

Технологии обработки финансовой информации

Лекции

ТЕМА 1. ВВЕДЕНИЕ В ПРЕДМЕТ. ОСНОВНЫЕ ПОНЯТИЯ, ТЕРМИНЫ И ОПРЕДЕЛЕНИЯ.

1.1. Введение

На данной лекции мы рассмотрим такие понятия как финансово-кредитная система, банковская система РБ, денежно-кредитная политика, рассмотрим основные функции Национального и коммерческих банков.

При формулировке понятий и определений главным образом будем опираться на Банковский кодекс Республики Беларусь.

Финансово-кредитная система является ключевым элементом, обеспечивающим движение капитала между субъектами финансово-экономической системы Республики Беларусь. Она включает в себя бюджетную систему, банковскую систему, а также финансовые средства внебюджетных фондов, предприятий, учреждений, организаций и граждан. На территории Республики Беларусь проводится единая бюджетно-финансовая, налоговая, денежно-кредитная, валютная политика.

Бюджетная система Республики Беларусь имеет два уровня: республиканский и местные бюджеты.

Доходы бюджета формируются за счет налогов, определяемых законом, других обязательных платежей, а также иных поступлений.

Банковская система Республики Беларусь является составной частью финансово-кредитной системы Республики Беларусь. Она является двухуровневой:

- 1-й уровень - Национальный банк;
- 2-й уровень - коммерческие банки.

Субъектами банковских правоотношений являются Национальный банк, банки и небанковские кредитно-финансовые организации.

Участниками банковских правоотношений могут быть государственные органы, органы местного управления и самоуправления, физические и юридические лица.

Объектами банковских правоотношений являются деньги (валюта), ценные бумаги и валютные ценности.

Денежно-кредитная политика Республики Беларусь - составная часть единой государственной экономической политики.

Правовой основой денежно-кредитной политики Республики Беларусь являются Основные направления денежно-кредитной политики Республики Беларусь, ежегодно утверждаемые Президентом Республики Беларусь по представлению Национального банка и Правительства Республики Беларусь.

Основные направления денежно-кредитной политики Республики Беларусь содержат важнейшие параметры развития денежно-кредитной сферы, определяют цели, задачи и приоритеты денежно-кредитной политики государства и предусматривают комплекс обеспечивающих достижение этих целей мероприятий, механизмов регулирования и контроля.

1.2. Банковская система

1.2.1 Национальный банк

Национальный банк — центральный банк Республики Беларусь, действующий исключительно в интересах Республики Беларусь. Он осуществляет свою деятельность в соответствии с Конституцией Республики Беларусь, Банковским Кодексом, законами Республики Беларусь, нормативными правовыми актами Президента Республики Беларусь, Уставом Национального банка и независим в своей деятельности. Национальный банк подотчетен Президенту Республики Беларусь и является юридическим лицом.

Основные цели деятельности Национального банка:

- защита и обеспечение устойчивости белорусского рубля, в том числе его покупательной способности и курса по отношению к иностранным валютам;
- развитие и укрепление банковской системы Республики Беларусь;
- обеспечение эффективного, надежного и безопасного функционирования платежной системы.

Получение прибыли не является основной целью деятельности Национального банка.

Национальный банк РБ выполняет следующие функции:

- разрабатывает и совместно с Правительством Республики Беларусь проводит единую денежно-кредитную политику РБ в порядке, установленном Конституцией Республики Беларусь, настоящим Кодексом и иными законодательными актами Республики Беларусь;
- осуществляет эмиссию денег;
- регулирует денежное обращение;
- регулирует кредитные отношения;
- является для банков кредитором последней инстанции, осуществляет их рефинансирование;

- осуществляет валютное регулирование;
- организует и осуществляет валютный контроль как непосредственно, так и через уполномоченные банки в соответствии законодательством Республики Беларусь;
- выполняет функции центрального депозитария государственных ценных бумаг и ценных бумаг Национального банка, если иное не определено Президентом Республики Беларусь;
- осуществляет эмиссию ценных бумаг Национального банка;
- организует эффективное, надежное и безопасное функционирование системы межбанковских расчетов;
- консультирует, кредитует и выполняет функции финансового агента Правительства Республики Беларусь и местных исполнительных и распорядительных органов по вопросам исполнения республиканского и местных бюджетов;
- осуществляет государственную регистрацию банков и небанковских кредитно-финансовых организаций, производит выдачу им лицензий на осуществление банковских операций;
- осуществляет регулирование деятельности банков и небанковских кредитно-финансовых организаций по ее безопасному и ликвидному осуществлению и надзор за этой деятельностью;
- устанавливает порядок осуществления банковских операций;
- регистрирует ценные бумаги банков и небанковских кредитно-финансовых организаций в соответствии с законодательством Республики Беларусь;
- разрабатывает и утверждает методику бухгалтерского учета и отчетности для банков и небанковских кредитно-финансовых организаций;
- определяет порядок проведения безналичных и наличных расчетов в Республике Беларусь;
- осуществляет операции, необходимые для выполнения основных целей деятельности Национального банка;
- организует расчетное и (или) кассовое обслуживание отдельных государственных органов, перечень которых определен в Уставе Национального банка;
- принимает участие в разработке прогноза платежного баланса Республики Беларусь и организует составление платежного баланса Республики Беларусь;
- создает золотовалютные резервы, в том числе золотой запас, и управляет ими;
- устанавливает цены купли-продажи драгоценных металлов и драгоценных камней при осуществлении банковских операций;
- организует инкассацию и перевозку денежной наличности, валютных и других ценностей;
- осуществляет контроль за обеспечением безопасности и защиты информации в банковской системе;
- заключает соглашения с центральными (национальными) банками и кредитными организациями иностранных государств;

- дает согласие на осуществление банками и небанковскими кредитно-финансовыми организациями операций с ценными бумагами;
- выполняет другие функции в соответствии с настоящим Кодексом и иными законодательными актами Республики Беларусь.

Национальный банк определяет основные направления развития платежной системы Республики Беларусь.

Национальный банк устанавливает правила, формы, сроки и стандарты при проведении безналичных и наличных расчетов в Республике Беларусь и ответственность за их нарушение.

Национальный банк ведет ведомственный архив данных и документов по межбанковским расчетам. Национальный банк вправе использовать этот архив для статистической и иной обработки, а также для обеспечения свидетельства о деятельности и операциях, осуществляемых при проведении межбанковских расчетов.

1.2.2 Коммерческие банки

Банк - юридическое лицо, имеющее исключительное право осуществлять в совокупности следующие банковские операции:

- привлечение денежных средств физических и (или) юридических лиц во вклады (депозиты);
- размещение привлеченных денежных средств от своего имени и за свой счет на условиях возвратности, платности и срочности;
- открытие и ведение банковских счетов физических и юридических лиц.

Национальный банк выдает следующие виды лицензий на осуществление банковских операций:

- общую - на осуществление указанных в ней банковских операций в белорусских рублях;
- на привлечение во вклады средств физических лиц;
- внутреннюю - на осуществление указанных в ней банковских операций в иностранной валюте на территории Республики Беларусь;
- генеральную - на осуществление указанных в ней банковских операций в иностранной валюте как на территории Республики Беларусь, так и за ее пределами. Под банковскими операциями, осуществляемыми в рамках генеральной лицензии за пределами Республики Беларусь, понимаются банковские операции в иностранной валюте, проводимые банком с банками (кредитно-финансовыми организациями) - нерезидентами;
- разовую - на осуществление отдельной банковской операции в иностранной валюте;
- на осуществление операций с драгоценными металлами и драгоценными камнями.

