСТ 28147-89;

аутентификацию передаваемых электронных документов посредством использования процедур формирования и проверки электронной цифровой подписи (ЭЦП) в соответствии с отечественными стандартами ГОСТ Р 34.10-94, ГОСТ Р 34.11-94;

защиту информации и компонентов СКЗИ от несанкционированных действий персонала;

юридическую значимость электронных документов посредством использования процедур формирования и проверки электронной цифровой подписи;

формирование, распределение, использование и уничтожение ключевых элементов.

Упрощенная схема функционирования СКЗИ "Янтарь АСБР" представлена на рис.11.

3.2. СТРУКТУРА СКЗИ "ЯНТАРЬ АСБР"

СКЗИ "Янтарь АСБР" состоит из следующих основных компонент:

серверной подсистемы, предназначенной для работы СКЗИ на высокопроизводительных и надежных серверах корпорации Digital, работающих под управлением операционной системы OpenVMS;

автоматизированное рабочее место (АРМ) дежурного программиста смены АСБР, реализованного на базе IBM PC-совместимой ПЭВМ, работающего под управлением операционной системы MS DOS (далее по тексту — АРМ дежурного программиста СКЗИ);

АРМ администратора регионального центра управления ключами (РЦУК), реализованного на базе IBM PC-совместимой ПЭВМ, работающей под управлением операционной системы MS DOS (далее по тексту — АРМ администратора РЦУК);

АРМ администратора безопасности СКЗИ, реализованного на базе IBM PC-совместимой ПЭВМ, работающего под управлением операционной системы MS Windows (далее по тексту — АРМ администратора СКЗИ);

клиентской части, предназначенной для работы на АРМ пользователей, реализованных на базе IBM PC-совместимых ПЭВМ, работающих под управлением операционных систем MS DOS, MS Windows (далее по тексту — АРМ абонента КБ (РКЦ)).

Для нормального ежедневного обеспечения функционирования всей системы в целом и защиты передаваемых данных между разными АРМ, а также при возникновении нештатных ситуаций в СКЗИ "Янтарь АСБР" установлены и выделены следующие структурные единицы:

- администратор регионального центра управления ключами (РЦУК);
- администратор безопасности СКЗИ;
- дежурный программист смены;
- оператор КБ (оператор РКЦ).

Их функции будут раскрыты ниже.

Запуск криптографической программной подсистемы на ЭВМ DEC Alpha осуществляется дежурным программистом смены, который должен обладать необходимыми системными правами, или автоматически при загрузке операционной системы, если программа загрузки криптографической системы внесена в стартовый файл. Загруженная криптографическая система в начальный момент времени не содержит ключевой информации и не может использоваться для выполнения криптографических функций.

Для выполнения начальной инициализации дежурный программист смены должен загрузить в криптографическую систему ключи, используя АРМ начальной инициализации (см. рис.11). При этом в систему загружаются криптографические ключи парной связи системы с АРМ администратора СКЗИ. После этого криптографическая система готова для работы с

данной АРМ. Криптографическая подсистема только с загруженными в нее ключами дежурного программиста смены не может выполнять криптографические функции над файлами, полученными от пользователей, так как не содержит ключей всех пользователей АСБР.

Для загрузки ключей всех пользователей администратор безопасности СКЗИ должен на АРМ управления криптографической системой запустить диалоговую управляющую программу, провести аутентификацию со всеми ЭВМ DEC AXP в кластере (после аутентификации автоматически устанавливается шифрованный канал связи), и загрузить таблицу ключей всех пользователей АСБР и свой ключ ЭЦП, при помощи которого будет подписываться информация в системе во время работы криптографической подсистемы. После этого криптографическая подсистема готова к работе.

Как видно из рис.11, к первоначальной схеме банковских расчетов (см. рис.6) добавились три структурные единицы: администратор РЦУК, администратор безопасности СКЗИ и дежурный программист смены, необходимые для обеспечения правильного функционирования СКЗИ.

Введенные в систему шифрование и цифровая подпись позволяют избавиться от большинства угроз в системах электронных расчетов. Рассмотрим более подробно, каким образом функционирует СКЗИ "Янтарь АСБР".

3.3. ФУНКЦИИ СКЗИ "ЯНТАРЬ АСБР"

В данной подсистеме реализован принцип абонентского шифрования. Другими словами — для каждого абонента организован канал связи с системой DEC Alpha, информация в котором шифруется на уникальном ключе, который имеется только у абонента КБ и в системе DEC AXP OpenVMS CryptSystem. Кроме того, любая транзакция (платеж, запрос), проводящаяся абонентом КБ (РКЦ), подписывается на его ключе и проверяется криптографической системой DEC AXP OpenVMS CryptSystem перед проведением операций в базе данных ЦБ РФ, что обеспечивает высокую защищенность системы. Информация, выходящая из программы терминала абонента, обрабатывается криптографическим драйвером

CRYDRV3 (рис.12). Затем зашифрованная и подписанная информация обрабатывается программным обеспечением, входящим в состав транспортного модуля, и посылается по каналу связи на DEC Alpha. Пройдя маршрутизатор DEC NIS, информация оператора попадает в сервер и обрабатывается программным модулем DEC NET OBJECT, который любой запрос, посланный абонентом КБ, посылает на криптосервер. Криптосервер расшифровывает сообщение и проверяет ЭЦП оператора, после чего расшифрованное сообщение через DEC NET OBJECT направляется в базу данных ЦБ, где и проводятся транзакции электронных расчетов. Таким образом, информация абонента КБ проходит весь путь от АРМ абонента КБ до серверной системы DEC Alpha в зашифрованном виде.

Ответная информация из базы данных (БД) проходит точно такой же путь до абонента КБ в обратной последовательности. Теперь информация в открытом виде находится только в АРМ абонента КБ и далее только в базе данных, где непосредственно проводятся расчеты. Если вернуться к нарушителю, имеющему возможность перехватывать сообщения, и посылать ложные, можно убедиться, что теперь он не сможет ознакомиться с данными абонента, поскольку информация зашифрована и расшифровать ее без знания ключа невозможно. Послать ложный документ нарушитель также не имеет возможности, поскольку не знает ключа абонента. Однако у нарушителя существует возможность периодически перехватывать, а затем посылать платежи ранее переданные легальным абонентом, и тем самым нарушить работу системы.

Надо сказать, что за рубежом коммерческий мир придает огромное значение обеспечению подлинности данных. Часто компании терпят крах не из-за утечки конфиденциальной информации, а из-за преднамеренной порчи их данных, навязывания ложной информации (см. разд.2.2). Для нейтрализации таких угроз, а также для точного определения зарегистрированных пользователей при вхождении в связь используется аутентификация абонентов с последующей выработкой сеансового ключа.

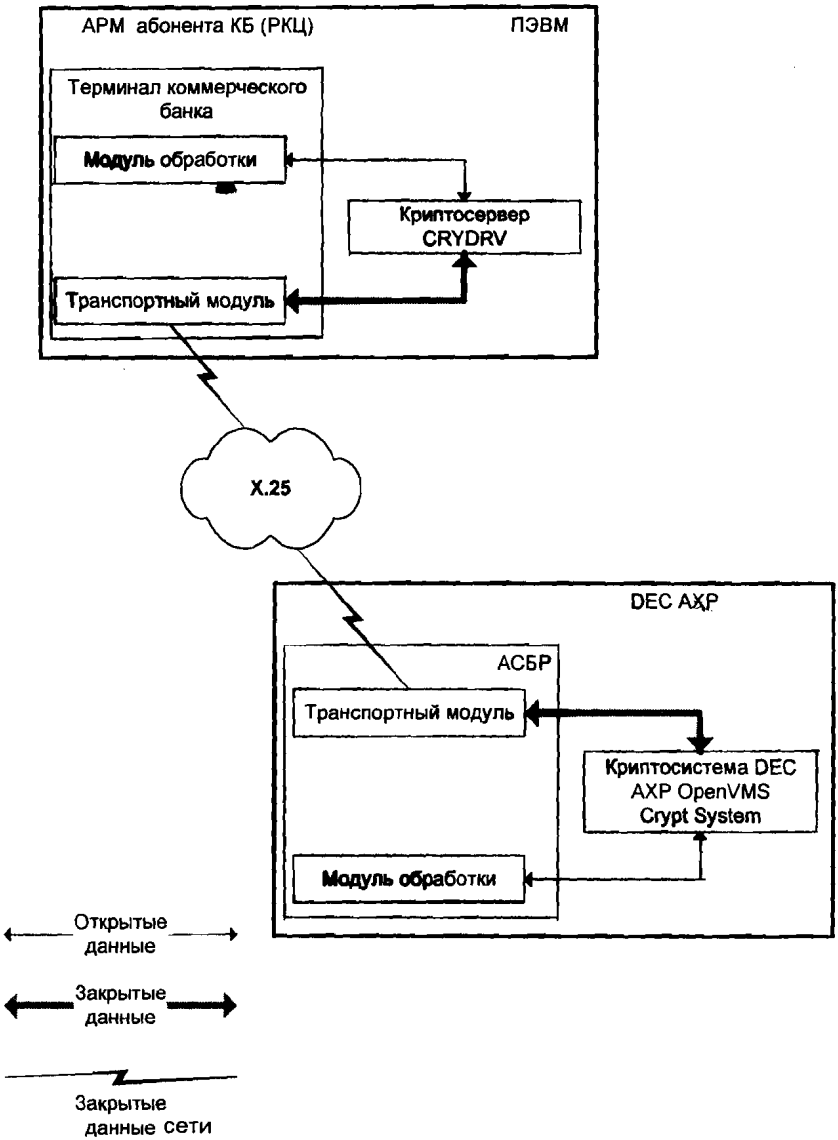

Рис.12. Схема взаимодействия АРМ абонента и DEC AXP Crypt System

Аутентификация информации в сетях — это обеспечение заданной степени уверенности получателя в том, что полученная информация была передана отправителем и при этом не была заменена или искажена. В системе "Янтарь АСБР" применяется аутентификация согласно рекомендациям международного стандарта ISO X.509.

Аутентификация в общих чертах происходит следующим образом: абонент вырабатывает случайную последовательность байт (случайное число) и посылает его системе DEC AXP Crypt System, зашифрованную на ключе их парной связи. Система вырабатывает свою случайную последовательность байт и посылает ее абоненту. Абонент производит определенные действия с этой последовательностью (подписывает) и возвращает на криптосервер, которую тот проверяет. Точно такие же операции производит криптосервер со случайной последовательностью абонента. При совпадении подписей (при положительных результатах проверки) считается, что абонент и система платежей подлинные. Кроме того, на основе данных случайных последовательностей вырабатывается сеансовый криптографический ключ, на котором шифруется вся информация во время текущего сеанса. По завершению сеанса ключ уничтожается. Таким образом, нейтрализуется угроза, при действии которой злоумышленник может пытаться нарушить работу системы путем повтора ранее переданного сообщения одним из абонентов. Кроме того, для каждого блока данных, передаваемого по каналу связи, вырабатывается имитовставка согласно ГОСТ 28147-89, которая служит для выявления попыток их искажения при передачи по каналам связи.

Другой криптографический метод, используемый в системе для защиты сообщений, — электронная цифровая подпись (ЭЦП). Более подробно об ЭЦП можно узнать в работах [28, 31, 36]. Напомним лишь угрозы, от которых позволяет избавиться применение ЭЦП при условии, что участники A, B и C не вступали в сговор друг с другом:

- отправитель A заявляет, что он не посылал сообщение Z получателю B, хотя в действительности его посылал(отказ от авторства);
- отправитель A заявляет, что он передал сообщение T, хотя в действительности передал Z (подмена отправленного сообщения);

- получатель В изменяет полученное от отправителя А сообщение Z на Т и заявляет, что получил измененное сообщение от отправителя (подмена принятого сообщения);
- получатель В формирует свое сообщение Т и заявляет, что получил его от отправителя (имитация принятого сообщения);
- злоумышленник С искажает сообщение, которое отправитель А передает получателю В (подмена сообщения);
- злоумышленник С формирует свое сообщение Т и посылает получателю В от имени отправителя А (имитация передаваемого сообщения).

Таким образом, в системе "Янтарь АСБР" учтены все главные требования обеспечения безопасности в автоматизированных банковских системах. Все основные операции автоматизированы и не требуют вмешательства операторов во время функционирования, что повышает общее состояние безопасности системы. Все криптографические функции выполняются в "прозрачном" режиме. Например, "абонент КБ" после подключения и загрузки своего автоматизированного рабочего места практически не замечает работы СКЗИ. Исключение представляют случаи, когда при отправке сообщения необходимо подписывать информацию (на экране монитора появляется надпись "Вставьте ключевую дискету") и при возникновении нештатных ситуаций (коллизий). Рассмотрим функции и задачи каждой части СКЗИ.

Серверной частью СКЗИ "Янтарь АСБР" является криптографическая система DEC AXP OpenVMS CryptSystem, устанавливаемая на многомашинный кластер ЭВМ DEC AXP и представляющая собой комплекс программных средств, предназначенных для одновременной асинхронной обработки криптографических запросов, поступающих от прикладных процессов. Она также осуществляет мониторинг процессов, управление процессом обработки запросов и верификацию их корректности. Модули криптографической системы исполняются в кластере из нескольких компьютеров DEC AXP под управлением операционной системы OpenVMS. Число пользовательских процессов, которое криптографическая система способна обслужить одновременно, определяется максимально возможным числом сетевых процессов для каждого узла в кластере.

В свою очередь, криптографическая система DEC AXP OpenVMS CryptSystem состоит из следующих компонент:

- криптографического сервера, представляющего собой процесс, работающий под управлением операционной системы OpenVMS на компьютерах семейства DEC AXP, предназначенный для одновременного обслуживания асинхронных запросов от пользовательских процессов. Предусматривается наличие одной исполняющейся копии криптографического сервера на каждом узле кластера;
- тестовой задачи, представляющей собой программу, запускаемую периодически с заданным администратором интервалом времени, и предназначенной для контроля целостности криптографических функций криптографического сервера и правильности выполнения им своих функций;
- интерфейсной библиотеки прикладного процесса, представляющей собой объектную библиотеку, которая предназначена для стандартизации механизма взаимодействия пользовательских процессов с криптографическим сервером при использовании между ними только обмена данными.

Криптографический сервер и тестовая задача исполняются на ЭВМ семейства DEC AXP под управлением ОС OpenVMS, а диалоговая управляющая программа — на IBM PC/AT-совместимом компьютере под управлением MS Windows. Диалоговая управляющая программа представляет собой программу, загруженную на "АРМ администратора безопасности СКЗИ", и предназначенную для визуального отображения состояния криптографических серверов на каждом узле кластера и оперативного изменения состояния криптографических серверов по команде администратора СКЗИ с "АРМ администратора безопасности СКЗИ".

Взаимодействие криптографического сервера и прикладных процессов внутри одного узла осуществляется стандартными механизмами межзадачного взаимодействия ОС OpenVMS, а межзадачное взаимодействие процессов криптографической системы на узле кластера и удаленной рабочей станции — средствами сети DECnet.

Указанные компоненты обеспечивают автоматическую обработку информации абонентов КБ и обеспечивают защиту информации в сервере DEC ALPHA от возможных угроз со

стороны абонентов сети и неправомерных действий легальных пользователей.

Криптографическая система DEC AXP OpenVMS CryptSystem выполняет в среде OpenVMS следующие криптографические операции:

- зашифрование файла по ГОСТ 28147-89 для одного или нескольких получателей (абонентов);
- расшифрование файла, полученного от зарегистрированного абонента;
- выработка электронной цифровой подписи (ЭЦП) файла по ГОСТ 34.10-94 и ГОСТ 34.11-94;
- проверки подлинности (соответствия) ЭЦП файла, полученного от зарегистрированного абонента;
- вычисления значения хэш-функции содержимого файла.

АРМ дежурного программиста смены АСБР, входящее в состав эксплуатационной смены, используется для начальной инициализации криптографической системы DEC AXP OpenVMS CryptSystem, выполнения загрузки в нее ключевых элементов дежурного программиста смены и администраторов СКЗИ, установления между ней и АРМ администратора СКЗИ защищенного управляющего канала для обеспечения возможности отслеживать и управлять состоянием серверной части СКЗИ "Янтарь АСБР". ПЭВМ должна быть соединена с сервером DEC AXP через последовательный порт "нуль-модемным" кабелем, обеспечивающим полный протокол асинхронной передачи данных (асинхронный коммуникационный интерфейс RS-232C).

Необходимость данной загрузки криптографических ключей обусловливается потребностью в дальнейшем устанавливать закрытый канал связи между криптографической системой DEC AXP OpenVMS CryptSystem и диалоговой управляющей программой DUP "АРМ администратора безопасности СКЗИ", соединенных между собой посредством локальной вычислительной сети.

Инициализация криптографической системы выполняется дежурным программистом смены — лицом, имеющим доступ в машинный зал и обладающим необходимыми правами для запуска криптографической системы. Дежурных программистов смены может быть несколько, для организации работы в необходимое количество смен или для устойчивой работы СКЗИ

"Янтарь АСБР" при компрометации ключа у одного из дежурных программистов.

АРМ администратора РЦУК, непосредственно не подключенное к системе электронных расчетов, позволяет выполнять функции по выдаче, генерации, регистрации и смены ключей (для шифрования и подписи) всех участников расчетов.

Каждый абонент (КБ), подключаемый к АСБР, должен зарегистрировать свои открытые ключи на АРМ АБ РЦУК. В случае отключения абонента от работы с АСБР или при компрометации ключа (ключевой дискеты) пользователя, администратор РЦУК удаляет запись в справочнике открытых ключей, используя программу HOST. Администратор РЦУК должен ежегодно проводить плановую смену всех ключевых элементов, используемых в системе СКЗИ "Янтарь АСБР", и вести архив всех справочников открытых ключей, которые использовались в системе за последние пять лет. Администратор РЦУК после каждой модификации справочника ключей переносит на дискете полную копию всех файлов справочника на ПЭВМ управления криптографической системой. При возникновении конфликтной ситуации между абонентами или другими пользователями системы, администратор РЦУК должен провести разбор конфликтной ситуации, используя для этого программу CHKSIGN, выполняя роль арбитра.