Банковские операции

Банковские операции могут быть *активными*, *пассивными* или *посредническими*.

Под активными банковскими операциями понимаются операции, направленные на предоставление денежных средств банками и небанковскими кредитно-финансовыми организациями.

Под пассивными банковскими операциями понимаются операции, направленные на привлечение денежных средств банками и небанковскими кредитно-финансовыми организациями.

Под посредническими банковскими операциями понимаются операции, содействующие осуществлению банковской деятельности банками и небанковскими кредитно-финансовыми организациями.

К банковским операциям относятся:

- привлечение денежных средств физических и (или) юридических лиц во вклады (депозиты);
- размещение привлеченных денежных средств от своего имени и за свой счет на условиях возвратности, платности и срочности;
- открытие и ведение банковских счетов физических и юридических лиц;
- открытие и ведение счетов в драгоценных металлах;
- осуществление расчетного и (или) кассового обслуживания физических и юридических лиц, в том числе банков-корреспондентов;
- валютно-обменные операции;
- купля-продажа драгоценных металлов и драгоценных камней в случаях, установленных законодательством Республики Беларусь;
- привлечение и размещение драгоценных металлов и драгоценных камней во вклады (депозиты);
- выдача банковских гарантий;
- доверительное управление денежными средствами, драгоценными металлами и драгоценными камнями;
- инкассация денежной наличности, валютных и других ценностей, а также платежных документов (платежных инструкций);
- хранение драгоценных металлов и драгоценных камней;
- выпуск в обращение банковских пластиковых карточек;
- финансирование под уступку денежного требования (факторинг);
- предоставление физическим и юридическим лицам специальных помещений или находящихся в них сейфов для хранения документов и ценностей (денежных средств, ценных бумаг, драгоценных металлов и драгоценных камней и др.).

Правила и порядок осуществления банковских операций устанавливаются Национальным банком.

Особенности регулирования банковских операций с драгоценными металлами и драгоценными камнями устанавливаются специальным законодательством.

Банки и небанковские кредитно-финансовые организации помимо указанных в части первой настоящей статьи банковских операций в соответствии с законодательством Республики Беларусь вправе осуществлять:

- поручительство за третьих лиц, предусматривающее исполнение обязательств в денежной форме;
- приобретение права (требования) исполнения обязательств в денежной форме от третьих лиц;
- операции (сделки) с драгоценными металлами и драгоценными камнями, не предусмотренные частью первой настоящей статьи;
- финансовую аренду (лизинг);
- операции с использованием банковских пластиковых карточек, за исключением операции, указанной в абзаце четырнадцатом части первой настоящей статьи;
- консультационные и информационные услуги;
- выпуск, продажу, покупку, учет, хранение ценных бумаг, выполняющих функции расчетного документа, и иные операции с этими ценными бумагами, а также с ценными бумагами, подтверждающими привлечение денежных средств во вклады (депозиты) и на счета;
- перевозку денежной наличности, валютных и других ценностей;
- охрану принадлежащих банку объектов (денежных средств и иного имущества), а также охрану своих штатных работников;
- иную деятельность, предусмотренную законодательством Республики Беларусь.

Банки и небанковские кредитно-финансовые организации не вправе осуществлять производственную и (или) торговую деятельность, за исключением случаев, когда такая деятельность осуществляется для их собственных нужд.

Банки и небанковские кредитно-финансовые организации не вправе осуществлять страховую деятельность в качестве страховщиков.

Банки и небанковские кредитно-финансовые организации могут осуществлять отдельные виды деятельности, перечень которых определяется законодательством Республики Беларусь, только на основании специального разрешения (лицензии).

1.2.3 Небанковская кредитно-финансовая организация

Небанковская кредитно-финансовая организация - юридическое лицо, имеющее право осуществлять отдельные банковские операции и виды деятельности, предусмотренные статьей 14 настоящего Кодекса, за исключением осуществления в совокупности следующих банковских операций:

- привлечения денежных средств физических и (или) юридических лиц во вклады (депозиты);

- размещения привлеченных денежных средств от своего имени и за свой счет на условиях возвратности, платности и срочности;
- открытия и ведения банковских счетов физических и юридических лиц.

Допустимые сочетания банковских операций, которые могут осуществлять небанковские кредитно-финансовые организации, устанавливаются Национальным банком.

При создании небанковской кредитно-финансовой организации, осуществлении и прекращении ее деятельности применяются положения, предусмотренные для банков, если иное не установлено настоящим Кодексом и иным банковским законодательством.

К таким институтам относятся кредитные союзы и кооперативы, финансовые и трастовые компании, страховые компании, инвестиционные фонды, ломбарды и другие учреждения. Они осуществляют кредитование предприятий и граждан, выступают посредниками на рынке межбанковских кредитов, выполняют доверительные операции.

ТЕМА 2: НОРМАТИВНО-ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАТИЗАЦИИ И ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

2.1. Общие положения

На ближайших двух лекциях мы рассмотрим ряд законодательных актов, затрагивающих вопросы информатизации, применения электронно-цифровой подписи и ответственности возникающей в случае осуществления правонарушений в сфере информационной безопасности.

Информация все в большей степени становится товаром, от наличия и сохранности которого зависит благополучие как отдельных граждан и организаций, так и общества в целом. Отсюда неизбежно возникает проблема обеспечения информационной безопасности с целью предотвращения хищения или искажения информации, блокирования процесса ее получения, противодействия попыткам внедрения ложной информации. При этом необходимо учитывать то, что информация является весьма специфическим продуктом, который может существовать в материализованном и в не материализованном (нефиксированном) виде.

Правовая защита информации как ресурса признана на международном, государственном уровне и определяется межгосударственными договорами, конвенциями, декларациями и реализуется патентами, авторским правом и лицензиями на их защиту.

Дадим определение следующим понятиям:

- **под информационной безопасностью** понимается состояние защищенности жизненно важных интересов личности, общества и государства от внешних и внутренних угроз в сфере информационных отношений (*не в информационной сфере*).
- **под безопасностью информации** понимается такое ее состояние, при котором исключается возможность *ознакомления* с этой информацией, ее *изменения или уничтожения* лицами, не имеющими на это права, а также *утечки* за счет побочных электромагнитных излучений и наводок, специальных устройств перехвата (уничтожения) при передаче между объектами вычислительной техники.
- **под защитой информации** понимается совокупность мероприятий, направленных на обеспечение *конфиденциальности и целостности* обрабатываемой информации, а также *доступности информации* для пользователей.

Для защиты информации необходимо наличие целого комплекса правовых норм, которые определили бы правовой режим информации. В самом общем виде “правовой режим информации” следует понимать как совокупность нормативно установленных правил, определяющих:

- права собственности, владения и распоряжения информацией;
- степень открытости информации (необходимость или возможность ее отнесения к категории ограниченного доступа);
- порядок отнесения информации к категории ограниченного доступа и перечень уполномоченных на это лиц;
- порядок документирования, доступа, хранения, контроля и распространения информации;
- нормы, регулирующие применение различных средств и методов обеспечения информационной безопасности;
- порядок привлечения к ответственности и меры наказания за нарушение установленных норм и правил в области информационных отношений.

Комплексное изучение установленных норм и правил в конкретной прикладной области является обязательным элементом правовой культуры работающего в этой области специалиста.