АРМ администратора безопасности СКЗИ позволяет выполнять непосредственное управление серверной системой DEC AXP OpenVMS CryptSystem и предназначено для:

- загрузки таблицы парных симметричных ключей шифрования и открытых ключей ЭЦП всех зарегистрированных пользователей на сервер, на котором установлена криптографическая система;
- отображения состояния криптографического сервера;
- оперативного изменения состояния криптографического сервера по команде администратора безопасности.

АРМ позволяет администратору СКЗИ выдавать на криптографический сервер следующие команды:

ОСТАНОВИТЬ КРИПТОСЕРВЕР;
ПРИОСТАНОВИТЬ УСТАНОВЛЕНИЕ СОЕДИНЕНИЙ;
ВОЗОБНОВИТЬ УСТАНОВЛЕНИЕ СОЕДИНЕНИЙ;
БЛОКИРОВАТЬ СОЕДИНЕНИЕ С ПОЛЬЗОВАТЕЛЕМ;
РАЗБЛОКИРОВАТЬ СОЕДИНЕНИЕ С ПОЛЬЗОВАТЕЛЕМ;
РАЗРЫВ СОЕДИНЕНИЯ С ПОЛЬЗОВАТЕЛЕМ.

3.4. КЛИЕНТСКАЯ ЧАСТЬ СКЗИ "ЯНТАРЬ АСБР"

Самой многочисленной составной единицей рассматриваемой автоматизированной банковской системы является клиентская часть СКЗИ "Янтарь АСБР". Ее основой служит "АРМ абонента КБ (РКЦ)", которое устанавливается на IBM PC-совместимых ПЭВМ, работающих под управлением операционных систем MS DOS, MS Windows. Для этого обычно используются абонентские ПЭВМ, отвечающие ряду минимальных требований по информационной безопасности. Например, выполнение требования на отсутствие компьютерных вирусов. Инструкция по установке АРМ абонента КБ(РКЦ) приведена в приложении 4.

АРМ абонента КБ(РКЦ), установленное на ПЭВМ пользователя, помимо осуществления телекоммуникационных функций предназначено для:

- чтения секретного ключа, выработанного программой системы криптографической защиты информации "Верба" HOST v6.0, и вычисления соответствующего ему открытого ключа электронной цифровой подписи (ЭЦП);
- формирования регистрационного файла открытых ключей ЭЦП;
- формирования регистрационных и контрольных карточек открытых ключей ЭЦП;
- регистрации открытых ключей ЭЦП и номеров парных симметричных ключей шифрования участников автоматизированной системы банковских расчетов (АСБР);
- хранения парных симметричных ключей шифрования на жестком диске в зашифрованном на личных ключах виде;
- просмотра базы данных (БД) атрибутов зарегистрированных участников автоматизированной системы банковских расчетов;
- создания текстового файла с основными атрибутами участников расчетов, зарегистрированных в БД;
- удаления из БД зарегистрированных участников автоматизированной системы банковских расчетов как при компрометации ими своих ключевых элементов, так и при прекращении ими права использования системы электронных расчетов;
- протоколирования всех операций, связанных с доступом к БД, и модификации ее содержимого.

В состав АРМ абонента КБ (РКЦ) входят:

- программа генерации ключей ЭЦП и ведения базы данных ключевых элементов (KEYGEN);

- криптографический драйвер (CRYDRV3);
- драйвер ДСЧ CYPRASW СКЗИ "Верба";
- программа HOST СКЗИ "Верба";
- подсистема защиты от НСД (некриптографическая).

Оператор коммерческого банка использует свои криптографические ключи для закрытия финансовых данных, передаваемых из коммерческого банка в АСБР. Операторы коммерческого банка и операторы РКЦ с позиций ключевой системы не разделяются.

3.5. СОСТАВ И НАЗНАЧЕНИЕ ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ СКЗИ "ЯНТАРЬ АСБР"

Функции клиентской системы, системы оперативного управления и мониторинга, управления ключевой системой, системы защиты от несанкционированного доступа (НСД), системы поддержки разбора конфликтных ситуаций и доказательства авторства электронного документа, снабженного ЭЦП, реализуются посредством композиций программного обеспечения (ПО) и технических средств. Они установлены в АРМ администратора РЦУК, АРМ администратора СКЗИ, АРМ дежурного программиста, АРМ оператора КБ(РКЦ)), которые представляют собой аппаратно-программные комплексы на базе IBM PC-совместимых ПЭВМ, работающих под управлением ОС MS DOS, MS Windows. Перечень ПО и технических средств приведен в табл.2.

Программа ведения справочника участников расчетной системы (программа CUB) предназначена для:

регистрации в базе данных (БД) информации о выданных ключевых дискетах Федерального агентства правительственной связи и информации при Президенте Российской Федерации (ФАПСИ) для всех участников автоматизированной системы банковских расчетов (АСБР);

регистрации в БД открытых ключей электронной цифровой подписи (ЭЦП) всех участников автоматизированной системы банковских расчетов;

просмотра и удаления администраторов регионального центра управления безопасностью (РЦУБ) из списка администраторов РЦУБ;

просмотра и удаления зарегистрированных в БД администраторов безопасности АСБР;

просмотра и удаления зарегистрированных в БД дежурных программистов смены АСБР;

просмотра и удаления зарегистрированных в БД операторов коммерческих банков (КБ) и операторов расчетно-кассовых центров (РКЦ);

формирования и выдачи на автоматизированное рабочее место (АРМ) администратора безопасности АСБР регистрационного файла зарегистрированных участников автоматизированной системы банковских расчетов;

выдачи списка всех участников автоматизированной системы банковских расчетов, находящихся на данный момент в БД.

Таблица 2

ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ И ТЕХНИЧЕСКИЕ СРЕДСТВА	АВТОМАТИЗИРОВАННОЕ РАБОЧЕЕ МЕСТО (АРМ)			
	администратора РЦУК	администратора СКЗИ	дежурного программиста	оператора КБ (РКЦ)
Программа ведения справочника участников расчетной системы (CUB)	+	—	—	—
Программа формирования личных ключевых дискет администраторов РЦУК (KEYCUB)	+	—	—	—
Драйвер ДСЧ (CYPRASW)	+	+	+	+
Программа HOST СКЗИ "Верба"	+	+	+	+
Криптографический драйвер (CRYDRV3)	+	+	+	+
Эталонная программа проверки ЭЦП (CHKSIGN)	+	+	+	+
Программа генерации ключей ЭЦП и ведения БД ключевых элементов (KEYGEN)	—	+	+	+
Программа ведения БД ключевых элементов участников расчетной системы (RCENTR)	—	+	—	—
Диалоговая управляющая программа (DUP)	—	+	—	—
Программа начальной инициализации системы DEC AXP OpenVMS CryptSystem (MKEYS)	—	—	+	—
Программно-аппаратный комплекс "Аккорд"	+	+	+	+

Программа формирования личных ключевых дискет администраторов РЦУБ (программа KEYCUB), являющаяся составной частью комплекса криптографических средств защиты информации "Янтарь АСБР", предназначена для:

- чтения секретного ключа выработанного программой СКЗИ "Верба" HOST v.6.11 ЯЦИТ. 00002-01 34 02 и вычисления соответствующего ему открытого ключа электронной цифровой подписи (ЭЦП);
- формирования личных ключевых дискет (одной основной и одной резервной) для администраторов регионального центра управления безопасности (РЦУБ);
- хранения парных симметричных ключей шифрования на жестком диске в зашифрованном на личных ключах шифрования виде.

Программа CYPRASW предназначена для выработки случайной последовательности, используемой в процессах шифрования, подписи и выработки ключей. Кроме того, CYPRASW используется для организации временного размещения индивидуальных ключей в ОЗУ при хранении рабочих ключей на жестком диске. Программа CYPRASW используется в составе СКЗИ "Верба", представляет собой программный драйвер, загружается перед использованием СКЗИ и остается резидентно в памяти. Программа CYPRASW функционирует под управлением операционной системы MS DOS ver. 5.00 и выше на персональных ЭВМ, совместимых с IBM PC/AT (процессор 80386 и выше). Требуемый объем оперативной памяти не более 3.5 Кбайт. Инициализация датчика случайных чисел (ДСЧ), входящего в состав драйвера, производится с использованием главного ключа gk.db3 и клавиатурного ДСЧ, работающего на принципе "момента отжатия".

Программа CYPRASW обеспечивает выполнение следующих функций:

расшифровать ключ подписи, хранящийся на жестком диске (ЖД), на ckdi;

расшифровать ключи парно-выборочной связи, хранящиеся на ЖД, на ckd;

дать N случайных байт (обращение к ДСЧ);

дать содержимое файла num (N аб + N сер);

дать ckdi;

дать ckd;

дать UZ;

стереть область данных драйвера (КЗУ, блок подстановки и буфера);

выдача на экран подсказки.

Программа HOST предназначена для создания рабочих ключевых дискет (форматирования, копирования и формирования ключей для подписи) и обеспечивает следующие функции:

выработку секретных ключей для подписи и запись их на ключевой диск;

выработку открытых ключей для проверки подписи, создание регистрационной записи и сохранение ее в файле;

просмотр регистрационной записи из файла;

подготовка секретных ключей для подписи на жестком диске;

подготовка ключей шифрования для хранения на жестком диске;

подготовка рабочей копии ключевой дискеты.

Программа HOST функционирует под управлением операционной системы MS DOS v.5.0 и выше на персональных ЭВМ, совместимых с IBM PC/AT 386, 486 или Pentium. Требуемый объем оперативной памяти не менее 250 Кбайт. Кроме того, необходим хотя бы один накопитель на гибких магнитных дисках (НГМД).

Криптографический драйвер CRYDRV обеспечивает функции аутентификации в соответствии с рекомендациями X.509, электронной цифровой подписи по ГОСТ Р 34.10-94, ГОСТ Р 34.11-94 и шифрования по ГОСТ 28147-89. Доступ к криптографическим функциям драйвера осуществляется посредством интерфейсной библиотеки, предназначенной для использования в среде MS DOS.

Реализация функций криптографического драйвера основана на использовании сертифицированной криптографической библиотеки СКЗИ "Верба" [28].

В качестве алгоритма электронной цифровой подписи используется асимметричный вариант электронной цифровой подписи (ЭЦП), а именно, криптосистема с двумя ключевыми элементами — открытым (общедоступным) и секретным, — соответствующая ГОСТ Р 34.10-94. Для формирования хэш-функции сообщения, используется алгоритм, соответствующий

ГОСТ Р 34.11-94. Шифрование информации выполняется по ГОСТ 28147-89.

Временные характеристики криптографического драйвера для ПЭВМ 433dx2 33 МГц следующие:

продолжительность формирования цифровой подписи сообщения — 0,055 с, не более;

продолжительность проверки цифровой подписи сообщения — 0,43 с, не более;

скорость хеширования сообщения — 99 Кбайт/с, не менее;

скорость шифрования сообщения по ГОСТ 28147-89 в режиме гаммирования — 173 Кбайт/с, не менее.

Эталонная программа проверки ЭЦП (программа CHKSIGN) предназначена для проверки соответствия ЭЦП содержанию электронного документа и определения участника автоматизированной системы банковских расчетов, выполнившего ее формирование. Программа CHKSIGN применяется при разборе конфликтных ситуаций, связанных с определением авторства электронного документа.

Программа генерации ключей ЭЦП и ведения БД ключевых элементов (программа KEYGEN) предназначена для:

- чтения секретного ключа, выработанного программой СКЗИ "Верба" HOST v.6.0, и вычисления соответствующего ему открытого ключа электронной цифровой подписи;
- формирования регистрационного файла открытых ключей ЭЦП;
- формирования регистрационных и контрольных карточек открытых ключей ЭЦП;
- регистрации открытых ключей ЭЦП и номеров парных симметричных ключей шифрования участников автоматизированной системы банковских расчетов;
- хранения парных симметричных ключей шифрования на жестком диске в зашифрованном на личных ключах виде;
- просмотра базы данных атрибутов зарегистрированных участников автоматизированной системы банковских расчетов;
- создания текстового файла с основными атрибутами участников расчетов, зарегистрированных в БД;
- удаления из БД зарегистрированных участников автоматизированной системы банковских расчетов как при компрометации ими своих ключевых элементов, так и при прекращении ими права использования системы электронных расчетов;

• протоколирования всех операций, связанных с доступом к БД, и модификации ее содержимого.

Программа KEYGEN позволяет контролировать целостность БД зарегистрированных абонентов путем вычисления имитовставок записей БД при выполнении регистрации и занесении в нее информации, и сравнения с ранее вычисленными значениями имитовставок при повторных обращениях к записям БД.

Доступ к БД ограничивается только теми участниками, которые формировали свои личные ключевые дискеты на данном рабочем месте.

Для контроля целостности программы KEYGEN используется метод самоконтроля целостности, выполняемый после запуска программы, который заключается в вычислении значений имитовставки исполняемого файла задачи и сравнении ее с вычисленной имитовставкой при формировании дистрибутивного носителя, а также присвоении ему серийного номера.

Программа ведения БД ключевых элементов участников расчетной системы также входит в комплекс криптографических средств защиты информации "Янтарь АСБР" (программа RCENTR) и предназначена для:

• регистрации в базе данных открытых ключей электронной цифровой подписи всех участников автоматизированной системы банковских расчетов;

• просмотра и удаления зарегистрированных в БД администраторов безопасности;

• просмотра и удаления зарегистрированных в БД дежурных программистов смены;

• просмотра и удаления зарегистрированных в БД операторов коммерческих банков и расчетно-кассовых центров;

• выдачи списка всех участников системы электронных расчетов, зарегистрированных на данный момент в БД.

Диалоговая управляющая программа (программа DUP) входит в состав программного обеспечения автоматизированного рабочего места администратора безопасности и предназначена для:

• загрузки на криптографический сервер системы DEC AXP OpenVMS CryptSystem ключей зарегистрированных абонентов;

• отображения состояния криптографического сервера;

• оперативного изменения состояния криптографического сервера по команде администратора безопасности.

Программа DUP работает под управлением MS Windows на АРМ администратора безопасности, обеспечивает передачу криптографическому серверу команд и прием от него информации о его состоянии. LOG-протокол работы диалоговой управляющей программы ведется средствами DEC AXP OpenVMS CryptSystem в отдельном LOG-протоколе на DEC AXP.

Программа DUP позволяет администратору СКЗИ выдачу на криптографический сервер следующих команд:

ОСТАНОВИТЬ КРИПТОСЕРВЕР — может быть либо немедленной, с разрывом всех соединений, либо "плавной", когда криптосервер ожидает окончания сеансов работы всех активных пользователей, одновременно с этим запрещая устанавливать новые соединения, и выполняет останов, когда не будет ни одного активного пользователя;

ПРИОСТАНОВИТЬ УСТАНОВЛЕНИЕ СОЕДИНЕНИЙ и ВОЗОБНОВИТЬ УСТАНОВЛЕНИЕ СОЕДИНЕНИЙ — позволяют запрещать установление новых соединений, переводя криптосервер в режим обслуживания только активных пользователей, блокируя возможность установления новых соединений, и возвращать криптосервер в штатный режим работы;

БЛОКИРОВАТЬ СОЕДИНЕНИЕ С ПОЛЬЗОВАТЕЛЕМ и РАЗБЛОКИРОВАТЬ СОЕДИНЕНИЕ С ПОЛЬЗОВАТЕЛЕМ — предоставляют возможность запретить установление соединений с любым зарегистрированным пользователем, например, при получении сигнала о компрометации его ключей, и снять блокировку с ранее заблокированного пользователя. Если блокируемый пользователь находится в активном состоянии, выдача команды БЛОКИРОВАТЬ СОЕДИНЕНИЕ С ПОЛЬЗОВАТЕЛЕМ вызовет выполнение принудительного разрыва сеанса связи и блокировку последующих установлений соединений до тех пор, пока для данного пользователя администратором безопасности СКЗИ АСБР не будет выдана команда РАЗБЛОКИРОВАТЬ СОЕДИНЕНИЕ С ПОЛЬЗОВАТЕЛЕМ;

БЛОКИРОВАТЬ СОЕДИНЕНИЕ С ПОЛЬЗОВАТЕЛЕМ — выполняется при помощи диалогового окна. При помощи данного окна администратор СКЗИ должен сначала выбрать организацию, работу пользователя которой он блокирует, а затем из

списка пользователей данной организации - конкретного пользователя;

РАЗБЛОКИРОВАТЬ СОЕДИНЕНИЕ С ПОЛЬЗОВАТЕЛЕМ — выполняется при помощи диалогового окна. При помощи данного окна администратор СКЗИ должен выбрать пользователя, работу которого он разблокирует. В списке отображаются только ранее заблокированные пользователи;

РАЗРЫВ СОЕДИНЕНИЯ С ПОЛЬЗОВАТЕЛЕМ — позволяет администратору безопасности СКЗИ АСБР немедленно разорвать соединение с любым активным пользователем. Блокировка установления последующих соединений не выполняется и пользователь может установить соединение, если не установлен режим обслуживания только активных пользователей при помощи команды ПРИОСТАНОВИТЬ УСТАНОВЛЕНИЕ СОЕДИНЕНИЙ.

При выполнении любой команды программа DUP запрашивает личную ключевую дискету администратора безопасности СКЗИ. После установки дискеты администратор безопасности СКЗИ должен нажать на кнопку ОК. Команда ВЫХОД позволяет администратору СКЗИ выйти из программы DUP.

Программа начальной инициализации системы DEC AXP OpenVMS CryptSystem (программа MKEYS) предназначена для выполнения загрузки в криптографическую систему DEC AXP OpenVMS CryptSystem ключевых элементов дежурного программиста смены и администраторов СКЗИ.