2.2. Правовое обеспечение защиты информации

Можно выделить следующую структуру законодательства Республики Беларусь в области информатизации:

- Конституционное законодательство
- Общие законы, кодексы, которые включают нормы по вопросам информатизации и информационной безопасности
 - Банковский кодекс
 - Закон Республики Беларусь «О государственных секретах»
 - Закон Республики Беларусь «Об информатизации»
 - Закон Республики Беларусь «Об национальном архивном фонде и архивах Республики Беларусь»
 - Декрет Президента Республики Беларусь «О лицензировании отдельных видов деятельности» от 14 июля 2003 г. N 17
- Законы об организации управления
 - Закон Республики Беларусь «Об органах государственной безопасности»
 - Закон Республики Беларусь «О милиции»
- Специальные законы
 - Закон Республики Беларусь «Об электронном документе»
- Подзаконные акты

- Положение о Государственном центре безопасности информации при Президенте Республики Беларусь
- Положение о коммерческой тайне
- Инструкция о ДСП
- Правоохранительное законодательство
 - Уголовный кодекс
 - Гражданский кодекс
 - Кодекс об административных правонарушениях

Далее мы кратко рассмотрим некоторые законодательные акты.

2.3. Закон РБ О государственных секретах

Закон РБ «О государственных секретах» определяет правовые и организационные основы отнесения сведений к государственным секретам, защиты государственных секретов, осуществления иной деятельности в сфере государственных секретов в целях обеспечения национальной безопасности Республики Беларусь.

Под государственными секретами (сведениями, составляющими государственные секреты) будем понимать сведения, отнесенные в установленном порядке к государственным секретам, защищаемые государством в соответствии с законодательством Республики Беларусь.

К государственным секретам могут быть отнесены:

- сведения в области политики:
 - о стратегии и тактике внешней политики, а также внешнеэкономической деятельности;
 - о подготовке, заключении, содержании, выполнении, приостановлении или прекращении действия международных договоров Республики Беларусь;
 - об экспорте и импорте вооружения и военной техники;
 - о содержании или объемах экономического сотрудничества с иностранными государствами в военное время;
- сведения в области экономики и финансов:
 - о содержании планов подготовки экономики к отражению возможной военной агрессии;
 - о мобилизационных мощностях промышленности по изготовлению и ремонту вооружения и военной техники;
 - о планах (заданиях) государственного оборонного заказа, об объемах выпуска и поставках вооружения и военной техники, военно-технического имущества;
 - об объемах финансирования из республиканского бюджета

Вооруженных Сил Республики Беларусь, других войск и воинских формирований, правоохранительных и иных государственных органов, обеспечивающих национальную безопасность Республики Беларусь;

- о технологии изготовления системы защиты, применяемой при производстве денежных знаков, бланков ценных бумаг и других документов с определенной степенью защиты, обеспечиваемых государством;
- сведения в области науки и техники:
 - о содержании государственных и других программ, концепций по направлениям, определяющим национальную безопасность Республики Беларусь;
 - о проведении научно-исследовательских, опытно-технологических и опытно-конструкторских работ в интересах национальной безопасности Республики Беларусь;
- сведения в военной области:
 - о планах строительства Вооруженных Сил Республики Беларусь, содержании основных направлений (программ) развития вооружения и военной техники;
 - о тактико-технических характеристиках и возможностях боевого применения вооружения и военной техники;
 - о системе управления Вооруженными Силами Республики Беларусь;
 - о содержании стратегических или оперативных планов, планов территориальной обороны, документов боевого управления по подготовке и проведению операций, стратегическому развертыванию Вооруженных Сил Республики Беларусь, других войск и воинских формирований, их боевой, мобилизационной готовности и мобилизационных ресурсах;
 - о назначении, местонахождении, степени защищенности, системе охраны особо режимных и режимных объектов, пунктов управления государством в военное время или их проектировании, строительстве, эксплуатации, степени готовности;
- сведения в области разведывательной, контрразведывательной и оперативно-розыскной деятельности:
 - об организации, тактике, силах, средствах, объектах, методах, планах разведывательной, контрразведывательной и оперативно-розыскной деятельности, в том числе по обеспечению собственной безопасности в органах, осуществляющих такую деятельность;
 - о финансировании мероприятий, проводимых органами, осуществляющими разведывательную, контрразведывательную и оперативно-розыскную деятельность;
 - о гражданах, сотрудничающих (сотрудничавших) на конфиденциальной основе с органами, осуществляющими разведывательную, контрразведывательную и оперативно-розыскную деятельность, а также о штатных негласных сотрудниках и

сотрудниках этих органов, в том числе внедренных в организованные группы, выполняющих (выполнявших) специальные задания;

- сведения в информационной и иных областях национальной безопасности Республики Беларусь:
 - о содержании, организации или результатах основных видов деятельности Совета Безопасности Республики Беларусь, государственных органов, обеспечивающих национальную безопасность Республики Беларусь;
 - об организации, силах, средствах и методах обеспечения безопасности охраняемых граждан и защиты охраняемых объектов;
 - о финансировании мероприятий, проводимых в целях обеспечения безопасности охраняемых граждан и защиты охраняемых объектов;
 - о системе, методах и средствах защиты государственных секретов, состоянии защиты государственных секретов;
 - о шифрах, системах шифрованной, других видов специальной связи;
- иные сведения в области политики, экономики, финансов, науки, техники, в военной области, области разведывательной, контрразведывательной, оперативно-розыскной деятельности, информационной и иных областях национальной безопасности Республики Беларусь, которые включаются в перечень сведений, подлежащих отнесению к государственным секретам.

К государственным секретам не могут быть отнесены сведения:

- являющиеся общедоступной информацией, доступ к которой, распространение и (или) предоставление которой не могут быть ограничены в соответствии с законодательными актами Республики Беларусь;
- находящиеся в собственности иностранных государств, международных организаций, межгосударственных образований и переданные Республике Беларусь.

Государственные секреты подразделяются на две категории: государственную тайну (сведения, составляющие государственную тайну) и служебную тайну (сведения, составляющие служебную тайну).

Государственная тайна – сведения, в результате разглашения или утраты которых могут наступить тяжкие последствия для национальной безопасности Республики Беларусь.

Служебная тайна – сведения, в результате разглашения или утраты которых может быть причинен существенный вред национальной безопасности Республики Беларусь.

Служебная тайна может являться составной частью государственной тайны, не раскрывая ее в целом.

Для государственных секретов в зависимости от тяжести последствий, которые наступили или могут наступить, размера вреда, который причинен или может быть причинен в результате их разглашения или утраты, устанавливаются следующие **степени секретности**:

- для государственной тайны – «Особой важности», «Совершенно секретно»;
- для служебной тайны – «Секретно».

На носителях государственных секретов и (или) сопроводительной документации к ним в зависимости от степени секретности государственных секретов проставляются **грифы секретности**:

- на носителях государственной тайны и (или) сопроводительной документации к ним – «Особой важности», «Совершенно секретно»;
- на носителях служебной тайны и (или) сопроводительной документации к ним – «Секретно».

Допуск к госсекретам связан с ограничениями прав и дополнительными обязанностями для физических лиц. В соответствии с законодательством ограничиваются права выезда за границу, пользования и распоряжения секретными сведениями. Так, только руководитель организации, допускаящей к секретам, может разрешить работнику выехать за границу в период, оговоренный в договоре о допуске. Даже авторы секретных изобретений и открытий вправе распространять сведения о них только в порядке, определяемом секретным делопроизводством.