3.6. КЛЮЧЕВАЯ СИСТЕМА И КЛЮЧЕВЫЕ ДОКУМЕНТЫ СКЗИ "ЯНТАРЬ АСБР"

3.6.1. Общие положения

Организация криптографической ключевой системы играет исключительно важную роль при использовании средств криптографической защиты информации в автоматизированных банковских технологиях. Высокие требования по надежности, оперативности и безотказности платежной системы в целом, ее подверженность постоянным нападениям со стороны злоумышленников (в том числе легальных пользователей), придание юридической значимости или силы электронным платежным документам и другие особенности платежной системы оказывают существенное влияние на выбор ключевых систем, а

также налагают дополнительные требования по управлению ключами. В частности, большое число абонентов банковских сетей, их постоянная динамика и неоднородность существенно усложняют управление ключами. Безопасность и надежность систем криптографической защиты, когда большая часть информации о них общедоступна, целиком зависит от защиты их секретных параметров или ключей, от надежности систем управления этими ключами. Под управлением ключами понимают процесс, посредством которого ключевой материал, используемый в симметричных или асимметричных криптосистемах, предоставляется в распоряжение пользователей, подвергается обработке определенными процедурами безопасности с момента его создания и вплоть до его уничтожения. Управление ключами содержит следующие основные процедуры:

- генерация,
- распространение,
- хранение,
- уничтожение.

Помимо них можно отметить процедуры регистрации, сертификации, инсталляции, архивации, замены и другие.

Для каждой из перечисленных процедур существуют свои угрозы безопасности ключевому материалу, которые могут привести к нарушению безопасности всей хранимой и передаваемой информации, вне зависимости от высокой стойкости применяемых базовых криптографических алгоритмов. Система управления ключами зависит от типа применяемой криптосистемы. Согласно международному стандарту ISO 8732-88 "Банковское дело — управление ключами (оптовые финансовые операции)", который связан с системой других стандартов ISO 646, 7982 -1, 8372, 8730, 8731, ANSI X.3.92, предполагается использование только симметричных криптоалгоритмов шифрования информации. С учетом данных стандартов, а также особенностей платежных систем (см. разд.1.3.2), системы управления ключами должны отвечать следующим требованиям [39]:

- устойчивость к компрометации ключей у части пользователей сети;
- быстрое восстановление пользователей в сети;
- минимальное число ключей, подлежащих сохранности организационными мерами;

- высокая степень защиты носители ключевой информации от копирования;
- плановая замена ключей;
- генерация ключей цифровой подписи самими владельцами подписи;
- автоматизация, исключающая ошибочные действия пользователей;
- незначительное влияние на производительность платежной системы;
- защищенность от умышленных и ошибочных действий пользователей;
- защищенность от несанкционированного доступа, включающего подсистему разграничения и контроля доступа;
- защищенность от внедрения программных вирусов и закладок;
- надежная аутентификация пользователей платежной системы;
- централизованная рассылка открытых ключей ЭЦП;
- невозможность фальсификации и подделки открытых ключей ЭЦП в системе;
- отработанная и юридически значимая технология разрешения конфликтных ситуаций.

Рассмотрим теперь, каким образом выполняются указанные требования в СКЗИ "Янтарь АСБР".

3.6.2. Ключевая система

Ключевая система для СКЗИ "Янтарь АСБР" представляет собой "звездообразную" структуру. Все абоненты при такой организации сети делятся на две группы абонентов: находящихся в центре "звезды" (администраторы СКЗИ) и находящихся на периферии "звезды" (операторы КБ, РКЦ, дежурные программисты смены).

Ключевая структура не ограничивает количество абонентов в сети, что позволяет организовать обслуживание СКЗИ в непрерывном режиме, организуя сменную работу. Ключевые элементы являются личными. Это означает, что каждый участник системы имеет свой персональный ключ, которым в свою очередь повышает персональную ответственность работников и устраняет необходимость передачи ключей от одного ответ-

ственного исполнителя к другому, существенно упрощая разбор возможных фактов их компрометации.

В ключевой системе для всех физических лиц, допущенных к работе на АРМ и участвующих в эксплуатации СКЗИ "Янтарь АСБР", введены следующие должностные категории:

- ответственный исполнитель;
- участник автоматизированной системы банковских расчетов.

Под термином "ответственный исполнитель" понимается физическое лицо, допущенное к работе на АРМ и обладающее секретным ключом подписи. В СКЗИ "Янтарь АСБР" ответственными исполнителями являются администраторы РЦУК, администраторы безопасности СКЗИ, дежурные программисты АСБР, операторы КБ(РКЦ).

Под термином "участник автоматизированной системы банковских расчетов" понимается ответственный исполнитель, зарегистрированный в базе данных (БД) системы DEC AXP OpenVMS CryptSystem. Участниками АСБР являются администраторы безопасности СКЗИ, дежурные программисты АСБР, операторы КБ(РКЦ).

Администратор РЦУК, непосредственно не являющийся участником расчетов, выполняет функции регистрации ключей всех остальных участников расчетов.

Администратор СКЗИ при помощи ПО "АРМ администратора СКЗИ" выполняет непосредственное управление серверной системой DEC AXP OpenVMS CryptSystem. Финансовые документы, формируемые АСБР, подписываются на секретных ключах администратора СКЗИ. Дежурный программист смены, входящий в состав эксплуатационной смены, использует свои ключи для начальной инициализации криптографической системы DEC AXP OpenVMS CryptSystem и установления защищенного управляющего канала между ней и диалоговой управляющей программой. Этот канал предоставляет возможность администратору СКЗИ отслеживать состояние и управлять состоянием серверной части СКЗИ "Янтарь АСБР". Оператор КБ(РКЦ) при помощи ПО "АРМ оператора КБ(РКЦ)" использует свои ключи для закрытия финансовых данных, передаваемых из коммерческого банка (расчетно-кассового центра) в АСБР.

Напомним, что операторы коммерческого банка и операторы РКЦ не разделяются с позиций ключевой системы.

В ключевой системе используется иерархия ключей, обеспечивающая хранение ключей в зашифрованном виде на главных ключах; выполнение аутентификации с применением парных симметричных ключей шифрования; шифрование данных на сеансовых, модифицируемых ключах; электронную цифровую подпись на асимметричных ключах.

3.6.3. Ключевые документы

Для шифрования информации в системе используются парные симметричные ключи, формируемые в виде полной матрицы (серии). Размер серии не может быть изменен во время действия ключей и должен быть определен при заказе серии с учетом количества уже имеющихся абонентов системы, числа абонентов, подключаемых к системе во время действия серии, и необходимого запаса на возможные случаи компрометации ключей.

Для ЭЦП используются асимметричные ключи, которые вырабатываются непосредственно абонентами системы.

В качестве носителей ключевой информации используются стандартные гибкие магнитные диски (ГМД) 3,5" типа HD, размеченные в формате DOS, для хранения ключевой информации, и имеющие нестандартный сектор для хранения маски, которая используется для защиты от копирования ключевой информации средствами DOS. Для повышения надежности при эксплуатации рекомендуется применять дискеты с тефлоновым защитным слоем.

Ключевыми документами СКЗИ "Янтарь АСБР" являются:

- ключевые комплекты ФАПСИ;
- личные ключи на ГМД ответственных исполнителей.

Ключевые комплекты ФАПСИ распределяются среди абонентов сети связи централизованно с участием Центра управления безопасностью (ЦУБ). Исходная ключевая информация для СКЗИ "Янтарь АСБР" генерируется и записывается на дискеты в ФАПСИ и поставляется в РЦУК в виде отдельных упаковок в соответствии с числом абонентов сети и с учетом резерва.

Ключевой комплект ФАПСИ представляет собой два ГМД (основной и резервный) в одной упаковке. Содержимое двух ГМД в одном комплекте одинаково. Дублирующий ГМД (экз. № 2) предназначен для использования в случае невозможности считывания информации с первого ГМД (экз. № 1). Каждая дискета содержит всю ключевую информацию, за исключением секретных ключей ЭЦП, необходимую для работы одного абонента.

Ключевой комплект помещается в упаковку. На этикетку наносятся:

- надпись "ШИФР";
- наименование ключевого комплекта ФАПСИ;
- шестизначный порядковый номер серии и четырехзначный номер комплекта;
- номер экземпляра.

Этикетка может содержать дополнительную технологическую информацию, наносимую изготовителем (рис.13).

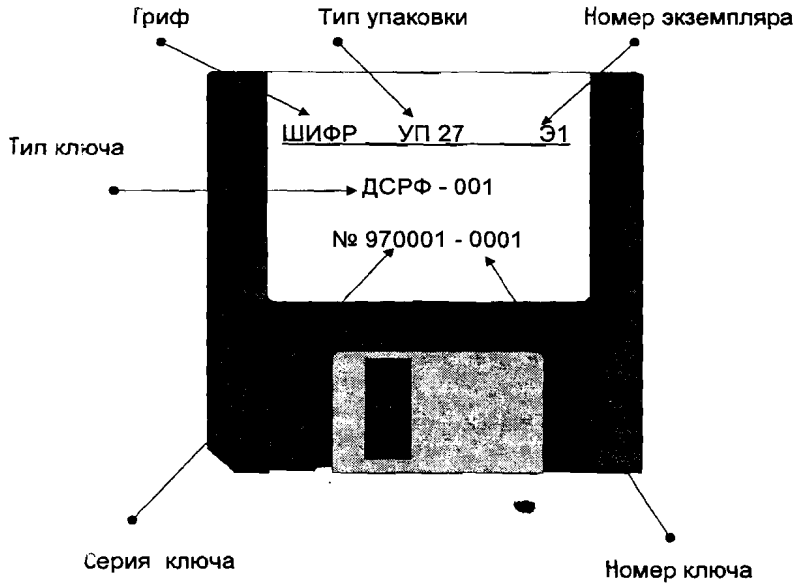

Рис.13. Ключевая дискета

Личные ключевые ГМД изготавливаются самими ответственными исполнителями. В качестве исходного ключевого документа используется ключевой диск ФАПСИ. Каждый ответственный исполнитель должен лично убедиться в целостности специальной упаковки ключевого комплекта ФАПСИ при получении его в РЦУК. Вскрытие специальной упаковки производится самими ответственными исполнителями непосредственно перед процедурой создания личных ключевых дискет.

Для оперативного восстановления связи в случае компрометации ключей, а также их повреждения, служат резервные ключевые комплекты, которые заказываются ЦБ РФ в ФАПСИ.

3.6.4. Управление ключами

РЕГИОНАЛЬНЫЙ ЦЕНТР УПРАВЛЕНИЯ КЛЮЧАМИ И ЕГО ФУНКЦИИ

В структуре СКЗИ "Янтарь АСБР" имеется региональный центр управления ключами (РЦУК).

Функции РЦУК:

подача заявок на требуемое количество ключевых упаковок для плановой смены ключей в сети;

получение комплекта ключевых упаковок;

организация и хранение ключевых упаковок (в том числе и резервных);

ведение журнала учета полученных, хранящихся в РЦУК и выданных абонентам ключевых упаковок;

регистрация новых абонентов сети;

выдача абонентам ключевых упаковок;

регистрация открытых ключей ЭЦП абонентов;

выдача абонентам регистрационных файлов открытых ключей ЭЦП из справочника участников расчетной системы;

организация схемы оперативного оповещения абонентов обо всех изменениях, происходящих в сети (компрометация ключей в КБ, РКЦ или в РЦУК, восстановление засекреченной связи после компрометации ключей, включение новых абонентов и т.п.). Разработка парольной системы оповещения в сети и карточек оповещения;

ведение (управление изменениями) регистрационной БД абонентов сети.

ЗАКАЗ КЛЮЧЕВЫХ ДОКУМЕНТОВ

Заявка на изготовление новой серии ключевых упаковок для плановой смены ключей направляется ЗАКАЗЧИКОМ, как правило, за 6 месяцев до момента желаемого их получения. Количество требуемых ГМД определяется из расчета два ГМД на один заказываемый комплект.

Количество комплектов ***n*** в серии определяется количеством участников банковских расчетов. Рекомендуется осуществлять заказ с учетом дополнительных комплектов на случай компрометации либо порчи ключевых блокнотов. Например, $n = k \cdot 1{,}5$; где k — число пользователей (операторов КБ, администраторов безопасности АСБР, дежурных программистов смены, операторов КБ(РКЦ)), работающих в сети.

Допустимый срок эксплуатации серии ключей — 1 год. Допустимый срок хранения серии ключевых упаковок до ввода ее в эксплуатацию — 1 год.

РАЗВЕРТЫВАНИЕ КЛЮЧЕВОЙ СИСТЕМЫ. ПЕРВИЧНАЯ РЕГИСТРАЦИЯ АБОНЕНТОВ И ПОЛУЧЕНИЕ КЛЮЧЕВЫХ УПАКОВОК

При первичной регистрации все абоненты сети (участники расчетов) прибывают в РЦУК для регистрации и получения упаковки с ключами шифрования. При получении ключевой упаковки абонент проверяет ее целостность, номер и серию и расписывается в журнале получения ключей РЦУК.

Все участники расчетов при развертывании ключевой системы выполняют следующие операции:

получение в РЦУК упаковки с ключами шифрования и личных дискет с записанными при выполнении регистрации выдачи ключей шифрования атрибутов (реквизитов) участника расчетов;

формирование личных секретных и открытых ключей ЭЦП; формирование регистрационных файлов открытых ключей, печать бумажных регистрационных форм открытых ключей;

доставка в РЦУК регистрационных данных (регистрационных файлов и бумажных регистрационных форм открытых ключей); выполнение регистрации открытых ключей;

получение от администратора РЦУК регистрационных данных других участников расчетов для выполнения взаимной регистрации открытых ключей и возможности в последующем выполнять проверку ЭЦП под принимаемыми документами;

регистрация в БД рабочей станции (на своем рабочем месте) полученных регистрационных данных.

Вышеописанная процедура требует двух прибытий участников расчетов в РЦУК: первый раз для получения дискет с ключами шифрования, второй — для регистрации сформированных на рабочих местах открытых ключей ЭЦП.

Включение в систему нового пользователя, восстановление работы пользователя после компрометации выполняется по аналогичной схеме, приведенной на рис.14.

Регистрация открытых ключей ЭЦП, выполняемая в РЦУК, должна проводиться последовательно, сначала для администраторов СКЗИ, затем для дежурных программистов смены, затем для всех операторов КБ (РКЦ). Регистрации открытых ключей на рабочих местах предшествует получение регистрационных данных, получаемых участниками расчетов одновременно при регистрации своих открытых ключей ЭЦП.

Для "АРМ администратора безопасности СКЗИ" администратор РЦУК подготавливает регистрационные данные о дежурных программистах смены и операторах КБ (РКЦ).

Для "АРМ дежурного программиста смены АСБР" администратор РЦУК подготавливает регистрационные данные только об администраторах СКЗИ.

Для "АРМ абонента КБ(РКЦ)" администратор РЦУК подготавливает регистрационные данные только об администраторах СКЗИ.

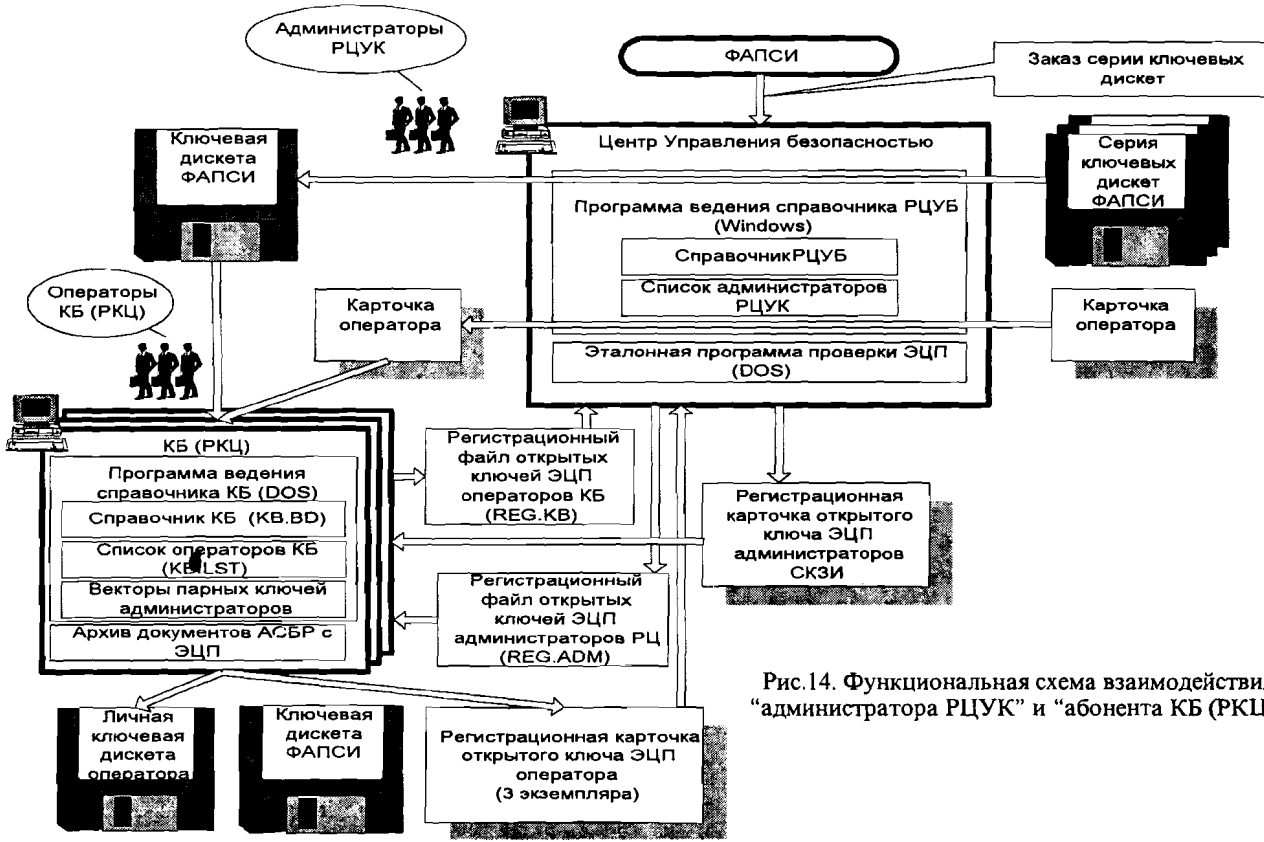

Рис.14. Функциональная схема взаимодействия "администратора РЦУК" и "абонента КБ (РКЦ)"

РЕГИСТРАЦИЯ ОТКРЫТЫХ КЛЮЧЕЙ АБОНЕНТОВ

Пользователи автоматизированной системы банковских расчетов, получив в РЦУК ключевые упаковки и личные дискеты с записанными на них личными атрибутами, самостоятельно формируют свои личные ключевые дискеты и записывают на них секретные ключи ЭЦП посредством "Программы генерации ключей ЭЦП и ведения БД ключевых элементов" (программа KEYGEN). Открытые ключи ЭЦП записываются на регистрационную дискету в регистрационный файл. Регистрационная дискета доставляется в РЦУК для регистрации открытых ключей. Вместе с регистрационным файлом в РЦУК доставляются регистрационные и контрольная карточки участников расчетов.

Регистрация в РЦУК открытых ключей ЭЦП каждого участника расчетов выполняется на АРМ РЦУК при помощи подпункта РЕГИСТРАЦИЯ пункта главного меню ВЕДЕНИЕ СПРАВОЧНИКА.

При выполнении регистрации открытых ключей программа последовательно для всех пользователей, информация о которых находится в регистрационном файле, выдает на экран значение всех атрибутов пользователя и значение его открытого ключа ЭЦП.

При полном совпадении значений отображаемых атрибутов и открытого ключа ЭЦП с атрибутами в регистрационной карточке можно выполнять регистрацию пользователя (кнопка ДА). Если значения различаются, то выполнять регистрацию открытого ключа нельзя (кнопка НЕТ).

Показ атрибутов последовательно выполняется для всех пользователей, информация о которых находится в регистрационном файле.

Формирование и выдача регистрационного файла зарегистрированных в БД участников расчетов выполняется при помощи подпункта ВЫДАЧА РЕГИСТРАЦИОННОГО ФАЙЛА пункта главного меню ВЕДЕНИЕ СПРАВОЧНИКА.

Администратор РЦУК подписывает регистрационную карточку участника расчетов и ставит на ней печать РЦУК. В случае, если регистрируемым участником расчетов является оператор КБ (РКЦ), то один экземпляр регистрационной карточки остается в РЦУК, второй (ксерокопия) — у участника расчетов. В случае, если регистрируемым участником расчетов является

администратор СКЗИ, то один экземпляр регистрационной карточки остается в РЦУК, второй (ксерокопия) — у участника расчетов, остальные экземпляры (ксерокопии) передаются в КБ и РКЦ. Подписанные участниками расчетов и администратором РЦУК регистрационные карточки (первые экземпляры) должны храниться в отдельной папке в сейфе РЦУК. Администратор РЦУК каждому прибывшему в РЦУК участнику расчетов выдает регистрационные файлы и соответствующие им регистрационные карточки (ксерокопии) абонентов сети, с которыми он будет устанавливать связь. Кроме того, каждому прибывшему в РЦУК участнику расчетов выдается "карточка оповещения", образец которой приведен ниже.

КАРТОЧКА ОПОВЕЩЕНИЯ

Телефоны администратора безопасности РЦУК	
Пароль РЦУК	
Пароль абонента	

В "карточке оповещения" указаны: телефоны РЦУК, пароль (кодовое слово) администратора РЦУК, уникальный пароль (кодовое слово), присвоенный участнику расчетов РЦУКом. "Карточка оповещения" используется участниками расчетов для сообщений о компрометации ключа по телефонным каналам общего пользования. "Карточка оповещения" должна храниться у абонента наравне с ключами. Участник расчетов должен зарегистрировать на своем АРМ открытые ключи абонентов (участников расчетов), с которыми он будет поддерживать связь. Регистрация на АРМ открытых ключей ЭЦП зарегистрированных в РЦУК абонентов выполняется выбором подпункта РЕГИСТРАЦИЯ ОТКРЫТЫХ КЛЮЧЕЙ пункта главного меню РЕГИСТРАЦИЯ.

При выполнении регистрации считывается информация из регистрационного файла и проверяется ее корректность. Затем на экран выдается значение хэш-функции, которое необходимо сравнить со значением хэш-функции, записанной на бумажном носителе. При совпадении значений хэш-функций и нажатии на кнопку РЕГИСТРАЦИЯ программа начнет выполнение регистрации открытых ключей ЭЦП и атрибутов их владельцев, информация о которых записана в регистрационном файле.

Если возникла необходимость удалить данные зарегистрированного пользователя, то в пункте главного меню ПРОСМОТР нужно выбрать соответствующий список участников. При выборе пункта подменю появится окно просмотра со списком, содержащим код и Ф.И.О. выбранной категории участников расчетов.

После выполнения изменения содержимого БД необходимо выполнить резервное копирование. Модификация содержимого БД происходит в следующих случаях:

- успешно сформированы обе личные ключевые дискеты для одного или нескольких новых пользователей и успешно создана регистрационная дискета с открытыми ключами ЭЦП;
- из БД удален зарегистрированный пользователь;
- успешно проведена регистрация открытых ключей ЭЦП администраторов СКЗИ с регистрационной дискеты, полученной в РЦУК.

Для создания резервной копии БД необходимо на заранее отформатированную дискету скопировать из рабочей директории (в которой расположен файл CRYDRV) файлы ADM.LST, MEMBER.BD и все файлы с именем, состоящим из 4-х цифр без расширения.

ПЛАНОВАЯ СМЕНА КЛЮЧЕЙ

Срок действия серии ключей определен в один год, после истечения которого необходимо выполнить процедуру плановой смены всех ключей, в том числе ключи ЭЦП.

РЦУК должен установить срок плановой смены ключей у абонентов сети, например, 01.01.199хг.

Новые упаковки ключей должны поступать в РЦУК не позднее, чем за месяц до плановой смены ключей в сети. После получения новые ключевые упаковки должны быть зарегистрированы в журнале регистрации ключей РЦУК и храниться в сейфе до выдачи их участникам расчетов.

Участник расчетов прибывает в РЦУК не позднее, чем за две недели до плановой смены ключей для получения новой ключевой упаковки. При получении новой ключевой упаковки участник расчетов проверяет ее целостность, номер и серию и расписывается в журнале регистрации ключей РЦУК.

Участник расчетов производит формирование секретного и открытого ключей ЭЦП на своем АРМ, записывает открытый ключ на специально выделенную для этого дискету, дублирует с помощью принтера код открытого ключа на бумажный носитель (регистрационные карточки), подписывает их и доставляет в РЦУК для регистрации не позднее, чем за неделю до плановой смены ключей.

Процесс регистрации новых открытых ключей ЭЦП в РЦУК происходит так же, как было описано ранее. Перевод работы СКЗИ "Янтарь АСБР" на новые плановые ключи осуществляется всеми участниками расчетов одновременно в день, предварительно указанный администратором РЦУК.

По завершении плановой смены ключи шифрования уничтожаются, а открытые ключи ЭЦП сохраняются в архивах для разбора конфликтных ситуаций (при необходимости).

ПОРЯДОК УНИЧТОЖЕНИЯ КЛЮЧЕЙ

Выведенные из действия после плановой смены ключевые комплекты ФАПСИ подлежат возврату в РЦУК для последующего уничтожения содержащейся на них информации. Ключевая информация уничтожается средствами программного обеспечения СКЗИ "Янтарь АСБР". ГМД подвергаются двойному форматированию (программа HOST, меню "Формат"). После этого ключевые дискеты разрезаются на две приблизительно равные части с помощью ножниц для резки по металлу. В случае, если дискета не форматируется, ее необходимо разрезать на части размером не более 1 см^2.

Абоненты — участники расчетов уничтожают выведенные из действия после плановой смены ключи шифрования и секретные ключи ЭЦП со всех магнитных носителей не позднее, чем через 1 сутки после момента вывода ключей из действия. С ЖМД ключи уничтожаются стиранием средствами DOS файла с ключами, имя которого совпадает с номером ключа абонента и состоит из 4-х цифр без расширения. Информация на личных ключевых дискетах уничтожается с помощью процесса двойного форматирования (программа HOST, меню "Формат"). После этого ключевые дискеты разрезаются на две приблизительно равные части с помощью ножниц для резки по металлу. В случае, если дискета не форматируется, ее необходимо разрезать на части размером не более 1 см^2.

После наступления дня плановой смены ключей в РЦУК уничтожаются все оставшиеся от предыдущей плановой смены резервные ключевые упаковки. Об уничтожении ключей участником расчетов делается запись в "Журнале АРМ". Администратором РЦУБ делается отметка об уничтожении ключевых дискет в графе "Примечание" Журнала регистрации (см. приложение 6).

3.6.5. Управление ключами при компрометации

КОМПРОМЕТАЦИЯ КЛЮЧЕВЫХ ДОКУМЕНТОВ

Под компрометацией ключевых документов понимается их утрата, хищение, несанкционированное копирование, передача их в линию связи в открытом виде, любые другие виды разглашения ключевой информации, а также случаи, когда нельзя достоверно установить, что произошло с магнитными носителями, содержащими ключевую информацию (в том числе случаи, когда ГМД вышел из строя и доказательно не опровергнута возможность того, что данный факт произошел в результате действий злоумышленника).

При компрометации любого из ключевых документов (личного ключевого ГМД администратора РЦУК, личного ключевого ГМД администратора безопасности АСБР, личного ключевого ГМД дежурного программиста, личного ключевого ГМД оператора КБ (РКЦ) и т.д.) все остальные ключевые ГМД данного абонента считаются скомпрометированными, и производится полная смена всех ключевых документов — ключевого комплекта "ДСРФ-***", личных ключевых ГМД ответственного исполнителя.

К событиям, связанным с компрометацией ключей, должны быть отнесены следующие факты:

- утрата ключевых дискет;
- утрата ключевых дискет с последующим обнаружением;
- увольнение сотрудников, имевших доступ к ключевой информации;
- возникновение подозрений на утечку информации или ее искажение в системе конфиденциальной связи;
- нерасшифровывание входящих или исходящих сообщений у абонентов;
- нарушение печати на сейфе с ключевыми дискетами.

Первые три события должны трактоваться как безусловная компрометация действующих ключей.

Три следующих события требуют специального рассмотрения в каждом конкретном случае.

При наступлении любого из перечисленных выше событий абонент должен немедленно прекратить связь с другими абонентами и сообщить о факте компрометации (или предполагаемом факте компрометации) в Центр управления безопасностью.

Центр управления безопасностью обязан оперативно оповестить всех абонентов сети о факте (или предполагаемой) компрометации.

Расследование факта (или предполагаемой) компрометации должно проводиться на месте происшествия группой безопасности объекта.

Результатом рассмотрения является квалификация или не квалификация данного события как компрометация действующих ключей.

Рассмотрим управление ключами при их компрометации.

РЕГЛАМЕНТАЦИЯ ДЕЙСТВИЙ ПЕРСОНАЛА В УСЛОВИЯХ КОМПРОМЕТАЦИИ КЛЮЧЕВЫХ ДОКУМЕНТОВ

Действия персонала при компрометации ключа в КБ и РКЦ

При компрометации ключа у абонента сети (оператора КБ, РКЦ, дежурного программиста смены) он должен немедленно прекратить работу в сети и сообщить о факте компрометации (или подозрении о происшедшей компрометации) администратору РЦУК с указанием времени компрометации. Сообщение о компрометации должно быть оперативно передано администратору РЦУК по телефону (с перепроверкой со стороны администратора РЦУК) с сообщением заранее условленного пароля (дежурный программист смены сообщает о компрометации путем личной явки в РЦУК). Пароль должен быть внесен в "карточку оповещения", которая выдается администратором РЦУК во время регистрации абонента. Абонент делает также соответствующие отметки в своем журнале АРМ. Одновременно, абонент готовит письменное уведомление о компрометации ключа (подписанное руководителем и заверенное печатью учреждения) и отправляет его в РЦУК. В данном уведомлении

должен быть указан номер ключа, его серия, а также время, дата и причина компрометации ключа.

Сразу после получения телефонного сообщения о компрометации администратор РЦУК дает указание (письменное или устное) администратору СКЗИ о блокировке связи с скомпрометированным абонентом и делает соответствующие отметки в журнале сети, кроме того, он удаляет из своей базы данных скомпрометированного абонента и делает соответствующую отметку в своем журнале.

Администратор СКЗИ после получения данного указания блокирует связь (с помощью кнопки БЛОКИРОВКА СОЕДИНЕНИЙ программы DUP) с скомпрометированным абонентом и делает соответствующую отметку в своем журнале, кроме того, он удаляет из своей базы данных скомпрометированного абонента и также делает соответствующую отметку в своем журнале.

Письменное уведомление о компрометации ключа администратор РЦУК хранит для разбора конфликтных ситуаций.

Администратор РЦУК производит формирование и выдачу для администратора СКЗИ нового регистрационного файла зарегистрированных в БД участников расчетов, которые выполняются при помощи подпункта ВЫДАЧА РЕГИСТРАЦИОННОГО ФАЙЛА пункта главного меню ВЕДЕНИЕ СПРАВОЧНИКА.

Затем администратор РЦУК производит формирование и выдачу для администратора СКЗИ нового файла списка участников, находящихся в БД участников расчетов.

Абонент обязан обеспечить доставку выведенных из действия (после компрометации) ключевых документов в РЦУК.

Уничтожение выведенных из действия ключевых документов производится в соответствии с разделом "порядок уничтожения ключей" настоящего документа только после установления причин, обстоятельств и последствий компрометации.

Действия персонала при компрометации ключа у администратора СКЗИ

При компрометации ключа у администратора СКЗИ, он должен немедленно прекратить работу в сети (осуществить плавную остановку криптосервера, нажав на клавишу ПРИОСТАНОВЛЕНИЕ СОЕДИНЕНИЙ) и сообщить о факте ком-

прометации (или подозрении о происшедшей компрометации) администратору РЦУК с указанием времени компрометации и причины. Сообщение о компрометации должно быть оперативно передано в РЦУК по телефону (с перепроверкой сообщения) с сообщением заранее условленного пароля или путем личной явки администратора СКЗИ в РЦУК. Пароль должен быть указан в "карточке оповещения", которая выдается администратором РЦУК во время регистрации открытого ключа администратора СКЗИ в РЦУК. Одновременно скомпрометированный администратор СКЗИ готовит письменное уведомление о компрометации ключа (подписанное руководителем организации и заверенное печатью) и отправляет его в РЦУК. В данном уведомлении должен быть указан номер ключа, его серия, а также время, дата и причина компрометации ключа.

Сразу после получения сообщения администратор РЦУК оповещает все КБ и РКЦ о необходимости прекращения связи с скомпрометированным администратором СКЗИ и делает соответствующие отметки в журнале событий, кроме того он удаляет из своей базы данных скомпрометированного администратора СКЗИ и также делает соответствующую отметку в своем журнале. Просмотр и удаление зарегистрированных в БД участников расчетов выполняется при помощи подпункта ПРОСМОТР пункта главного меню ВЕДЕНИЕ СПРАВОЧНИКА. Для удаления участника расчетов необходимо выбрать нужного участника и нажать на кнопку УДАЛИТЬ. Удаление выполняется только после подтверждения удаления.

Оповещение абонентов производится РЦУК по телефонным каналам с сообщением пароля РЦУК, который указан в "карточке оповещения", и перепроверкой. Все абоненты (КБ, РКЦ, дежурный программист смены) после получения сообщения о компрометации удаляют из своих баз данных, включив режим ПРОСМОТР, скомпрометированного администратора СКЗИ и делают соответствующую отметку в своем "Журнале АРМ".

Письменное уведомление о компрометации ключа администратор РЦУК хранит для разбора конфликтных ситуаций.

Восстановление связи после компрометации ключа у оператора КБ (РКЦ)

Абонент (оператор КБ, РКЦ), у которого были скомпрометированы ключи (или другое должностное лицо, которому будет доверено получение новых ключевых документов), обращается в РЦУК для получения новой (резервной) упаковки ключевых документов. Процесс регистрации нового открытого ключа подписи происходит так же, как и при плановой смене ключей.

После регистрации нового открытого ключа ЭЦП восстанавливаемого абонента администратор РЦУК передает администратору СКЗИ регистрационный файл с новым открытым ключом оператора КБ (РКЦ).

Регистрация в БД АРМ администратора безопасности СКЗИ нового открытого ключа ЭЦП, зарегистрированного в РЦУК, восстанавливаемого абонента выполняется при помощи подпункта РЕГИСТРАЦИЯ пункта главного меню ВЕДЕНИЕ СПРАВОЧНИКА.

С целью более оперативного восстановления связи после компрометации ключа в КБ (РКЦ) предлагается, например, заместителю руководителя организации (КБ, РКЦ) зарегистрироваться в РЦУК в качестве абонента сети (одновременно со своим оператором), получить на себя упаковку с ключевыми документами, произвести генерацию секретного и открытого ключей подписи и пройти соответствующую регистрацию открытого ключа. Все имеющиеся у него ключевые документы он должен хранить в собственном сейфе. После наступления события, квалифицируемого как факт компрометации ключей у оператора, и оповещения РЦУК о компрометации, заместитель руководителя организации может либо взять на себя функции оператора, либо доверить эти полномочия другому должностному лицу. Поскольку в БД АРМ администратора безопасности СКЗИ его ключи уже существуют с момента регистрации, то скомпрометированный абонент может тут же начать работу на новых ключах. Однако доверенный представитель этой организации (КБ, РКЦ) все равно должен прибыть в РЦУК для получения и регистрации новых ключей на случай повторной компрометации ключей и оперативного восстановления засекреченной связи в соответствии с данным алгоритмом.

Восстановление связи после компрометации ключа у администратора СКЗИ

Администратор СКЗИ, у которого были скомпрометированы ключи (или другое должностное лицо, которому будет доверено получение новых ключевых документов), обращается в РЦУК для получения новой (резервной) упаковки ключевых документов. Процесс регистрации нового открытого ключа подписи происходит так же, как и при плановой смене ключей.