Наряду с ограничениями существуют определенные гарантии прав и интересов лиц, связанных с секретами. В первую очередь это касается защиты интеллектуальной собственности в сфере науки и технологий, обеспечении конкурентоспособности отечественных производителей на рынке наукоемкой продукции, а также права на получение более обширной информации по каким-либо вопросам или в определенной сфере деятельности, что для профессиональной деятельности многих весьма важно. Сейчас, например, ведется разработка нормативных правовых актов, которые будут регулировать вопросы защиты прав и законных интересов физических и юридических лиц в рассматриваемой сфере.

Кроме этого, законодательство предусматривает компенсации за ограничения прав носителя секретов, которые выражаются в виде доплат к должностному окладу или тарифной ставке в размерах, определяемых постановлениями Совмина, Минтруда и соцзащиты.

Допуск к государственным секретам гражданам предоставляется, если:

- граждане ознакомлены с правами и обязанностями, предусмотренными Законом «О государственных секретах» и другими актами законодательства Республики Беларусь о государственных секретах, с возможным временным ограничением их права на выезд из Республики Беларусь, а также с законодательными актами Республики Беларусь, устанавливающими ответственность за нарушение законодательства Республики Беларусь о государственных секретах;
- имеется письменное согласие граждан на проведение в отношении их проверочных мероприятий в связи с предоставлением им допуска к государственным секретам;
- гражданами представлены их персональные данные;
- гражданами приняты письменные обязательства перед государством о соблюдении законодательства Республики Беларусь о государственных секретах;
- имеется согласование уполномоченным государственным органом по защите государственных секретов предоставления им допуска к государственным секретам;
- проведены проверочные мероприятия в отношении граждан в связи с предоставлением им допуска к государственным секретам.

2.4. Положение о коммерческой тайне

06.11.1992 Советом Министров РБ было принято Положение о коммерческой тайне.

Данное положение определяет экономические и правовые основы защиты коммерческой тайны.

Коммерческую тайну составляют преднамеренно скрываемые экономические интересы и информация о различных сторонах и сферах производственно-хозяйственной, управленческой, научно-технической, финансовой деятельности субъекта хозяйствования, охрана которых обусловлена интересами конкуренции и возможной угрозой экономической безопасности субъекта хозяйствования.

Информация, составляющая коммерческую тайну, является собственностью субъекта хозяйствования либо находится в его владении, пользовании, распоряжении в пределах, установленных собственником и законодательными актами.

Информация, составляющая коммерческую тайну, должна соответствовать следующим требованиям:

- иметь действительную или потенциальную ценность для субъекта хозяйствования по коммерческим причинам;

- не являться общеизвестной или общедоступной согласно законодательству Республики Беларусь;
- обозначаться соответствующим образом с осуществлением субъектом хозяйствования надлежащих мер по сохранению ее конфиденциальности через систему классификации информации как коммерческой тайны, разработки внутренних правил засекречивания, введения соответствующей маркировки документов и иных носителей информации, организации секретного делопроизводства;
- не являться государственным секретом и не защищаться авторским и патентным правом;
- не касаться негативной деятельности субъекта хозяйствования, способной нанести ущерб интересам государства.

Коммерческую тайну субъекта хозяйствования не могут составлять:

- учредительные документы, а также документы, дающие право на занятие предпринимательской деятельностью и отдельными видами хозяйственной деятельности;
- сведения по установленным формам отчетности о финансово-хозяйственной деятельности и иные данные, необходимые для проверки правильности исчисления и уплаты налогов и других обязательных платежей;
- документы о платежеспособности;
- сведения о численности и составе работающих, их заработной плате и условиях труда, а также о наличии свободных рабочих мест.

Содержание и объем информации, составляющей коммерческую тайну, а также порядок ее защиты определяются руководителем субъекта хозяйствования, который доводит их до работников либо лиц, имеющих доступ к таким сведениям.

Работники субъекта хозяйствования и лица, заключившие гражданско-правовые договоры, имеющие доступ к коммерческой тайне субъекта хозяйствования, принимают обязательство сохранять коммерческую тайну и без разрешения, выданного в установленном порядке, не разглашать сведения, ее составляющие, при условии, что эта информация ранее не была известна работникам или иному лицу, получившему к ней доступ, либо не была получена от третьей стороны без обязательства соблюдать в отношении ее конфиденциальность.

Данное обязательство дается в письменной форме при приеме на работу, заключении гражданско-правового договора либо в процессе его исполнения.

Указанные лица вправе передать конфиденциальную информацию третьим лицам в случае привлечения их к деятельности, требующей знания такой информации, только в том объеме, который необходим для реализации целей и задач субъекта хозяйствования.

Передача третьим лицам информации, являющейся коммерческой тайной, влечет за собой установленную законодательством ответственность при условии, что сведения содержались в тайне, что они были в установленном порядке вверены разгласившему их лицу без согласия на разглашение и что разглашением был причинен ущерб.

2.5. Закон РБ «Об электронном документе и электронной цифровой подписи»

Впервые Закон об электронном документе был принят в Беларуси 10 января 2000 года.

Однако в связи с необходимостью более широкого применения электронных документов в деятельности различных субъектов хозяйствования нашей страны, а также с целью создания правовой предпосылки построения инфраструктуры открытых ключей, в декабре 2009г. был подписан новый Закон Республики Беларусь «Об электронном документе и электронной цифровой подписи».

Данный Закон устанавливает правовые основы применения электронных документов, определяет основные требования, предъявляемые к электронным документам, а также права, обязанности и ответственность участников правоотношений, возникающих в сфере обращения электронных документов.

Рассмотрим основные понятия, применяемые в данном законе:

Электронный документ (далее ЭД) – документ в электронном виде с реквизитами, позволяющими установить его целостность и подлинность.

Под **подлинностью** понимается свойство электронного документа, определяющее, что электронный документ подписан действительной электронной цифровой подписью (или несколькими электронными цифровыми подписями). **Целостность** ЭД - это свойство электронного документа, определяющее, что в электронный документ не были внесены изменения и (или) дополнения (например, в процессе его передачи по каналам связи).

Реквизитом, позволяющим установить подлинность и целостность ЭД является **электронная цифровая подпись** (далее ЭЦП).

Для генерации ЭЦП используются асимметричные алгоритмы. В таких алгоритмах применяется пара ключей – открытый и закрытый (личный).

Личный ключ электронной цифровой подписи (далее – личный ключ) – последовательность символов, принадлежащая определенной организации или

физическому лицу и используемая при выработке электронной цифровой подписи.

Открытый ключ — последовательность символов, соответствующая определенному личному ключу, доступная для всех заинтересованных организаций или физических лиц и применяемая при проверке электронной цифровой подписи.

Необходимым условием того, чтобы электронный документ имел юридическую силу на территории Беларуси, для генерации ЭЦП необходимо использовать сертифицированные средства ЭЦП.

Под **средством ЭЦП** будем понимать программное, программно-техническое или техническое средство, с помощью которого реализуются одна или несколько из следующих функций: выработка электронной цифровой подписи, проверка электронной цифровой подписи, выработка личного ключа или открытого ключа.

При широком использовании электронных документов встает вопрос о передаче открытого ключа ЭЦП своим контрагентам, таким образом, чтобы сохранилась его целостность и подлинность.

Именно с этой целью встает вопрос о создании инфраструктуры открытых ключей (создание правил и организационно-технических способов их распространения).

Как правило, распространения открытых ключей происходит посредством сертификатов открытого ключа.

Сертификат открытого ключа — электронный документ, изданный поставщиком услуг и содержащий информацию, подтверждающую принадлежность указанного в нем открытого ключа определенной организации или физическому лицу, и иную информацию, предусмотренную законодательством Республики Беларусь.