После регистрации нового открытого ключа ЭЦП РЦУК пересылает всем абонентам сети заверенные им копии регистрационной карточки с новым открытым ключом ЭЦП скомпрометированного администратора СКЗИ. Все абоненты сети (КБ, РКЦ) добавляют новую регистрационную запись в свои справочники. Регистрация открытых ключей ЭЦП, зарегистрированного в РЦУК администратора СКЗИ выполняется выбором подпункта РЕГИСТРАЦИЯ ОТКРЫТЫХ КЛЮЧЕЙ пункта главного меню РЕГИСТРАЦИЯ на АРМ абонента КБ(РКЦ).

С целью более оперативного восстановления связи после компрометации ключа предлагается, например, начальнику отдела организации и эксплуатации СКЗИ "Янтарь АСБР" или его заместителю зарегистрироваться в РЦУК в качестве администратора СКЗИ, получить на себя упаковку с ключевыми документами, произвести генерацию секретного и открытого ключей подписи и пройти соответствующую регистрацию открытого ключа. Все имеющиеся у него ключевые документы он должен хранить в собственном сейфе. После наступления события, квалифицируемого как факт компрометации ключей, и оповещения администратора РЦУК о компрометации, он может либо взять на себя функции администратора СКЗИ, либо доверить эти полномочия другому должностному лицу (например, либо прежнему, либо новому администратору СКЗИ). Поскольку в БД ключей остальных абонентов его ключи уже существуют с момента регистрации, то он может тут же начать работу на новых ключах.

3.6.6. Создание личных ключей

В документах организации детально расписывается порядок выдачи, формирования и регистрации различных личных ключей, который охватывает следующие положения:

формирование личных ключевых дискет для администраторов РЦУК;

порядок выдачи администратором РЦУК упаковок ключевых дискет всем категориям пользователей;

порядок формирования личных секретных и открытых ключей ЭЦП и подготовка регистрационных данных;

порядок регистрации личных открытых ключей ЭЦП в РЦУК и выдача им регистрационных данных о других участниках расчетов;

порядок регистрации личных открытых ключей ЭЦП на АРМ администраторов СКЗИ;

порядок регистрации личных открытых ключей ЭЦП на АРМ операторов КБ(РКЦ) и АРМ дежурных программистов смены.

В частности, для подготовки личных ключевых дискет участникам расчетов АСБР администратору РЦУК необходимо иметь по одному ключевому комплекту ФАПСИ и по две чистые отформатированные дискеты на каждого пользователя. Запись на личные дискеты в РЦУК используемых в системе реквизитов (атрибутов) участников расчетов позволяет избежать их повторного ввода. Следовательно, можно избежать ошибок, которые будут выявляться на этапе регистрации открытых ключей ЭЦП в РЦУК.

В РЦУК процесс начинается с запуска программы CUB.

Перед запуском программы CUB необходимо загрузить в оперативное запоминающее устройство (ОЗУ) драйвер-датчик случайных чисел (ДСЧ) CYPRASW СКЗИ "Верба". Программа CUB может быть запущена двойным нажатием кнопки мыши на изображение символа программы. После запуска программа CUB выполняет самоконтроль целостности и контроль целостности БД, для чего запрашивает личную ключевую дискету администратора РЦУК. После установки дискеты администратор должен нажать на кнопку ОК. При успешной проверке целостности БД программа переходит в главное меню.

Далее происходит формирование дискет с атрибутами участника расчетов для всех категорий пользователей.

Выбирается в главном меню программы CUB пункт ВЕДЕНИЕ СПРАВОЧНИКА, подпункт ВЫДАЧА КЛЮЧЕВЫХ ДИСКЕТ, категория пользователя. После выдачи на экран формы карточки участника электронных расчетов заполняются все поля. Поле ввода данных КОД УЧАСТНИКА заполняется только латинскими буквами. В поле ввода КОД ОРГАНИЗАЦИИ необходимо ввести девятизначный банковский код МФО организации. Поля ввода ОРГАНИЗАЦИЯ и Ф.И.О. можно заполнять любыми буквами и нельзя оставлять пустыми. В поля ввода СЕРИЯ и НОМЕР КЛЮЧА необходимо ввести шестизначный порядковый номер серии и четырехзначный номер комплекта соответственно, совпадающие с номерами, записанными на этикетке ключевого комплекта. После заполнения полей формы необходимо нажать на кнопку ОК. Программа проверит корректность заполнения полей формы и выдаст запрос на установку первой личной дискеты для записи на нее атрибутов пользователя и выданных ему ключевых дискет.

В процессе изложенной выше процедуры производится запись на первую и вторую личную ключевую дискету атрибутов (реквизитов) участника расчетов (файл user) и выполняется модификация файла member.bd (БД пользователей).

После завершения процедуры выдачи ключевых дискет одному пользователю администратор РЦУК может начать процедуру выдачи ключевых дискет ФАПСИ следующему пользователю. Затем производится выдача ключевых дискет и атрибутов участника расчетов пользователям.

На этикетку ключевого диска наносятся:

- надписи ЛИЧНАЯ, Ф.И.О. пользователя, порядковый номер дискеты (1 или 2);
- наименование исходного ключевого комплекта "ДСРФ-***", где *** — трехзначный номер;
- шестизначный порядковый номер серии и четырехзначный номер комплекта, совпадающие с номерами, записанными на этикетке ключевого комплекта;
- год выпуска.

Например:

ЛИЧНАЯ, Петров Петр Петрович, 1
ДСРФ-***
000600-0023
1996

Администратор РЦУК фиксирует факт выдачи ключевых документов ответственному исполнителю или доверенному представителю в "Журнале регистрации ключей".

Этот пример одной из множества операций подчеркивает сложность и ответственность многогранного процесса создания личных ключевых документов. Строгое и подробное описание каждой процедуры создания личных ключей изложено в материалах организации-пользователя и разнообразной эксплуатационной документации.

3.6.7. Порядок загрузки ключей на криптографический сервер

Полученная ключевая информация загружается в криптографический сервер для обеспечения защищенного режима работы АСБР. Для этого проводится инициализация криптографического сервера системы DEC AXP OpenVMS CryptSystem. Инициализация заключается в загрузке в криптографическую систему ключевых элементов дежурного программиста смены и администраторов СКЗИ. Необходимость данной загрузки ключей конкретно обусловливается необходимостью в дальнейшем устанавливать закрытый канал связи между криптографической системой и диалоговой управляющей программой АРМ администратора СКЗИ, соединенных между собой посредством локальной вычислительной сети.

"Программа начальной инициализации системы DEC AXP OpenVMS CryptSystem" (программа MKEYS) предназначена для работы на АРМ дежурного программиста. ПЭВМ должна быть соединена с сервером DEC AXP через последовательный порт "нуль-модемным" кабелем, обеспечивающим полный протокол асинхронной передачи данных (асинхронный коммуникационный интерфейс RS-232C).

В процессе работы программа MKEYS выполняет обращения к криптографическому драйверу CRYDRV, который должен быть обязательно загружен в ОЗУ, и к файлам базы данных (БД) открытых ключей, которые должны располагаться в

той же директории, в которой располагается криптографический драйвер CRYDRV.EXE.

Программа MKEYS может быть запущена из командной строки DOS при помощи команды

MKEYS <номер_порта>,

где <номер_порта> — параметр командной строки, указывающий номер последовательного порта ПЭВМ, через который выполняется передача данных на криптографическую систему DEC AXP OpenVMS CryptSystem. В начале работы программы MKEYS выполняет самоконтроль целостности СКЗИ.

Остальная работа программы выполняется в автоматическом режиме и не требует каких-либо действий. По окончании работы программа выдает количество ключевых элементов шифрования, загруженных на DEC AXP OpenVMS CryptSystem. Количество загруженных ключей должно соответствовать числу администраторов безопасности СКЗИ. Дежурный программист делает отметку о загрузке ключей в "Журнале АРМ дежурного программиста".

Загрузка на криптографический сервер системы DEC AXP OpenVMS CryptSystem ключей зарегистрированных абонентов осуществляется с помощью программы DUP. Диалоговая управляющая программа работает под управлением MS Windows на АРМ администратора безопасности СКЗИ СКЗИ. Диалоговая управляющая программа обеспечивает передачу криптографическому серверу команд и прием от него информации о его состоянии. LOG-протокол работы диалоговой управляющей программы ведется средствами DEC AXP OpenVMS CryptSystem в отдельном LOG-протоколе на DEC AXP.

При успешной проверке целостности БД программа выполняет установление соединения с криптографическим сервером. При успешном установлении соединения программа переходит в главное окно диалоговой управляющей программы. Но если дежурным программистом АСБР криптосервер не запущен, то выдается сообщение об ошибке.

После установления соединения и выполнения строгой аутентификации программа получает статус состояния криптографического сервера. В начальный момент криптографический сервер не содержит загруженной таблицы ключей и первой операцией, которую необходимо выполнить, является опе-

рация загрузки в криптографический сервер таблицы ключей зарегистрированных абонентов.

Обслуживание криптографическим сервером запросов прикладных задач возможно только после загрузки таблицы ключей. При выполнении запросов от прикладных задач криптографический сервер сохраняет информацию о выполненных операциях и передает их в диалоговую управляющую программу, когда она выдает запрос на получение состояния сервера.

Администратор безопасности СКЗИ делает отметку о загрузке таблицы ключей в "Журнале АРМ администратора безопасности СКЗИ".

3.7. ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ПРИМЕНЕНИЯ СКЗИ

3.7.1. Общие правила

Средствами СКЗИ "Янтарь АСБР" допускается защищать только ограниченного распространения информацию, не составляющую государственной тайны. Минимальные требования к заявителю на право установки и эксплуатации сертифицированных ФАПСИ шифровальных средств и предоставления услуг по шифрованию информации при защите информации по уровню "С" изложены в приложении 2.

Заданный уровень защиты "С" и подлинность передаваемой информации обеспечиваются при выполнении следующих условий:

- сохранении от компрометации ключевой информации;
- сохранении в тайне паролей пользователей, выполненных в соответствии с требованиями (см. приложение 3) на носителях touch-memory;
- отсутствии закладок в используемом программном и аппаратном обеспечении в том числе в DOS и BIOS;
- соблюдении организационно-технических мер, препятствующих извлечению платы "Аккорд" из ПЭВМ.

Эксплуатация СКЗИ "Янтарь АСБР" разрешается только в организациях, имеющих лицензию на эксплуатацию средств криптографической защиты данных. Правом доступа к АРМ с установленными СКЗИ "Янтарь АСБР" должны обладать

только определенные для эксплуатации лица, прошедшие соответствующую подготовку, изучившие эксплуатационную документацию.

3.7.2. Требования по размещению, охране и специальному оборудованию объектов с СКЗИ "Янтарь АСБР"

Помещения, в которых размещаются средства СКЗИ "ЯНТАРЬ АСБР" должны удовлетворять требованиям документа "Методические рекомендации по обеспечению безопасности конфиденциальной банковской информации (несекретной) при проектировании объектов и помещений для размещения СКЗБИ" от 10.06.94.

Должны быть приняты меры по исключению несанкционированного доступа посторонних лиц в помещения.

Во вне рабочее время помещения должны быть опечатаны.

Помещения и технические средства, расположенные в них, должны пройти проверку на отсутствие в них электронных устройств перехвата информации (закладок).

Размещение, охрана и специальное оборудование помещений должны обеспечивать сохранность информации, криптоключей, невозможность неконтролируемого доступа к СКЗИ, прослушивания ведущихся там переговоров и просмотра процедур работы с СКЗИ посторонними лицами.

Двери и окна помещений оборудуются охранной сигнализацией. При расположении помещений на первых и последних этажах зданий, а также при наличии рядом с окнами балконов, пожарных лестниц и т.п., окна помещений оборудуются внутренними раздвижными металлическими решетками или ставнями.

Для хранения криптоключей, нормативной и эксплуатационной документации помещения обеспечиваются металлическими шкафами (хранилищами, сейфами), оборудованными внутренними замками с двумя экземплярами ключей. Запасные экземпляры ключей от хранилищ и входных дверей должны храниться в сейфе руководителя учреждения или руководителя службы безопасности. Хранилища, предназначенные для магнитных носителей с криптоключами или программным обеспечением, должны быть надежно заземлены.

Личные ключевые дискеты и ключевые дискеты ФАПСИ каждого пользователя должны храниться в металлическом контейнере, приспособленном для опечатывания. Пользователи должны иметь личную металлическую печать для опечатывания контейнера.

По окончании рабочего дня (а в случаях длительного отсутствия и в течение рабочего дня) помещения, а также находящиеся вне их другие хранилища с криптоключами, закрываются и ставятся под сигнализацию, извещатели которой могут выходить на посты ведомственной или вневедомственной охраны. Сдача под охрану производится с указанием времени приема-сдачи в журнале установленной формы. Рабочие экземпляры ключей от хранилищ передаются в опечатанном пенале охране или дежурному по управленческо-финансовому учреждению под расписку в журнале приема (сдачи) под охрану.

Устанавливаемый руководителем учреждения порядок охраны помещений объектов СКЗИ должен предусматривать периодический контроль технического состояния средств охранной сигнализации и соблюдения режима охраны с отражением в журнале проверок, находящимся в службе охраны.

На время отсутствия пользователей в зоне безопасности и контроля за этой зоной со стороны службы безопасности оборудование СКЗИ, в котором установлены средства криптографической защиты, должно отключаться от сети питания.

В соответствии с направлениями своей деятельности отдел организации и эксплуатации СКЗИ "Янтарь АСБР" должен быть расположен в двух отдельных помещениях:

- помещении РЦУК;
- помещении администраторов СКЗИ.

В помещении регионального центра управления ключами (РЦУК) организуются рабочие места начальника отдела и главного инженера — администратора РЦУК.

Помещение РЦУК должно быть разделено на две части (перегорожено барьером): в одной части располагаются рабочие места сотрудников РЦУК, другая предназначена для приема посетителей. В помещение допускаются только пользователи для получения необходимых криптоматериалов. Во время изготовления криптоматериалов и проведения контрольных и регламентных работ с СКЗИ допуск пользователей в эти помещения не разрешается.

В помещение РЦУК должны находиться следующие технические и оргсредства:

- сейф или металлический шкаф с двумя комплектами ключей и приспособлением для опечатывания для хранения ключевых документов, изготовленных в ФАПСИ, резиновой печати, журналов и регистрационных карточек открытых ключей ЭЦП абонентов сети;
- журнал зарегистрированных абонентов;
- журнал регистрации имеющихся в наличии и выданных абонентам упаковок с ключевыми дискетами;
- журнал ежедневного учета событий, происходящих в сети;
- резиновая печать РЦУК;
- металлическая печать для опечатывания помещения и сейфа (шкафа);
- ПЭВМ типа IBM PC 486 — Pentium (АРМ администратора РЦУК);
- выделенная (не подключенная к сети) ПЭВМ типа IBM PC 486 — Pentium для генерации ключей абонента;
- принтер;
- аппарат для получения ксерокопий;
- телефонные аппараты (с отдельными номерами) — 2 шт.

В помещении администраторов СКЗИ организуется работа дежурного администратора СКЗИ. Доступ в помещение должны иметь только администраторы СКЗИ.

В помещении администраторов СКЗИ должны располагаться следующие технические и оргсредства:

- сейф или металлический шкаф с двумя комплектами ключей и приспособлением для опечатывания, предназначенный для хранения личных ключевых документов, журналов и регистрационных карточек открытых ключей ЭЦП абонентов сети;
- журнал ежедневного учета событий, происходящих в сети;
- папка для хранения регистрационных карточек открытых ключей ЭЦП абонентов сети;
- металлическая печать для опечатывания помещения и сейфа (шкафа);
- ПЭВМ типа IBM PC 386 — 486 (АРМ администратора СКЗИ);

- принтер;
- телефонный аппарат — 1 шт.

Для эксплуатации СКЗИ "Янтарь АСБР" в ГРКЦ, РКЦ и КБ должны быть выделены отдельные помещения.

В помещении организуются рабочие места операторов КБ(РКЦ) и администратора безопасности КБ(РКЦ).

В помещении должны располагаться следующие технические и оргсредства:

- сейф или металлический шкаф с двумя комплектами ключей и приспособлением для опечатывания, предназначенный для хранения личных ключевых документов, журналов и регистрационных карточек открытых ключей ЭЦП абонентов сети;
- журнал абонента сети;
- папка для хранения регистрационных карточек открытых ключей ЭЦП абонентов сети;
- металлическая печать для опечатывания помещения и сейфа (шкафа);
- ПЭВМ типа IBM PC 386 — 486 (АРМ оператора КБ(РКЦ));
- принтер;
- телефонный аппарат — 1 шт.

Для эксплуатации серверной части СКЗИ "Янтарь АСБР" должно быть выделено отдельное помещение. Помещение, в котором установлен вычислительный комплекс DEC AXP и его системные консоли, является режимным. Вход в данное помещение осуществляется при условии аутентификации персонала.

В помещении организуются рабочие места администратора системы и дежурного программиста смены. В помещении должны находиться следующие технические и оргсредства:

- сейф или металлический шкаф с двумя комплектами ключей и приспособлением для опечатывания для хранения ключевых документов, изготовленных в ФАПСИ;
- вычислительный комплекс DEC AXP;
- системные консоли (АРМ администратора системы);
- металлическая печать для опечатывания помещения и сейфа (шкафа);
- ПЭВМ типа IBM PC 386 — 486 (АРМ администратора РЦУК);

- выделенная (не подключенная к сети) ПЭВМ типа IBM PC 386 — 486(АРМ дежурного программиста смены АСБР);
- принтер;
- аппарат для получения ксерокопий;
- телефонные аппараты (с отдельными номерами) — 2 шт.

3.7.3. Защита программного обеспечения СКЗИ "Янтарь АСБР"

Программное обеспечение СКЗИ "Янтарь АСБР" в свою очередь также нуждается в защите от несанкционированного доступа (НСД). Наибольшую угрозу для него представляют внутренние пользователи. В этом случае максимальной эффективностью по обеспечению безопасности программного обеспечения (ПО) обладает комплекс аппаратных средств и организационно-технических мероприятий. Для этих целей в СКЗИ "Янтарь АСБР" используется комплекс "Аккорд", предназначенный для защиты информации от несанкционированного доступа и обеспечения конфиденциальности информации при ее обработке в ПЭВМ. Комплекс "Аккорд" работает в MS DOS версий 3.10 и выше. Объем дискового пространства для размещения программных средств комплекса "Аккорд" составляет около 700 Кбайт на логическом диске "С" и около 10 Кбайт на физическом диске С. Этот комплекс является преимущественно аппаратным средством с программной поддержкой.

Комплекс "Аккорд" обеспечивает:

идентификацию, проверку подлинности и контроль доступа субъектов: в систему (ПЭВМ); к внешним устройствам ПЭВМ; к файлам, томам, каталогам;

регистрацию и учет: входа (выхода) субъектов доступа в (из) системы; запуска (завершения) программ и процессов (заданий, задач); доступа программ субъектов к защищаемым файлам, включая их создание и удаление; доступа программ субъектов доступа к внешним устройствам ПЭВМ; изменение полномочий субъектов доступа; создаваемых защищаемых объектов доступа;

обеспечение целостности программных средств и обрабатываемой информации.

Комплектность комплекса "Аккорд" (СТЮИ.00506-02 ТУ) приведена в табл.3.

Таблица 3

Обозначения	Наименование
СТЮИ.00506-02 91	Программные средства комплекса "Аккорд"
СТЮИ.00506-02 92	Контролер
СТЮИ.00506-02 93	Съемник
СТЮИ.00506-02 94	Идентификатор
СТЮИ.00506-02 ЭД	Ведомость эксплуатационной документации

Однако применение комплекса "Аккорд" максимально эффективно при проведении мер организационного характера изложенных ниже.

Средства защиты информации от НСД программного обеспечения АРМ оператора КБ(РКЦ) в организациях — абонентах системы должны обслуживаться администраторами информационной безопасности этих организаций. Средства защиты от НСД в криптографической системе DEC AXP OpenVMS CryptSystem должны обслуживаться администратором системы.

Процедура загрузки ключей в криптосервер осуществляется последовательно дежурным программистом смены и администратором безопасности АСБР. Оперативное управление криптосервером и контроль его функционирования осуществляется администратором безопасности АСБР.

Все файловые системы всех ПЭВМ, используемых в СКЗИ "Янтарь АСБР", должны содержать только файлы, необходимые для эксплуатации. Системные блоки ПЭВМ после установки технических средств и программного обеспечения и настройки их на требуемую конфигурацию, а также все накопители внешних устройств DEC AXP должны быть опечатаны специально выделенной для этих целей печатью. Администратор информационной безопасности должен периодически (не реже одного раза в сутки) проводить контроль сохранности входящего в состав ПЭВМ оборудования и печатей системных блоков. Наряду с этим допускается применение других дополнительных средств контроля за доступом к ПЭВМ.

Для предотвращения внесения в компьютер программно-аппаратных закладок и программ вирусов каждый раз при включении питания АРМ должен проводиться с помощью ПАК "Аккорд" контроль целостности программного обеспечения установленного на АРМ.

Кроме того, администратор информационной безопасности должен периодически (не реже одного раза в два месяца) проводить контроль целостности и легальности установленных копий ПО на АРМах СКЗИ "Янтарь АСБР" с помощью программ верификации, входящих в комплект СКЗИ "Янтарь АСБР", в соответствии с "Руководством оператора" ЯЦИТ.00004-01 34 12.

В случае обнаружения "посторонних" (не зарегистрированных) программ, нарушения целостности программного обеспечения либо выявления факта повреждения печатей на системных блоках работа на АРМ должна быть прекращена. По данному факту должно быть проведено служебное расследование комиссией в составе представителей служб информационной безопасности организации-владельца сети и организации-абонента сети, где произошло нарушение, и организованы работы по анализу и ликвидации негативных последствий данного нарушения. При необходимости к работе комиссии могут быть привлечены представители ФАПСИ, организаций-разработчиков СКЗИ, АСБР и сетевого оборудования.

АРМы администратора безопасности АСБР и подключаемые к ЛВС Ethernet АРМы операторов КБ (РКЦ) должны подключаться к выделенному сегменту ЛВС. АРМы дежурного программиста смены не должны быть подключены ни к какой сети компьютерной связи и должны использоваться только для работы в режиме АРМ дежурного программиста смены.

Системные блоки ПЭВМ должны быть опечатаны специально выделенной для этих целей печатью. Наряду с этим допускается применение других дополнительных средств контроля за доступом к ПЭВМ.

Администратор безопасности должен периодически (не реже одного раза в сутки) проводить контроль сохранности входящего в состав ПЭВМ оборудования и печатей системных блоков.

Вскрытие системных блоков при необходимости ремонта должно осуществляться при наличие разрешения на вскрытие руководителя службы информационной безопасности. Вся ключевая информация, хранящаяся на жестком диске, должна быть до вскрытия удалена с него в соответствии с "Инструкцией по порядку заказа, смены и уничтожения ключевых элементов" (ЯЦИТ.00004-01 94). В случае невозможности удале-

ния ключевой информации жесткий диск после вскрытия должен быть уничтожен путем разрезания на части размером не более 1 см^2 с помощью ножниц для резки по металлу. Все действия по вскрытию и уничтожению ключей должны визуально контролироваться службой информационной безопасности и защиты информации организации-владельца системы.

Запрещается:

1) осуществлять копирование ключевых носителей;

2) разглашать содержимое носителей ключевой информации или передавать сами носители лицам, к ним не допущенным, выводить ключевую информацию на дисплей и принтер;

3) вставлять ключевой ГМД в дисковод ПЭВМ в режимах, не предусмотренных функционированием СКЗИ, а также в дисководы других ПЭВМ;

4) записывать на ГМД с ключами постороннюю информацию;

5) работать на компьютере, если во время его начальной загрузки не проходит встроенный тест;

6) при включенном питании и загруженном специальном программном обеспечении СКЗИ оставлять без контроля ПЭВМ;

7) обрабатывать на ПЭВМ, оснащенной СКЗИ "Янтарь АСБР" секретную информацию;

8) использовать бывшие в работе ключевые ГМД;

9) производить несанкционированное подключение ПЭВМ к локальной сети, а также подключать без согласования с разработчиком СКЗИ к ПЭВМ дополнительные устройства и соединители, не предусмотренные в комплектации;

10) использовать в выделенных сегментах локальной сети при наличии в них маршрутизаторов любых сетевых протоколов кроме DECnet;

11) вносить какие-либо изменения в программное обеспечение СКЗИ;

12) несанкционированно устанавливать, создавать и выполнять на ПЭВМ посторонние программы;

13) осуществлять несанкционированное вскрытие системных блоков ПЭВМ;

14) приносить и использовать в помещениях, где размещены средства СКЗИ, радиотелефоны и другую радиопередающую аппаратуру.

Защита от НСД криптографической системы DEC AXP CryptSystem осуществляется средствами операционной системы Open VMS. Программное обеспечение, реализующее алгоритмы криптозащиты, выполнено таким образом, что все сегменты данных всех исполняемых файлов, работающих под управлением Open VMS, не перемещаются в swap-память на внешние носители. Программное обеспечение, позволяющее производить монтирование файловых систем Open VMS DEC AXP на другие ЭВМ, а также монтирование файловых систем других ЭВМ на Open VMS DEC AXP не применяется. Должны быть выполнены следующие требования:

1. Создание списка пользователей и добавление в список нового пользователя в Open VMS должно осуществляться только администратором системы.

2. Создание идентификаторов доступа в системной базе данных прав доступа и выдача созданных идентификаторов пользователям в Open VMS должно осуществляться только администратором системы.

3. Доступ к управлению привилегиями, квотами и установке прав доступа пользователей к файловой системе Open VMS должен иметь только администратор системы.

4. Управление привилегиями и квотами Open VMS осуществляется для каждого пользователя персонально на основе его системной учетной информации.

5. Права доступа каждого пользователя к файловой системе Open VMS определяются администратором системы в соответствии с правилами эксплуатации системы.

6. Пользователи Open VMS должны иметь доступ только к собственным разделам на смонтированных файловых томах. Доступа к смонтированным файловым томам в целом пользователи иметь не должны.

7. Проведение регламентных работ с остановом или перезагрузкой Open VMS производится в присутствии и под руководством администратора системы.

8. На ЭВМ DEC AXP, предназначенной для постоянной эксплуатации системы, не должны устанавливаться средства разработки программного обеспечения.

Все действия администратора системы должны визуально контролироваться службой информационной безопасности и защиты информации организации- владельца системы.

Установка комплекса "Аккорд" на АРМ выполняется специалистами поставщика ККСЗ или представителями службы информационной безопасности организации-владельца ККСЗ.

Настройка комплекса "Аккорд" на требуемую конфигурацию выполняется администратором информационной безопасности.

Перед эксплуатацией ПАК "Аккорд" в составе АРМ СКЗИ "Янтарь АСБР" необходимо внимательно ознакомиться с комплектом документации на данный комплекс, в том числе принять необходимые защитные оргмеры, рекомендуемые в документации на комплекс "Аккорд" (например, в "Руководстве администратора" СТЮИ.00506-02 90).

Применение защитных мер комплекса "Аккорд" должно дополняться общими мерами предосторожности и физической безопасности ПЭВМ. Для эффективного применения комплекса "Аккорд" и поддержания уровня защищенности необходимы следующие организационные меры:

1) администратор информационной безопасности и пользователи обязаны использовать периодически обновляемые пароли;

2) администратор информационной безопасности обязан следить за целостностью файлов;

3) программы, закрепленные за пользователями, не должны иметь возможность запуска интерпретатора командной строки DOS, доступа к дискам по абсолютным секторам, возможность прямого редактирования памяти;

4) администратор информационной безопасности должен регулярно анализировать содержание системного журнала;

5) администратор информационной безопасности должен довести до пользователей распоряжение о запрете снятия задач с выполнения при помощи выключения питания или нажатия на кнопку RESET;

6) при отказах и сбоях в работе средств защиты от НСД (ПАК "Аккорд") необходимо произвести замену вышедшего из строя ПАК "Аккорд" на исправный;

7) при утере пользователем личного ТМ-идентификатора администратор должен удалить с АРМ пользователя, утерявшего идентификатор, выдать ему новый идентификатор, провести регистрацию пользователя на АРМ с учетом нового идентификатора.

Администратор информационной безопасности (пользователь) должен предварительно выбрать и запомнить пароль, который он будет набирать на клавиатуре. При этом необходимо руководствоваться требованиями, изложенными в приложении 3.

4. ПОРЯДОК РАЗБОРА КОНФЛИКТНЫХ СИТУАЦИЙ, СВЯЗАННЫХ С ПРИМЕНЕНИЕМ ЭЦП

Наивно было бы предполагать, что ни один из участников платежной системы не использовал бы возможность при возникновении спорных ситуаций уйти от ответственности за нарушение правил проведения платежей и т.п.

Действующие в России автоматизированные системы передачи данных в большинстве своем имеют недостаток, который заключается в том, что они не дают возможности юридически значимой проверки авторства пересылаемых документов. Решение проблемы авторства документа может быть достигнуто с использованием сертифицированной электронно-цифровой подписи — средства, позволяющего однозначно и юридически значимо установить авторство и подлинность документа. Международная организация по стандартизации ISO предлагает использовать средство "цифровая подпись" (ЭЦП), позволяющее устанавливать подлинность автора сообщения (электронного документа) при возникновении спора относительно авторства этого сообщения, которое передается по сетям ЭВМ. Цифровая подпись не имеет ничего общего с последовательностью байт данных, соответствующей графической подписи или печати, поставленных на документ. В этом случае было бы очень легко выделять подписи из передаваемых документов и подсоединять их к ложным сообщениям. Невозможность подделки ЭЦП основывается не на отсутствии возможности подделать почерк или выделить нужное количество байт из сообщения, а на необходимости выполнения очень большого объема математических вычислений. Выполнить гигантский объем вычислений за приемлемые сроки, которые позволят использовать ЭЦП, практически *невозможно*. ЭЦП является неразрывной частью сообщения. Она зависит от текста сообщения, секретного и общедоступного ключа абонента, отправившего сообщение.

Обобщая, можно сказать, что ЭЦП обладает следующими свойствами:

- подпись практически невозможно подделать, она определяет лицо, подписавшее документ;

- подпись не тиражируется, она является функцией от конкретного сообщения и каждый раз вычисляется снова;
- подписанный документ неизменяем, при изменении документа легко доказать, что он подделан;
- от подписи нельзя отказаться, если отправитель попытается отказаться от посланного сообщения, то арбитр (третья сторона, имеющая сертификаты всех открытых ключей абонентов) легко докажет обратное.

Применение электронной цифровой подписи в автоматизированной системе банковских расчетов может приводить к конфликтным ситуациям, заключающимся в оспаривании сторонами (участниками системы банковских расчетов) авторства или содержимого документа, подписанного электронной цифровой подписью. Поэтому применение ЭЦП требует тщательной проработки договорных документов, в которых в обязательном порядке должна быть отражена процедура разбора конфликтных ситуаций.

Разбор подобных конфликтных ситуаций в соответствии с действующим законодательством и особенностями формирования самой электронной цифровой подписи требует применения специального программного обеспечения для выполнения проверок и документирования данных, используемых при выполнении процедуры проверки соответствия ЭЦП содержимому электронного документа.

Разбор конфликтной ситуации заключается в доказательстве авторства подписи конкретного электронного документа конкретным исполнителем.

Данный разбор основывается на математических свойствах алгоритма ЭЦП, реализованного в соответствии со стандартами Российской Федерации ГОСТ Р 34.10-49 и ГОСТ Р 34.11-94, гарантирующими практическую невозможность подделки значения ЭЦП любым лицом, не обладающим секретным ключом подписи [31, 32].

При проверке значения ЭЦП используется открытый ключ ЭЦП, значение которого вычисляется по значению секретного ключа ЭЦП.

Напомним некоторые положения действующих законов, которыми регламентируется применение ЭЦП.

1. Федеральный закон "Об информации, информатизации и защите информации" [10], гл.2, ст.5, п.3: "Юридическая сила

документа, хранимого, обрабатываемого и передаваемого с помощью автоматизированных информационных и телекоммуникационных систем, может подтверждаться электронной цифровой подписью. Юридическая сила электронной цифровой подписи признается при наличии в автоматизированной информационной системе программно-технических средств, обеспечивающих идентификацию подписи, и соблюдение установленного режима их использования".

2. Гражданский кодекс Российской Федерации [33]:

• Часть первая, ст.160, п.2: "Использование при совершении сделок факсимильного воспроизведения подписи с помощью средств механического или иного копирования, электронно-цифровой подписи либо иного аналога собственноручной подписи допускается в случаях и в порядке, предусмотренных законом, иными правовыми актами или соглашением сторон".

• Часть первая, ст.434, п.2: "Договор в письменной форме может быть заключен путем составления одного документа, подписанного сторонами, а также путем обмена документами посредством почтовой, телеграфной, телетайпной, телефонной, электронной или иной связи, позволяющей достоверно установить, что документ исходит от стороны по договору".

3. Официальные материалы Высшего Арбитражного Суда РФ:

• Письмо от 19 августа 1994 г. № С1-7/оп-578, где сказано: "В том случае, когда стороны изготовили и подписали договор с помощью электронно-вычислительной техники, в которой использована система цифровой (электронной) подписи, они могут представлять в арбитражный суд доказательства по спору, вытекающему из этого договора, также заверенные цифровой (электронной) подписью.

Если же между сторонами возник спор о наличии договора и других документов, подписанных цифровой (электронной) подписью, арбитражному суду следует запросить у сторон выписку из договора, в котором указана процедура порядка согласования разногласий, на какой стороне лежит бремя доказывания тех или иных фактов и достоверности подписи.

С учетом этой процедуры арбитражный суд проверяет достоверность представленных сторонами доказательств. При необходимости арбитражный суд вправе назначить экспертизу

по спорному вопросу, используя при этом предусмотренную договором процедуру.

В случае отсутствия в таком договоре процедуры согласования разногласий и порядка доказывания подлинности договора и других документов, а одна из сторон оспаривает наличие подписанного договора и других документов, арбитражный суд вправе не принимать в качестве доказательств документы, подписанные цифровой (электронной) подписью.

Арбитражному суду, разрешающему подобный спор, следует оценить заключенный таким образом договор, всесторонне рассмотреть вопрос и о том, добровольно ли и со знанием дела стороны включили в договор процедуру рассмотрения споров и доказывания тех или иных фактов, не была ли она навязана стороне другой стороной с целью обеспечения только своих интересов и ущемления интересов другой стороны, и с учетом этой оценки вынести решение по конкретному спору".

• Письмо от 7 июня 1995 г. № С1/03-316, в котором сказано: "Следует иметь в виду, что при соблюдении указанных условий, в том числе при подтверждении юридической силы документа электронной цифровой подписью, этот документ может признаваться в качестве доказательства по делу, рассматриваемому арбитражным судом".

При заключении договора, где будет закреплена процедура разбора конфликтных ситуаций необходимо учитывать следующие положения.

Стороны действуют на основе взаимного соглашения, опираясь на нормативные акты Российской Федерации (см. выше).

Стороны принимают в качестве электронных документов специальным образом оформленные блоки информации (файлы, записи баз данных и т.п.), подлинность и авторство которых удостоверяются цифровыми подписями уполномоченных лиц с помощью официально зарегистрированного открытого ключа отправителя.

Стороны согласны принимать на себя в полном объеме все обязательства, вытекающие из электронных документов, подписанных от их имени цифровыми подписями лиц, открытые ключи которых официально зарегистрированы в соответствии с установленным порядком, если при проверке эти цифровые подписи признаются достоверными и к моменту приема документа не было зафиксировано официального заявления подпи-

савшего лица о компрометации или выводе из действия своего индивидуального ключа подписи или программного обеспечения. Невыполнение любой из сторон этого условия является основанием для расторжения договора по инициативе другой стороны.

В случае если одна из сторон отказывается от принятия на себя обязательств по документу, заверенному ее действующей цифровой подписью, признаваемой подлинной программой проверки другой стороны, то:

• проверяется целостность программного обеспечения сторон, путем сравнения используемого программного обеспечения для проверки подписи с эталонным образцом (эталонный образец программного обеспечения для проверки цифровых подписей может по договоренности сторон храниться у одной или у каждой из них либо у третьей стороны, или предоставляться по запросу фирмой-изготовителем);

• повторно проверяется подлинность электронной подписи с помощью программного обеспечения, соответствующего эталону.