Электронный документ состоит из двух неотъемлемых частей — общей и особенной.

Общая часть электронного документа состоит из информации, составляющей содержание документа.

Особенная часть электронного документа состоит из одной или нескольких электронных цифровых подписей, а также может содержать дополнительные данные, необходимые для проверки электронной цифровой подписи (электронных цифровых подписей) и идентификации электронного документа, которые устанавливаются техническими нормативными правовыми актами.

Оригинал электронного документа существует только в электронном виде. Все идентичные экземпляры электронного документа являются оригиналами и имеют одинаковую юридическую силу.

Документы, созданные организацией или физическим лицом на бумажном носителе и в электронном виде, идентичные по содержанию, имеют одинаковую юридическую силу. В этом случае документ на бумажном носителе не является копией электронного документа.

Копией электронного документа считается форма внешнего представления электронного документа на бумажном носителе, удостоверенная в порядке, установленном законодательством Республики Беларусь.

Удостоверять ЭД могут:

- нотариус или другое должностное лицо, имеющее право совершать нотариальные действия;
- организация или индивидуальный предприниматель, имеющий право на осуществление подобной деятельности.

Копия электронного документа должна содержать указание на то, что она является копией соответствующего электронного документа.

Стоит отметить, что подлинный электронный документ приравнивается к документу на бумажном носителе, подписанному собственноручно, и имеет одинаковую с ним юридическую силу.

Сегодня электронные документы широко применяются в банковских организациях Беларуси. Например, большинство документов между Национальным банком и коммерческими банками, а также между ком.банком и его клиентами идет в виде электронных документов.

ТЕМА 3: ОТВЕТСТВЕННОСТЬ ЗА ПРЕСТУПЛЕНИЯ ПРОТИВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

3.1. Общие положения

В данной теме мы рассмотрим некоторые аспекты законодательства Республики Беларусь, регулирующего правоотношения в сфере ответственности за совершение противоправных деяний, связанных с ИТ-технологиями.

Согласно Гражданскому кодексу Республики Беларусь (далее ГК) можно выделить следующие виды объектов гражданских прав:

- вещи, включая деньги и ценные бумаги, иное имущество, в том числе имущественные права;
- работы и услуги;
- охраняемая информация;
- исключительные права на результаты интеллектуальной деятельности (интеллектуальная собственность);
- нематериальные блага.

В случаях и порядке, установленных ГК и иным законодательством, признается исключительное право (интеллектуальная собственность) гражданина или юридического лица на охраняемые результаты интеллектуальной деятельности и приравненные к ним средства индивидуализации юридического лица, индивидуализации продукции, выполняемых работ и услуг (фирменное наименование, товарный знак, знак обслуживания и т.п.).

Использование результатов интеллектуальной собственности и средств индивидуализации, которые являются объектом исключительных прав, может осуществляться третьими лицами только с согласия правообладателя.

В прошлой теме мы уже рассматривали понятие коммерческой тайны. В ГК дается следующее понятие служебной и коммерческой тайны:

Информация составляет служебную или коммерческую тайну в случае, когда информация имеет действительную или потенциальную коммерческую ценность в силу неизвестности ее третьим лицам, к ней нет свободного доступа на законном основании и обладатель информации принимает меры к охране ее конфиденциальности.

Лица, незаконными методами получившие информацию, которая составляет служебную или коммерческую тайну, обязаны возместить причиненные убытки. Такая же обязанность возлагается на работников, разгласивших служебную или

коммерческую тайну вопреки трудовому договору, в том числе контракту, и на контрагентов, сделавших это вопреки гражданско-правовому договору.

Условия правовой охраны нераскрытой информации

Согласно статьи 1010 ГК лицо, правомерно обладающее технической, организационной или коммерческой информацией, в том числе секретами производства (ноу-хау), не известной третьим лицам (нераскрытая информация), имеет право на защиту этой информации от незаконного использования, если соблюдены условия, установленные пунктом 1 статьи 140 настоящего Кодекса.

Право на защиту нераскрытой информации от незаконного использования возникает независимо от выполнения в отношении этой информации каких-либо формальностей (ее регистрации, получения свидетельств и т.п.).

Лицо, без законных оснований получившее или распространившее нераскрытую информацию либо использующее ее, обязано возместить тому, кто правомерно обладает этой информацией, убытки, причиненные ее незаконным использованием.

Если лицо, незаконно использующее нераскрытую информацию, получило ее от лица, которое не имело права ее распространять, о чем приобретатель информации не знал и не должен был знать (добросовестный приобретатель), правомерный обладатель нераскрытой информации вправе потребовать от него возмещения убытков, причиненных использованием нераскрытой информации после того, как добросовестный приобретатель узнал, что ее использование незаконно.

Лицо, правомерно обладающее нераскрытой информацией, вправе потребовать от того, кто ее незаконно использует, немедленного прекращения ее использования. Однако суд с учетом средств, израсходованных добросовестным приобретателем нераскрытой информации на ее использование, может разрешить ее дальнейшее использование на условиях возмездной исключительной лицензии.

Лицо, самостоятельно и правомерно получившее сведения, составляющие содержание нераскрытой информации, вправе использовать эти сведения независимо от прав обладателя соответствующей нераскрытой информации и не отвечает перед ним за такое использование.

Ответственность за разглашение коммерческой тайны также предусмотрена Уголовным кодексом Республики Беларусь (далее УК РБ). Согласно статье 255 умышленное разглашение коммерческой или банковской тайны без согласия ее владельца при отсутствии признаков преступления, предусмотренного статьей

254 УК РБ, лицом, которому такая коммерческая или банковская тайна известна в связи с его профессиональной или служебной деятельностью, повлекшее причинение ущерба в крупном размере, - наказывается штрафом, или лишением права занимать определенные должности или заниматься определенной деятельностью, или арестом на срок до шести месяцев, или ограничением свободы на срок до трех лет, или лишением свободы на тот же срок.

То же действие, совершенное из корыстной или иной личной заинтересованности, - наказывается ограничением свободы на срок до четырех лет или лишением свободы на срок до пяти лет.

3.2. Преступления в сфере высоких технологий

Первое высокотехнологичное преступление на территории нашей республики было зарегистрировано 20 ноября 1998 года. Внедрив в программное обеспечение «компьютера-жертвы» вредоносную программу типа «троянский конь» под названием «BackOrifice», злоумышленник осуществил несанкционированный доступ к сетевым реквизитам пользователей сети Интернет из числа клиентов крупнейшего в Беларуси столичного сервис-провайдера.

В 2001 году руководство МВД республики проанализировало криминогенную ситуацию, складывающуюся в сфере компьютерной информации и телекоммуникаций в нашей стране, а также странах дальнего и ближнего зарубежья, принимая во внимание правонарушения, зарегистрированные в 1998–2000 годах, вступление в действие нового Уголовного кодекса, предусматривающего ответственность за преступления против информационной безопасности, а также высокую степень вероятности дальнейшего распространения киберпреступности на территории нашей республики, было принято решение о создании подразделения, специализирующегося на профилактике и раскрытии злодеяний данной категории.

На данный момент раскрытием высокотехнологичных преступлений занимается Управление по раскрытию преступлений в сфере высоких технологий МВД РБ.

На протяжении последних 8 лет количество официально зарегистрированных преступлений в сфере высоких технологий постоянно растет (правда стоит отметить, что темпы прироста постепенно снижаются).

- в 2007 году – зарегистрировано 996 преступлений;
- в 2008 – 1614 (+618);
- в 2009 – 2154 (+540);

- в 2010 – 2514 (+360).

Далее приведены статьи УК РБ, предусматривающие ответственность за высокотехнологичные преступления.

Статья 212. Хищение путем использования компьютерной техники

1. Хищение имущества путем изменения информации, обрабатываемой в компьютерной системе, хранящейся на машинных носителях или передаваемой по сетям передачи данных, либо путем введения в компьютерную систему ложной информации – наказывается штрафом, или лишением права занимать определенные должности или заниматься определенной деятельностью, или арестом на срок до шести месяцев, или ограничением свободы на срок до трех лет, или лишением свободы на тот же срок.

2. То же деяние, совершенное повторно, либо группой лиц по предварительному сговору, либо сопряженное с несанкционированным доступом к компьютерной информации, – наказывается ограничением свободы на срок от двух до пяти лет или лишением свободы на срок до пяти лет с лишением права занимать определенные должности или заниматься определенной деятельностью или без лишения.

3. Деяния, предусмотренные частями первой или второй настоящей статьи, совершенные в крупном размере, – наказываются лишением свободы на срок от трех до десяти лет с конфискацией имущества или без конфискации и с лишением права занимать определенные должности или заниматься определенной деятельностью или без лишения.

4. Деяния, предусмотренные частями первой, второй или третьей настоящей статьи, совершенные организованной группой либо в особо крупном размере, – наказываются лишением свободы на срок от шести до пятнадцати лет с конфискацией имущества и с лишением права занимать определенные должности или заниматься определенной деятельностью или без лишения.

Глава 31. Преступления против информационной безопасности

Статья 349. Несанкционированный доступ к компьютерной информации

1. Несанкционированный доступ к информации, хранящейся в компьютерной системе, сети или на машинных носителях, сопровождающийся нарушением системы защиты и повлекший по неосторожности изменение, уничтожение, блокирование информации или вывод из строя компьютерного оборудования либо причинение иного существенного вреда, - наказывается штрафом или арестом на срок до шести месяцев.

2. То же действие, совершенное из корыстной или иной личной заинтересованности, либо группой лиц по предварительному сговору, либо лицом, имеющим доступ к компьютерной системе или сети, - наказывается штрафом, или лишением права занимать определенные должности или заниматься определенной деятельностью, или арестом на срок от трех до шести

месяцев, или ограничением свободы на срок до двух лет, или лишением свободы на тот же срок.

3. Несанкционированный доступ к компьютерной информации либо самовольное пользование электронной вычислительной техникой, средствами связи компьютеризованной системы, компьютерной сети, повлекшие по неосторожности крушение, аварию, катастрофу, несчастные случаи с людьми, отрицательные изменения в окружающей среде или иные тяжкие последствия, - наказываются ограничением свободы на срок до пяти лет или лишением свободы на срок до семи лет.

Статья 350. Модификация компьютерной информации

1. Изменение информации, хранящейся в компьютерной системе, сети или на машинных носителях, либо внесение заведомо ложной информации, причинившие существенный вред, при отсутствии признаков преступления против собственности (модификация компьютерной информации) - наказываются штрафом, или лишением права занимать определенные должности или заниматься определенной деятельностью, или арестом на срок от трех до шести месяцев, или ограничением свободы на срок до трех лет, или лишением свободы на тот же срок.

2. Модификация компьютерной информации, сопряженная с несанкционированным доступом к компьютерной системе или сети либо повлекшая по неосторожности последствия, указанные в части третьей статьи 349 настоящего Кодекса, - наказывается ограничением свободы на срок до пяти лет или лишением свободы на срок до семи лет с лишением права занимать определенные должности или заниматься определенной деятельностью или без лишения.

Статья 351. Компьютерный саботаж

Умышленные уничтожение, блокирование, приведение в непригодное состояние компьютерной информации или программы, либо вывод из строя компьютерного оборудования, либо разрушение компьютерной системы, сети или машинного носителя (компьютерный саботаж) - наказываются штрафом, или лишением права занимать определенные должности или заниматься определенной деятельностью, или арестом на срок от трех до шести месяцев, или ограничением свободы на срок до пяти лет, или лишением свободы на срок от одного года до пяти лет.

2. Компьютерный саботаж, сопряженный с несанкционированным доступом к компьютерной системе или сети либо повлекший тяжкие последствия, - наказывается лишением свободы на срок от трех до десяти лет.

Статья 352. Неправомерное завладение компьютерной информацией

Несанкционированное копирование либо иное неправомерное завладение информацией, хранящейся в компьютерной системе, сети или на машинных носителях, либо перехват информации, передаваемой с использованием средств компьютерной связи, повлекшие причинение существенного вреда, - наказываются общественными работами, или штрафом, или арестом на срок до

шести месяцев, или ограничением свободы на срок до двух лет, или лишением свободы на тот же срок.

Статья 353. Изготовление либо сбыт специальных средств для получения неправомерного доступа к компьютерной системе или сети

Изготовление с целью сбыта либо сбыт специальных программных или аппаратных средств для получения неправомерного доступа к защищенной компьютерной системе или сети - наказываются штрафом, или арестом на срок от трех до шести месяцев, или ограничением свободы на срок до двух лет.

Статья 354. Разработка, использование либо распространение вредоносных программ

1. Разработка компьютерных программ или внесение изменений в существующие программы с целью несанкционированного уничтожения, блокирования, модификации или копирования информации, хранящейся в компьютерной системе, сети или на машинных носителях, либо разработка специальных вирусных программ, либо заведомое их использование, либо распространение носителей с такими программами - наказываются штрафом, или арестом на срок от трех до шести месяцев, или ограничением свободы на срок до двух лет, или лишением свободы на тот же срок.

2. Те же действия, повлекшие тяжкие последствия, - наказываются лишением свободы на срок от трех до десяти лет.

Статья 355. Нарушение правил эксплуатации компьютерной системы или сети

1. Умышленное нарушение правил эксплуатации компьютерной системы или сети лицом, имеющим доступ к этой системе или сети, повлекшее по неосторожности уничтожение, блокирование, модификацию компьютерной информации, нарушение работы компьютерного оборудования либо причинение иного существенного вреда, - наказывается штрафом, или лишением права занимать определенные должности или заниматься определенной деятельностью, или исправительными работами на срок до двух лет, или ограничением свободы на тот же срок.

2. То же деяние, совершенное при эксплуатации компьютерной системы или сети, содержащей информацию особой ценности, - наказывается лишением права занимать определенные должности или заниматься определенной деятельностью, или ограничением свободы на срок до трех лет, или лишением свободы на тот же срок.

3. Деяния, предусмотренные частями первой или второй настоящей статьи, повлекшие по неосторожности последствия, указанные в части третьей статьи 349 настоящего Кодекса, - наказываются ограничением свободы на срок до пяти лет или лишением свободы на срок до семи лет с лишением права занимать

определенные должности или заниматься определенной деятельностью или без лишения.

3.3. Типы преступлений

Наиболее популярными ИТ-преступлениями являются следующие:

- Хищение денежных средств, используя украденные реквизиты банковских пластиковых карточек;
- «Нигерийские письма», «Лотерии», «Аукционы», «Брачные контракты», «Финансовые пирамиды»;
- Мобильные телефоны;
- Фишинг.