При выполнении всех перечисленных условий комиссия выносит заключение о подлинности цифровой подписи и ее соответствии содержимому документа, который тем самым признается действительным.

В случае если одна из сторон отказывается от приема и рассмотрения документа другой стороны на основании того, что цифровая подпись второй стороны под документом воспринимается программой проверки как фальшивая либо невозможно расшифровать данный документ, то:

• сторона, отказавшая в приеме документа, заверяет по требованию отправителя (возможны просьбы повторить передачу подписанного и зашифрованного документа, которые мотивированы плохим качеством связи, ошибкой оператора и т.д. С точки зрения надежности защиты информации они не являются опасными и могут быть выполнены). Свой официальный отказ от рассмотрения документа своей цифровой подписью и передает его отправителю, а вторая сторона повторно подписывает документ своей цифровой подписью либо повторно шифрует и передает документ;

• если новая цифровая подпись также признается первой стороной недействительной либо расшифровка повторно на-

правленного документа невозможна, то стороны проверяют сохранность своих программ подписывания и проверки, а также программ шифрования и генерации ключей путем сравнения их с эталонными образцами.

Если в результате проверки сохранности программного обеспечения выяснится, что:

• разрушено программное обеспечение у автора документа, то отказ другой стороны от рассмотрения документа является правомерным;

• разрушено программное обеспечение у стороны, отказавшейся от приема документа, тогда она обязана возместить убытки, возникшие у другой стороны вследствие ее отказа от рассмотрения документа; основанием для привлечения к ответственности служит официальный отказ от приема документа;

• не выявлено отличия программного обеспечения ни одной из сторон от эталонного образца, то признается несоответствие программного обеспечения техническому описанию используемых алгоритмов (ответственность ложится на фирму — изготовителя программ и алгоритмов).

Рассмотрим вышеизложенное применительно к СКЗИ "Янтарь АСБР", которое позволяет выполнять проверку значения ЭЦП в течение пяти лет с момента выполнения подписания документа, для чего средствами ведения базы данных (БД) участников системы сохраняются открытые ключи ЭЦП в течение указанного срока.

Разбор конфликтной ситуации выполняется комиссией, состоящей из представителей сторон, службы безопасности и экспертов. Состав комиссии, порядок ее формирования, регламент работы, рассмотрение результатов определяется в приложении к договору, заключаемому между участниками автоматизированной системы банковских расчетов.

Оспаривание результатов работы комиссии и возмещение пострадавшей стороне принесенного ущерба выполняется в установленном действующим законодательством Российской Федерации порядке.

Все отношения между участниками расчетов и ЦБ закрепляются в специальных договорах, где оговаривается ответственность сторон за правильное соблюдение правил работы в данной системе.

Разбор конфликтной ситуации заключается в доказательстве авторства подписи конкретного электронного документа конкретным исполнителем, и выполняется по инициативе любого участника АСБР и состоит из:

- предъявления претензии одной стороны другой;
- формирования комиссии;
- разбора конфликтной ситуации;
- взыскания с виновной стороны принесенного ущерба.

Разбор конфликтной ситуации заключается в выполнении "Эталонной программы проверки ЭЦП" (программа CHKSIGN) для электронного документа, авторство или содержание которого оспаривается. Описание программы CHKSIGN приведено в документе "Комплекс криптографических средств защиты информации ЯНТАРЬ. Эталонная программа проверки ЭЦП. Руководство оператора" ЯЦИТ.00004-01 34 01. "Протокол проверки ЭЦП", формируемый данной программой, является основным документом работы комиссии и должен быть подписан всеми членами комиссии. Содержащееся в протоколе проверки значение открытого ключа необходимо сравнить со значением открытого ключа из "Регистрационной карточки" участника АСБР. При совпадении их значений, авторство подписи под документом считается установленным. Формы "Протокола проверки ЭЦП" регистрационной карточки приведены в приложении 5.

При отсутствии в файлах БД открытого ключа участника, выполнившего ЭЦП, доказать ее авторство невозможно. В связи с этим, файлы БД необходимо подвергать регулярному резервному копированию.

"Эталонная программа проверки ЭЦП" (программа CHKSIGN) предназначена для проверки соответствия ЭЦП содержанию электронного документа и определения участника автоматизированной системы банковских расчетов (АСБР), выполнившего ее формирование.

"Эталонная программа проверки ЭЦП" CHKSIGN предназначена для работы на IBM PC AT-совместимой ПЭВМ под управлением операционной системы MS DOS версии 3.30 и выше.

В процессе работы программа CHKSIGN занимает не более 50 Кбайт оперативного запоминающего устройства (ОЗУ) и

выполняет обращения к файлам базы данных открытых ключей ЭЦП MEMDER.BD.

Файлы БД MEMDER.BD могут располагаться в различных поддиректориях, имеющих имя, соответствующее номеру года действия ключей. Например: 1995, 1996 и т.д.

Программа CHKSIGN запускается из командной строки DOS при помощи команды

CHKSIGN [<путь>] <имя_файла>,

где

<путь> — необязательный параметр командной строки, указывающий директорию, в поддиректориях которой расположены файлы БД открытых ключей MEMBER.BD. Если параметр <путь> не указан в командной строке, то программа CHKSIGN начинает поиск файлов БД открытых ключей, начиная с текущей директории;

<имя_файла> — имя файла, содержащего ЭЦП и исходные данные. Данный файл создается прикладным программным обеспечением АСБР посредством извлечения документа из архива документов. Формат данного файла должен соответствовать формату файла разбора конфликтных ситуаций, приведенному в документе "Комплекс криптографических средств защиты информации ЯНТАРЬ. Структуры ключевых элементов и баз данных".

В процессе работы программы CHKSIGN в текущей директории создается файл протокола проверки с именем REPORT.SGN, содержащий информацию о проверке истинности ЭЦП под документом.

"Протокол проверки электронной цифровой подписи" является основным документом при разборе конфликтных ситуаций, связанных с применением ЭЦП.

"Эталонная программа проверки ЭЦП" при своем запуске выполняет самоконтроль целостности. При обнаружении нарушения целостности программа выдает сообщение:

ЦЕЛОСТНОСТЬ ПРОГРАММЫ НАРУШЕНА
ИЛИ НЕКОРРЕКТНАЯ ЛИЦЕНЗИЯ !

При выдаче данного сообщения необходимо выполнить восстановление программы с дистрибутивного носителя.

ЗАКЛЮЧЕНИЕ

Изложенный материал представляет собой набор минимальных сведений, необходимых для начального ознакомления с практическим решением вопросов обеспечения информационной безопасности новейших автоматизированных систем банковских расчетов. Большой объем данной работы подчеркивает многогранность и сложность освоения безопасных информационных технологий, изучения эксплуатационной документации. Простой перенос существующих технологий обработки платежной информации в среду автоматизированных банковских систем не позволяет решить проблему обеспечения гибкого и безопасного управления финансовыми учреждениями и не учитывает тенденции развития финансово-экономической политики ЦБ РФ. Существующая структура учреждений ЦБ РФ постепенно будет подвергаться значительным структурным изменениям. Как указано в "Стратегии развития платежной системы России", утвержденной Советом Директоров ЦБ РФ 01.04.96, расчетная система страны должна ориентироваться на работу с единственным видом документов — электронным — и предусматривать возможность плавного перехода от используемых в настоящее время схем расчетов к централизованной схеме. Такой подход обеспечит единообразие потоков информации внутри расчетной системы и реализацию в случае необходимости дополнительных возможностей при проведении расчетов.

СПИСОК ЛИТЕРАТУРЫ

1. Банковская революция // Мир карточек. № 12. 1996.

2. Единая информационно-телекоммуникационная сеть Центробанка России / *М.Ю.Сенаторов, Ю.А.Тимофеев, С.Ф.Михайлов, В.И.Красовский, А.А.Карасев* // Сети. № 1. 1996.

3. Федеральный закон "О Центральном банке Российской Федерации (Банке России)".

4. *Лубенская Т.В., Мартынова В.В., Скородумов Б.И.* Безопасность информации в системах электронных платежей с пластиковыми карточками: Учебное пособие. М.: МИФИ, 1997. — 132 с.

5. Приказ ЦБ РФ №02-372 от 28.08.97.

6. Приказ ЦБ РФ №03-144 от 03.04.97.

7. Условия комплексного страхования банков международного страхового полиса Ллойда "Worldwide Bankers Policy" NMA 2626 (27/1/94).

8. Условия страхования от электронных и компьютерных преступлений страхового полиса Ллойда LSW 238 (7/91).

9. *Красовский В.И., Храмов А.В.* Аппаратно-программные средства телекоммуникационных сетей фирмы OST. М.: МИФИ, 1996. — 68 с.

10. Об информации, информатизации и защите информации. Федеральный закон. Принят Госдумой 25.01.95.

11. О внесении изменений и дополнений в Закон РСФСР "О банках и банковской деятельности в РСФСР". Федеральный закон. Принят Госдумой 07.07.95.

12. О внесении изменений и дополнений в Закон РСФСР "О Центральном банке РСФСР (Банке России)". Федеральный закон. Принят Госдумой 12.04.95.

13. Оценка экономической эффективности системы защиты от несанкционированного доступа СНЕГ 2.0 / *В.В. Левкин, В.А. Лыков, А.В. Шеин, Н.Г. Милославская, В.А. Петров* // Безопасность информационных технологий, № 3. 1996. С.90-101.

14. Секреты безопасности сетей / *Девид Стенг, Сильвия Мун* // ICE. Киев, 1996.

15. Криминальные расчеты: уголовно-правовая охрана инвестиций: Научно-практическое пособие. М.: Учебно-консультационный центр "ЮрИнфоР", 1995. — 128 с.

16. *Вехов В.Б.* Компьютерные преступления: способы совершения и раскрытия / *Под ред. акад. Б.П. Смагоринского.* М.: Право и Закон, 1996. — 182 с.

17. Информационное агентство ФРГ по обеспечению надежности систем. 1994.

18. Security Architecture for open Systems Interconnection. Recommendation X800, ICCTT, 1991.

19. ISO/IEC 7498-2:1989 Information Processing Systems. Open Systems Interconnection (OSI) Reference Model. Part 2: Security architecture.

20. ISO EDIFACT. Security implementation guideline (SIG).

21. ГОСТ Р 50739-95. ГОСУДАРСТВЕННЫЙ СТАНДАРТ РОССИЙСКОЙ ФЕДЕРАЦИИ. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Общие технические требования.

22. Концепция защиты средств вычислительной техники и автоматизированных систем то несанкционированного доступа к информации. Руководящий документ Гостехкомиссии России. М.: ГОСТЕХКОМИССИЯ РФ, 1992. — 13 с.

23. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищенности СВТ от НСД к информации. Руководящий документ Гостехкомиссии России. М.: ГОСТЕХКОМИССИЯ РФ, 1992. — 25 с.

24. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации. Руководящий документ Гостехкомиссии России. М.: ГОСТЕХКОМИССИЯ РФ, 1992. — 39 с.

25. Временное положение по организации разработки, изготовления и эксплуатации программных и технических средств защиты информации от НСД в автоматизированных системах и средствах вычислительной техники. Руководящий документ Гостехкомиссии России. М.: ГОСТЕХКОМИССИЯ РФ, 1992. — 29 с.

26. Требования к заявителю на право установки (инсталляции), эксплуатации сертифицированных ФАПСИ шифро-

вальных средств и предоставления услуг по шифрованию информации при защите информации по уровню "С". 1996.

27. *Скородумов Б.И.* Информационная безопасность. Обеспечение безопасности информации электронных банков: Учебное пособие. М.: МИФИ, 1995. — 104 с.

28. Информационная безопасность. Новые средства криптографической защиты информации: Учебное пособие / *Е.В. Давыдова, И.Л. Дмитриев, И.А. Курепкин, В.Л. Кущ, А.Г. Мухин, Б.И. Скородумов, Д.А. Старовойтов, А.Е. Шарков.* М.: МИФИ, 1996.

29. *Скородумов Б.И.* Программно-аппаратные комплексы защиты от несанкционированного доступа к информации: Учебное пособие. М: МИФИ, 1996. — 108 с.

30. ГОСТ 28147-89. Системы обработки информации. Защита криптографическая. Алгоритм криптографического преобразования.

31. ГОСТ Р 34.10-94. Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной подписи на базе асимметричного криптографического алгоритма.

32. ГОСТ Р 34.11-94. Информационная технология. Криптографическая защита информации. Функция хэширования.

33. Гражданский кодекс Российской Федерации.

34. Положение о государственном лицензировании деятельности в области защиты информации от 24 июня 1997 г. № 60.

35. *Аминов Д.И., Ревин В.П.* Преступность в кредитно-банковской сфере в вопросах и ответах. М.: Брандес, 1997. — 120 с.

36. *Варфоломеев А.А., Пеленицын М.Б.* Методы криптографии и их применение в банковских технологиях. М.: МИФИ, 1995.

37. *Рудакова О.С.* Банковские электронные услуги: Учебное пособие для вузов. М.: Банки и биржи, ЮНИТИ, 1997. — 261 с.

38. *Захарушкин В.Ф.* Построение автоматизированных клиринговых систем // Сети. № 1, 1996.

39. *Варфоломеев А.А., Домнина О.С., Пеленицын М.Б.* Управление ключами в системах криптографической защиты банковской информации. М.: МИФИ, 1995.

40. *Фомичев В.М.* Симметричные криптосистемы. М.: МИФИ, 1995.

ПЕРЕЧЕНЬ ИСПОЛЬЗОВАННЫХ ТЕРМИНОВ И ИХ ОПРЕДЕЛЕНИЙ

Абонент (клиент) — объект или субъект, зарегистрированный в системе обработки информации (сети, базе данных) пользующийся ее ресурсами и услугами.

Абонентская система — система, выполняющая функции, связанные с предоставлением либо с потреблением информационных ресурсов, а также взаимодействие с другими системами.

Архитектура — общее описание модели (системы, сети и т.п.), определяющее основные ее элементы, характер и топологию их взаимодействия.

Автоматизированная банковская система (АБС) — совокупность взаимодействующих средств автоматизации банковской деятельности (внутри и вне банка), которая реализуется посредством вычислительной и телекоммуникационной техники.

Авторизация — предоставление доступа пользователю, программе или процессу.

Администратор информационной безопасности — лицо, ответственное за защиту автоматизированной системы от несанкционированного доступа к информации.

Активная угроза безопасности — угроза намеренного несанкционированного изменения состояния системы.

Аутентификация — установление (проверка) подлинности сообщения, источника данных и приемника данных.

Банковский идентификационный код (БИК) —девятизначное число, присвоенное банку, которое указано в "Справочнике банковских идентификационных кодов участников расчетов на территории Российской Федерации", позволяющее идентифицировать банк в системе банковских взаиморасчетов.

База данных — совокупность определенным образом организованных и предназначенных для обработки на ЭВМ данных, существенная для некоторой деятельности человека.

Виртуальный канал — канал в сети с пакетной коммутацией, создаваемый для передачи пакета (пакетов) данных между двумя абонентами.

Виртуальное соединение — совокупность процедур по созданию виртуального канала в сети с пакетной коммутацией.

Документированная информация (документ) — зафиксированная на материальном носителе информация с реквизитами, позволяющими ее идентифицировать.

Доступ к информации — ознакомление с информацией, ее обработка, в частности копирование, модификация или уничтожение информации.

Доступность информации — свойство или качество, характеризующееся способностью своевременного беспрепятственного доступа к информации субъектов, имеющих на это надлежащие полномочия.

Заверение (нотаризация) — регистрация данных у доверенного третьего лица для повышения уверенности в правильности таких характеристик, как содержание, источник данных, время доставки.

Зашифрование (информации) — процесс преобразования открытых данных в зашифрованные с помощью шифра.

Защита от несанкционированного доступа — предотвращение или существенное затруднение несанкционированного доступа.

Идентификатор доступа — уникальный признак субъекта или объекта доступа.

Идентификационные данные — уникальные данные субъекта или объекта системы, по которым можно однозначно его идентифицировать.

Идентификация — присвоение субъектам и объектам доступа идентификатора и (или) сравнение предъявляемого идентификатора с утвержденным.

Имитовставка — информация фиксированной длины, полученная по определенному правилу из открытых данных и ключа и добавленная к зашифрованным данным для обеспечения имитозащиты.

Имитозащита — защита системы шифрованной связи от навязывания ложных данных.

Информационная система — организационно упорядоченная совокупность документов (массивов документов) и информационных технологий, в том числе с использованием средств вычислительной техники и связи, реализующих информационные процессы.

Канал связи — совокупность технических средств каналообразования, а также линий и сооружений связи, обеспечивающих соединение и связь абонентов требуемой пропускной способности.

Канальное шифрование — применение процедур шифрования данных в каждом канале передачи данных коммуникационной системы.

Контроль доступа (управление доступом) — процесс ограничения доступа к ресурсам системы только разрешенным субъектам или объектам.

Клиринг — система безналичных взаиморасчетов за товары, услуги и ценные бумаги, основанная на взаимозачете сторонами требований и обязательств.

Клиринговые сети — сетевые автоматизированные платежные системы межбанковских расчетов.

Контроль эффективности защиты информации — проверка соответствия эффективности мероприятий по защите информации установленным требованиям или нормам эффективности защиты.

Конфиденциальность (секретность) информации — субъективно определяемая (приписываемая) информации характеристика (свойство), указывающая на необходимость введения ограничений на круг субъектов, имеющих доступ к данной информации, и обеспечиваемая способностью системы (среды) сохранять указанную информацию в тайне от субъектов, не имеющих полномочий на право доступа к ней.

Конфиденциальная информация — информация, доступ к которой ограничивается в соответствии с законодательством РФ.

Криптографическая защита — защита данных при помощи криптографического преобразования данных.

Криптографический ключ — конкретное секретное состояние некоторых параметров алгоритма криптографического преобразования данных, обеспечивающее выбор одного преобразования из совокупности всевозможных для данного алгоритма преобразований.