Приведем пример некоторых преступлений (согласно официального ресурса Управления К МВД РБ):

Нигерийские письма

Как правило, в данной корреспонденции рассказывается о том, что некто, являясь наследником крупного состояния, по каким либо причинам не может его получить, а поэтому просит о денежной помощи, обещая вернуть многократно больше. Алгоритм дальнейших действий понятен. К сожалению, среди нас есть еще те, кто хочет опровергнуть известную пословицу про сыр в мышеловке.

Письмо от «жены» бывшего диктатора Заира»:

Dear friend,

I am Mrs. Sese-seko widow of late President Mobutu Sese-seko of Zaire, now known as Democratic Republic of Congo (DRC). I am moved to write you this letter. This was in confidence considering my present circumstance and situation. I escaped along with my husband and two of our sons Alfred and Basher out of Democratic Republic of Congo (DRC) to Abidjan, Cote d'ivoire where my family and I settled, while we later moved to settled in Morroco where my husband later died of cancer disease.

I have deposited the sum Eighteen Million United State Dollars (US\$ 18,000,000,00.) With a security company for safe keeping. What I want you to do is to indicate your interest that you can assist us in receiving the money on our behalf, so that I can introduce you to my son (Alfred) who has the out modalities for the claim of the said funds. I want you to assist in investing this money, but I will not want my identity revealed. I will also want to acquire real/landed properties and stock in multi-national companies and to engage in other safe and non-speculative investments as advise by your good self.

Yours sincerely, Mrs. Mariam M. Seseseiko.

На самом деле, все вышеописанное является распространенным видом мошенничества, для совершения которого меняется лишь содержание.

В августе 2004 года на электронный почтовый ящик одного из жителей нашей столицы пришло письмо на английском языке, в котором предлагалось инвестировать деньги под какие-нибудь проекты. Белоруса заинтересовало предложение, поскольку он искал инвесторов для строительства торгового центра в Минске. Последний вступил в переписку с человеком, представившимся гражданином ЮАР – работником Министерства горнодобывающей промышленности. В ходе телефонных переговоров потерпевшему было предложено приехать в Лондон для заключения контракта. В столице Великобритании предприимчивого белоруса встретили на дорогой автомашине и отвезли в шикарно обставленное офисное помещение, которое злоумышленники представили гражданину Республики Беларусь как банк. Здесь и состоялось подписание контракта. Далее, минчанин в несколько этапов осуществил перечисление денежных средств на счета, предоставленные компаньонами. Надо ли говорить, что ни денег, ни новых знакомых, белорусский предприниматель больше не увидел.

Общая сумма ущерба от мошеннических действий в отношении незадачливого предпринимателя составила около 700 тысяч долларов США и более 30 тысяч английских фунтов.

Разновидность «нигерийских писем»

Лотерея	Аукцион	Работа	Брачный контакт
Открываете электронный ящик и с удивлением читаете письмо: «С радостью сообщаем, что Вы стали победителем нашей лотереи и выиграли главный приз – автомобиль! Для оформления расходов по доставке приза	На специальных сайтах проводятся торги, в качестве лотов которых оказываются дорогостоящие вещи. Вы торгуетесь, посредством персонального банковского чека или чека почтового ведомства, оплачиваете	Речь идет о письмах с предложениями «\$200 в день», «\$500 в день» за несложную законную работу в интернете. Потенциальным жертвам предлагается сделать выгодные капиталовложения или устроиться на высокооплачиваемую работу, перечислив мизерную сумму.	Все, что для этой аферы требуется: придуманное имя, несколько фотографий молодых и красивых славянок. Жулик тонко «обрабатывает» жертву, играя на слабостях человека. Виртуальный роман заканчивается

<p>переведите такую-то сумму». Для убедительности высылаются всевозможные атрибуты, подтверждающие подлинность: фотография автомобиля, номер лицензии, свидетельство о регистрации и прочая сфабрикованная макулатура.</p>	<p>товар и ждете его. В лучшем случае, вместо заказанных вами швейцарских часов, получите однодневные часы «желтой» сборки. А в худшем – ваши деньги растворяются в реальных карманах виртуальных мошенников.</p>		<p>тем, что жертва высылает деньги на оплату визы и билетов для «возлюбленной». Самое удивительное то, что даже спустя месяцы после обмана любовник с цветами продолжает выжидать свою подружку в аэропорту...</p>
--	---	--	--

ТЕМА 4: РЫНКИ, ФОНДЫ, ДЕНЬГИ. СТРУКТУРА ФИНАНСОВО-КРЕДИТНОЙ СИСТЕМЫ РБ

4.1. Общие положения

Дадим основные понятия и определения, которые нам будут нужны в данной теме.

Рынок— вся совокупность форм и организаций сотрудничества людей друг с другом, предназначенных для того, чтобы свести вместе в коммерческих целях продавцов и покупателей и дать возможным первым продать, а вторым купить товары.

Фондовый рынок— комплекс организаций (прежде всего фондовая биржа), обеспечивающих куплю продажу акций и облигаций и потому позволяющих фирмам привлекать денежные средства (фонды) для своего развития в обмен на такие ценные бумаги.

Фондовая биржа — организация, осуществляющая торговлю ценными бумагами коммерческих фирм и обеспечивающая за счет этого переток средств акционеров из одной фирмы или отрасли в другую.

Дилер— биржевой посредник, покупающий товар от своего имени и на свои деньги с целью последующей продажи на бирже.

Брокер — биржевой посредник, покупающий товар от имени клиента и на его деньги

Треjder — 1) работник брокерской фирмы, непосредственно исполняющий заказы на куплю-продажу ценных бумаг в торговом зале биржи. 2) любое юридическое или физическое лицо, имеющее право заключать сделки на бирже.

В первой теме мы уже первично познакомились с финансово-кредитной системой Республики Беларусь.

Финансово-кредитная система является ключевым элементом, обеспечивающим движение капитала между субъектами финансово-экономической системы Республики Беларусь.

Структурно ФКС включает:

- банковскую систему
- платежную систему
- систему финансовых рынков.

Субъектами ФКС являются:

- Национальный банк и иные банки,
- небанковские кредитно-финансовые организации,

- государственные органы, органы местного управления и самоуправления,
- физические и юридические лица.

Объектом управления ФКС являются деньги (валюта), ценные бумаги и валютные ценности. От эффективности функционирования ФКС в целом зависит эффективность денежного обращения в ФЭС, значит, и показатели финансово-экономической деятельности Республики Беларусь.

Функциональная структура ФКС и основные потоки капиталов в ней показаны на рис.1.

В ФКС Национальный банк выступает как орган денежно–кредитного регулирования, как участник банковской системы и как субъект хозяйственной деятельности.

Как центральный банк Республики Беларусь, Национальный банк разрабатывает и совместно с Правительством Республики Беларусь проводит единую денежно-кредитную политику, отвечающую динамичному социально-экономическому развитию страны, реализует монетарную политику на внутренних и внешних финансовых рынках, направленную на защиту и обеспечение устойчивости национальной валюты.

Как участник банковской системы, Национальный банк кредитует и выполняет функции финансового агента Правительства Республики Беларусь и местных исполнительных и распорядительных органов по вопросам исполнения республиканского и местных бюджетов, организует расчетное и (или) кассовое обслуживание отдельных государственных органов, перечень которых определен в Уставе Национального банка.

Как субъект хозяйствования – осуществляет организационное и хозяйственное обеспечение деятельности Национального банка в целом.