Криптографическое преобразование — преобразование данных при помощи шифрования и (или) выработки имитовставки.

Лицензия в области защиты информации — оформленное соответствующим образом разрешение на право проведения тех или иных работ в области защиты информации.

Многоуровневая защита — защита, обеспечивающая разграничение доступа субъектов с различными правами доступа к объектам различных уровней.

Модель нарушителя правил разграничения доступа (модель нарушителя ПРД) — абстрактное (формализованное или неформализованное) описание нарушителя правил разграничения доступа.

Несанкционированный доступ к информации (НСД) — доступ к информации с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами, нарушающий правила разграничения доступа.

Объект доступа — единица информационного ресурса автоматизированной системы, доступ к которой регламентируется правилами разграничения доступа.

Оконечное (абонентское) шифрование — шифрование данных в реальной оконечной системе (источнике данных) и соответствующее расшифрование, которое производится в реальной оконечной системе (приемнике данных).

Открытый ключ — общедоступная часть информации о криптографическом ключе.

Пакетная коммутация — современный способ распределения информационного потока в сложной территориальной информационной системе, характеризующийся обменом "пакетами" информации в соответствии с рекомендациям МККТТ(X.25).

Пакет данных — блок информации, без разборки на части, передаваемый через сеть передачи данных или ЛВС.

Пароль — информация ограниченного доступа для идентификации, обычно представляющая собой строку знаков, которой должен обладать пользователь для доступа к защищенным данным.

Пассивная угроза безопасности — угроза несанкционированного доступа к информации без изменения состояния системы.

Политика безопасности — набор правил, определяющих процедуры и механизмы обеспечения безопасности заданного подмножества объектов и субъектов безопасности.

Пользователь (потребитель) информации — субъект, обращающийся к информационной системе или посреднику за получением необходимой ему информации и пользующийся ею.

Правила разграничения доступа (ПРД) — совокупность правил, регламентирующих права доступа субъектов доступа к объектам доступа.

Протокол — общеизвестная, заранее согласованная процедура действий, состоящая из последовательности вычислений и передачи данных между сторонами, обеспечивающая работоспособность и требуемые свойства системы.

***Р**асшифрование данных* — процесс преобразования зашифрованных данных в открытые при помощи шифра.

***С**анкционированный доступ к информации* — доступ к информации, не нарушающий правила разграничения доступа.

Секретный ключ — часть информации о криптографическом ключе, сохраняемая в секрете.

Сертификат защиты (сертификат) — документ, удостоверяющий соответствие средства вычислительной техники или автоматизированной системы набору определенных требований по защите от несанкционированного доступа к информации и дающий право разработчику на использование и (или) распространение их как защищенных.

Система защиты информации от несанкционированного доступа (СЗИ НСД) — комплекс организационных мер, программных и технических (в том числе криптографических) средств защиты от несанкционированного доступа к информации в автоматизированных системах.

Средство защиты от несанкционированного доступа к информации — программное, техническое или программно-техническое средство, предназначенное для предотвращения или существенного затруднения несанкционированного доступа к информации.

Средство криптографической защиты информации (СКЗИ) — средство вычислительной техники, осуществляющее

криптографическое преобразование информации для обеспечения ее безопасности.

СУБД — система управления базой данных.

***У**гроза безопасности* — потенциально возможное нарушение безопасности.

Управление ключами — построение ключей, их хранение, распространение, удаление, учет и применение в соответствии с политикой безопасности.

***Ц**елостность информации* — свойство информации, заключающееся в ее существовании в неискаженном виде (неизменном по отношению к некоторому фиксированному ее состоянию).

Цифровая подпись — данные, добавляемые к блоку данных или полученные в результате его криптографического преобразования, которые позволяют приемнику данных удостовериться в целостности блока данных и подлинности источника данных, а также обеспечить защиту от подлога со стороны приемника данных.

***Ш**ифр* — совокупность обратимых преобразований множества возможных открытых данных на множество возможных зашифрованных данных, осуществляемых по определенным правилам с применением ключей.

Шифрование — процесс зашифрования или расшифрования.

Электронный журнал — файл, содержащий информацию по всем операциям, проведенным данным электронным устройством.

ТРЕБОВАНИЯ К ЗАЯВИТЕЛЮ НА ПРАВО УСТАНОВКИ (ИНСТАЛЛЯЦИИ), ЭКСПЛУАТАЦИИ СЕРТИФИЦИРОВАННЫХ ФАПСИ ШИФРОВАЛЬНЫХ СРЕДСТВ И ПРЕДОСТАВЛЕНИЯ УСЛУГ ПО ШИФРОВАНИЮ ИНФОРМАЦИИ ПРИ ЗАЩИТЕ ИНФОРМАЦИИ ПО УРОВНЮ "С"*

Настоящие требования предъявляются к юридическим лицам — предприятиям, учреждениям и организациям (далее — предприятия), независимо от их организационно-правовой формы, подавшим заявление на получение лицензии на право установки (инсталляции), эксплуатации сертифицированных ФАПСИ шифровальных средств (средств криптографической защиты информации — СКЗИ) и предоставления услуг по шифрованию информации.

Настоящие требования распространяются на СКЗИ, предназначенные для защиты информации, не содержащей сведений, составляющих государственную тайну, при обеспечении безопасности информации по уровню "С".

"С"-криптографическая защита на уровне потребителя. Информационно-телекоммуникационные системы создаются предприятием самостоятельно на основе сертифицированных СКЗИ, встраивание которых в прикладные системы должно происходить с выполнением интерфейсных и криптографических протоколов, определенных технической документацией на СКЗИ.

I. Требования по организационному обеспечению безопасности СКЗИ

1. На предприятии-заявителе руководством должны быть выделены должностные лица, ответственные за разработку и практическое осуществление мероприятий по обеспечению функционирования и безопасности СКЗИ.

---

* Козюра Д. Право на шифрование // Мир связи. CONNECT!. № 9. 1997. С.60-63.

2. Вопросы обеспечения функционирования и безопасности СКЗИ должны быть отражены в специально разработанных документах, утвержденных руководством предприятия, с учетом эксплуатационной документации на СКЗИ.

3. На предприятии должны быть созданы условия, обеспечивающие сохранность конфиденциальной информации, доверенной предприятию юридическими и физическими лицами, пользующимися его услугами.

II. Требования по размещению, специальному оборудованию, охране и режиму в помещениях, в которых размещены СКЗИ

4. Размещение, специальное оборудование, охрана и режим в помещениях, в которых размещены СКЗИ (далее помещения), должны обеспечивать безопасность информации, СКЗИ и шифрключей, сведение к минимуму возможности неконтролируемого доступа к СКЗИ, просмотра процедур работы с СКЗИ посторонними лицами.

5. Порядок допуска в помещения определяется внутренней инструкцией, которая разрабатывается с учетом специфики и условий функционирования конкретной структуры предприятия.

6. При расположении помещений на первых и последних этажах зданий, а также при наличии рядом с окнами балконов, пожарных лестниц и т.п., окна помещений оборудуются металлическими решетками, ставнями, охранной сигнализацией или другими средствами, препятствующими несанкционированному доступу в помещения. Эти помещения должны иметь прочные входные двери, на которые устанавливаются надежные замки.

7. Для хранения шифрключей, нормативной и эксплуатационной документации, инсталляционных дискет помещения обеспечиваются металлическими шкафами (хранилищами, сейфами), оборудованными внутренними замками с двумя экземплярами ключей. Дубликаты ключей от хранилищ и входных дверей должны храниться в сейфе ответственного лица, назначаемого руководством предприятия.

8. Устанавливаемый руководителем предприятия порядок охраны помещений должен предусматривать периодический

контроль технического состояния средств охранной и пожарной сигнализации и соблюдения режима охраны.

9. Размещение и установка СКЗИ осуществляется в соответствии с требованиями документации на СКЗИ.

10. Системные блоки ЭВМ с СКЗИ должны быть оборудованы средствами контроля их вскрытия.

III. Требования по обеспечению безопасности шифрключей

11. Все поступающие для использования шифрключи и инсталляционные дискеты должны браться на предприятии на поэкземплярный учет в выделенных для этих целей журналах.

12. Учет и хранение носителей шифрключей и инсталляционных дискет, непосредственная работа с ними поручается руководством предприятия специально выделенным работникам предприятия. Эти работники несут персональную ответственность за сохранность шифрключей.

13. Учет изготовленных для пользователей шифрключей, регистрация их выдачи для работы, возврата от пользователей и уничтожения ведется на предприятии.

14. Хранение шифрключей, инсталляционных дискет допускается в одном хранилище с другими документами при условиях, исключающих их непреднамеренное уничтожение или иное, не предусмотренное правилами пользования СКЗИ, применение.

Наряду с этим должна быть предусмотрена возможность раздельного безопасного хранения рабочих и резервных шифрключей, предназначенных для использования в случае компрометации рабочих шифрключей в соответствии с правилами пользования СКЗИ.

15. При пересылке шифрключей клиентам предприятия должны быть обеспечены условия транспортировки, исключающие возможность физических повреждений и внешнего воздействия на записанную ключевую информацию.

16. В случае отсутствия у оператора СКЗИ индивидуального хранилища шифрключи по окончании рабочего дня должны сдаваться лицу, ответственному за их хранение.

17. Уполномоченными лицами периодически должен проводиться контроль сохранности входящего в состав СКЗИ оборудования, а также всего используемого программного обеспече-

ния для предотвращения внесения программно-аппаратных закладок и программ вирусов.

IV. Требования к сотрудникам, осуществляющим эксплуатацию и установку (инсталляцию) СКЗИ

18. К работе с СКЗИ допускаются решением руководства предприятия только сотрудники, знающие правила его эксплуатации, владеющие практическими навыками работы на ПЭВМ, изучившие правила пользования, эксплуатационную документацию и прошедшие обучение работе с СКЗИ.

19. Руководитель предприятия или лицо, уполномоченное на руководство заявленными видами деятельности, должно иметь представление о возможных угрозах информации при ее обработке, передаче, хранении, методах и средствах защиты информации.

ТРЕБОВАНИЯ К ОРГАНИЗАЦИИ ПАРОЛЬНОЙ ЗАЩИТЫ АВТОМАТИЗИРОВАННОЙ СИСТЕМЫ УЧАСТНИКА ЭЛЕКТРОННЫХ ПЛАТЕЖЕЙ*

1. Участником электронных платежей должна быть организована централизованная служба (группа в составе подразделения безопасности и защиты информации) парольной защиты. Задачей данной службы является организационно-техническое обеспечение процессов генерации, смены и удаления паролей во всех автоматизированных системах и ЭВМ участника электронных платежей, разработка всех необходимых инструкций и контроль за действиями персонала по работе с паролями.

2. Личные пароли должны выбираться пользователями автоматизированной системы самостоятельно, но с учетом следующих требований:

- длина пароля должна быть не менее 8 символов;
- в числе символов пароля обязательно должны присутствовать буквы в верхнем и нижнем регистрах, цифры и специальные символы (@, #, $, &, *, % и т.п.);
- пароль не должен включать в себя легко вычисляемые сочетания символов (имена, фамилии, наименования АРМ и т.д.), а также общепринятые сокращения (ЭВМ, ЛВС, USER, SYSOP и т.д.);
- при смене пароля новое значение должно отличаться от предыдущего не менее чем в 6 позициях;
- личный пароль пользователь не имеет права сообщать никому.

Владельцы паролей должны быть ознакомлены под расписку с перечисленными выше требованиями и предупреждены об ответственности за использование паролей, не соответствующих данным требованиям, а также за разглашение парольной информации.

3. В случае, если формирование личных паролей пользователей осуществляется централизованной службой парольной

* Выдержка из приказа ЦБ РФ № 02-144 от 3.04.97.

защиты, ответственность за правильность их формирования и распределение возлагается на указанную службу.

4. Резервная копия пароля каждого сотрудника в отдельном опечатанном конверте должна храниться в сейфе руководителя подразделения. Для опечатывания конвертов с паролями должны применяться либо личные печати владельцев (при наличии), либо печать уполномоченного представителя Управления (отдела) безопасности и защиты информации территориального учреждения Банка России.

5. Полная плановая смена паролей должна проводиться регулярно, не реже одного раза в месяц.

6. Внеплановая смена (удаление) личного пароля любого пользователя автоматизированной системы в случае прекращения его полномочий (увольнение либо переход на другую работу внутри участника электронных платежей) должна производиться немедленно после окончания последнего сеанса работы данного пользователя с системой.

7. Внеплановая полная смена паролей должна производиться в случае прекращения полномочий (увольнение, переход на другую работу внутри участника электронных платежей и другие обстоятельства) администраторов информационной безопасности и других сотрудников, которым по роду работы были предоставлены либо полномочия по управлению автоматизированной системой в целом, либо полномочия по управлению подсистемой защиты информации данной автоматизированной системы, а значит, кроме личного пароля, им могут быть известны пароли других пользователей системы.

8. В случае компрометации личного пароля хотя бы одного пользователя автоматизированной системы должны быть немедленно предприняты меры в соответствии с п.6 или 7 настоящих Требований в зависимости от полномочий владельца скомпрометированного пароля.

ИНСТРУКЦИЯ ПО УСТАНОВКЕ АРМ КБ(РКЦ) СКЗИ "ЯНТАРЬ АСБР"

1. Проверить ПЭВМ на отсутствие компьютерных вирусов.
2. Установить плату комплекса "Аккорд".
3. Инсталлировать ПО "ACCESS" с дискеты комплекса "Аккорд".
4. В случае необходимости (по сообщению в процессе инсталляции "ACCESS"), запустить утилиту MS DOS **defrag.exe** с опцией дефрагментации файлов.
5. Из каталога ACCESS запустить драйвер **tmdrv.com P:340**.
6. Запустить программу **memscan** и проверить, нет ли конфликта по объему занимаемой памяти.
7. Запустить программу **access.exe**.

7.1. Пользователю с именем SUPERVISOR назначаются следующие атрибуты:

- стартовый каталог — C:\ ;
- выполняемая программа — C:\command.com;
- режим запроса проверки целостности — до запуска, с запросом.

7.2. Пользователям с именами USER1, USER2, ... (в соответствии с количеством приобретенных идентификаторов типа Touch Memory) назначаются следующие атрибуты:

- стартовый каталог — C:\ ;
- выполняемая программа — C:\INGN\monitor.exe;
- режим запроса проверки целостности — до запуска (без запроса).

7.3. Всем пользователям назначаются на контроль целостности следующие файлы:

- с расширениями *.exe; *.com; *.ovl; *.bat; *.sys из каталогов C:\ACCESS; C:\; C:\INGN; C:\JANTAR\KB,

причем

- в каталоге C:\ обязателен контроль файлов autoexec.bat, config.sys (после их модификации в п.8), command.com, Io.sys и Ms.dos, или аналогов.

Остальные файлы каталога контролируются или нет с учетом конкретных обстоятельств;

- в каталоге C:\JANTAR\KB контролируются еще и файлы uz.bd3; adm.lst; member.bd и файлы, имена которых состоят из четырех цифр.

8. Модифицировать файлы
CONFIG.SYS и AUTOEXEC.BAT:

⇒ в файл **config.sys** включить строки:

SWITCHES=/F/N/K
DEVICE=KEYBOFF.SYS

⇒ в файле **autoexec.bat**:

включить строку загрузки драйвера TMDRV

tmdrv.com P:340

последнюю строку сделать в виде

access.exe /E

Приложение 5

ФОРМА ПРОТОКОЛА ПРОВЕРКИ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ

Форма 4А (PR)	"ЯНТАРЬ АСБР"
Протокол проверки ЭЦП	
Дата проверки: 00-00-0000	
Криптографические константы:	
P:	XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX
	XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX
	XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX
	XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX
Q:	XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX
	XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX
A:	XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX
	XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX
	XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX
	XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX
Данные:	XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX
	XX XX XX XX XX XX XX XX XX XX
Подпись:	XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX
	XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX
	XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX
	XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX
Открытый ключ:	
	XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX
	XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX
	XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX
	XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX XX
Дата регистрации: 00-00-0000 Дата архивации: 00-00-0000 Код банка: XXXXXXXXX Код участника: XXXXXXXXXXXX Категория: ..... Ф.И.О: ..... Организация: ..... Уникальный идентификатор: XX XX XX XX	
Результат проверки ЭЦП:	
Члены комиссии:	
Ф.И.О _____	"____"_____ 199 г.
Ф.И.О _____	"____"_____ 199 г.
Ф.И.О _____	"____"_____ 199 г.

РЕГИСТРАЦИОННЫЕ ЖУРНАЛЫ

В РЦУК ведется журнал регистрации ключей (ЖРК), в котором фиксируется получение комплекта ключевых упаковок и выдача их абонентам.

Администратор РЦУК ежедневно ведет журнал сети, где отражаются все штатные и нештатные ситуации, происходящие в сети.

Каждый абонент сети ведет журнал АРМ, в котором фиксируются все штатные и нештатные ситуации, происходящие на рабочих местах, а также информация, получаемая от РЦУК.

Форма ЖРК

п/п	Серия и номер ключевой упаковки	Абонент	Дата	Расписка в получении ключевой упаковки	Расписка в получении сертификата ЭЦП	Дата	Примечание

Форма журнала сети

Дата, время	Абонент	Событие	Причина	Изменение в работе сети (решение)	Примечание

Форма журнала АРМ

Дата, время	Событие	Причина	Изменение в работе АРМ	Примечание

Михаил Юрьевич Романов
Борис Иванович Скородумов

БЕЗОПАСНОСТЬ ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ БАНКОВСКИХ РАСЧЕТОВ

Редактор *Т.В.Волвенкова*
Оригинал-макет изготовлен *М.В.Макаровой*
с использованием программы Microsoft Word 6.0

ЛР № 020676 от 09.12.97. Подписано в печать 25.02.98.
Формат 60x84 1/16. Уч.-изд.л. 9,75. Печ.л. 9,75. Тираж 500 экз.
Изд. № 004-3. Заказ № 168

Московский государственный инженерно-физический институт (технический университет)

Типография МИФИ

115409, Москва, Каширское ш., 31

40р 00к