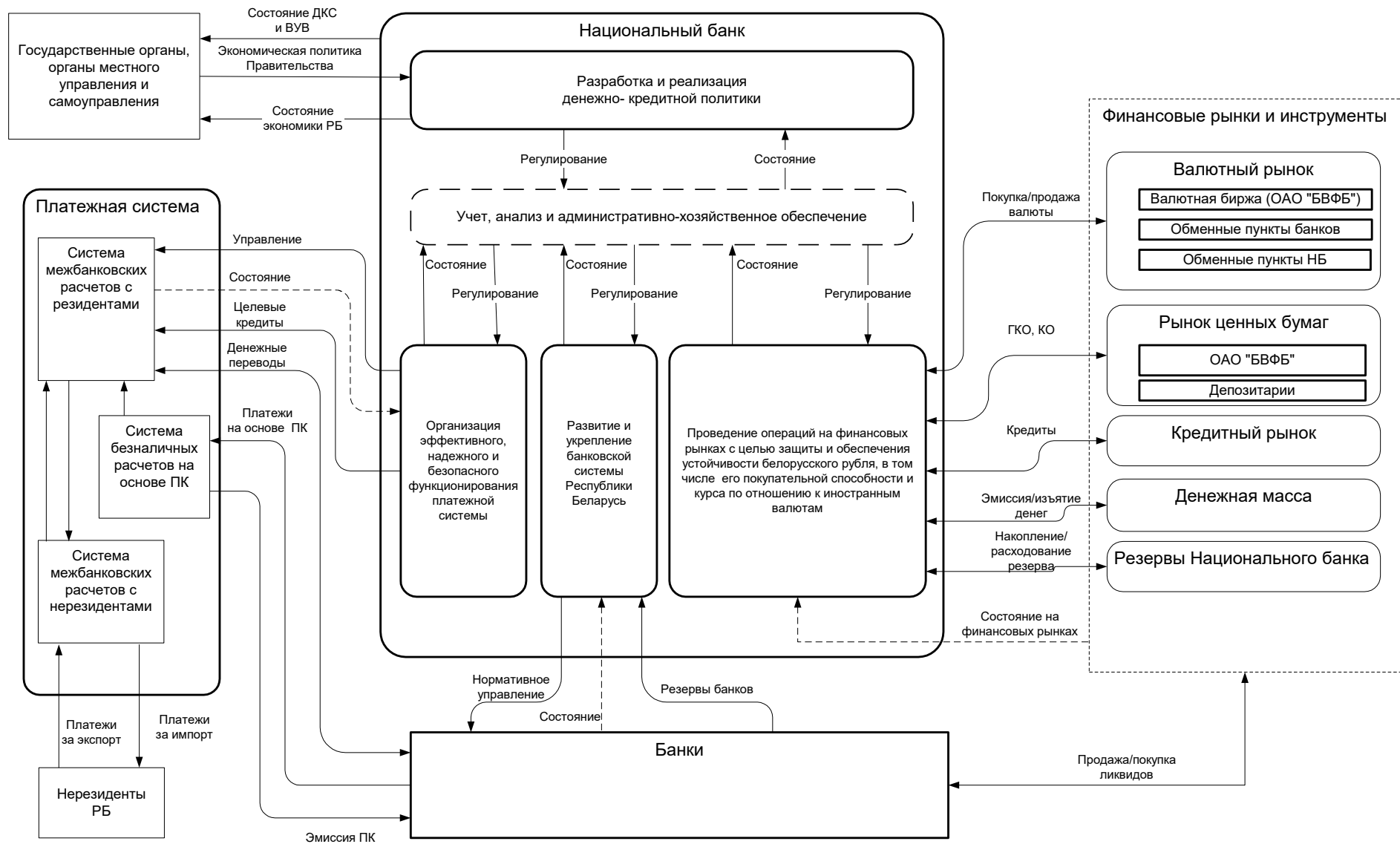


Рис. 1. Функциональная структура ФКС

4.2. Фондовый рынок

Фондовый рынок - это институт или механизм, сводящий вместе покупателей (предъявителей спроса) и продавцов (поставщиков) фондовых ценностей, т.е. ценных бумаг.

Понятия фондового рынка и рынка ценных бумаг совпадают. Согласно определению, товаром, обращающимся на данном рынке, являются ценные бумаги, которые, в свою очередь, определяют состав участников данного рынка, его местоположение, порядок функционирования, правила регулирования и т.п.

Участники рынка ЦБ

Состав участников рынка ценных бумаг зависит от той степени на которой находится производство и банковская система, а также каковы экономические функции государства. Этим определяется способ финансирования производства и государственных расходов. Важным является также и объем накопления средств у населения сверх удовлетворения необходимых текущих потребностей.

Если мелкое производство финансируется за счет собственных накоплений и капиталов собственников - владельцев производства и банковских кредитов, то крупное акционерное производство финансирует свои капитальные затраты почти полностью за счет эмиссии акций и облигаций. Результатом является отделение собственности и финансирования предприятий от самого производства.

Государство в лице центрального правительства и местных органов власти со временем все в большей степени прибегает к заимствованию средств для финансирования бюджетных расходов в дополнение к взиманию налогов, а также в интервалах между поступлениями налогов. Главную массу эмитентов акций составляют нефинансовые корпорации. Они же выпускают среднесрочные и долгосрочные облигации, предназначенные как для пополнения их основного капитала, так и для реализации различных инвестиционных программ, связанных с расширением и модернизацией производства.

Важнейшую посредническую роль на рынке ценных капитальных бумаг играют инвестиционные банки - особые финансовые институты, которые занимаются организацией и гарантированием реализации публичного размещения прежде всего акций. В качестве консультанта по всем финансовым вопросам, связанным с эмиссией, банк вместе с потенциальным эмитентом определяет реальные и наиболее экономичные возможности выхода на конкретный рынок, а затем в качестве ведущего гаранта берет на себя обязанность организовать

синдикат или другую группу, которая обеспечит полное размещение выпущенных ценных бумаг. В случае неправильной оценки ситуации банк рискует не разместить бумаги, оставить их у себя, а затем продать со скидкой. В США старейшей (с 1885 года) и крупнейшей компанией - инвестиционным банком - является "Мерилл Линч". На конец 80-х годов у нее было несколько миллионов клиентов в США и за рубежом, в том числе частные лица, фирмы и правительства, она имеет около полусотни отделений в 40 странах мира.

Некоторые виды ценных бумаг:

Акция – Ценная бумага, удостоверяющая право собственности на долю в капитале акционерного общества, свидетельствующая о вносе определенной суммы денег и дающая право на получение ежегодного дохода в виде дивидендов.

Акция обыкновенная (простая) - Акция, дающая право на получение дохода в зависимости от результата деятельности акционерного общества, а также принимать участие в управлении и голосовании на общем собрании акционеров.

Акция привилегированная - Акция, не дающая права голоса на общем собрании акционеров, но дающая право на фиксированный дивиденд, выплачиваемый в первоочередном порядке независимо от результатов деятельности акционерного общества, при ликвидации акционерного общества или его реорганизации.

Акция именная - Закрепляется за акционером посредством занесения его фамилии в саму акцию и в книгу записей.

Акция на предъявителя - Принадлежит только ее фактическому владельцу и не закрепляется за каким-либо конкретным лицом. Передача такой акции означает автоматическую смену ее владельца.

Подписка на акции - договор, в рамках которого каждый из подписавшихся обязуется внести известную сумму в уставный фонд АО в качестве своего пая или его части.

Облигация - ценная бумага, подтверждающая обязательство эмитента возместить владельцу ценной бумаги ее номинальную стоимость в установленный срок с уплатой фиксированного процента (если иное не предусмотрено условиями выпуска).

К государственным эмиссионным ценным бумагам относятся:

- государственные краткосрочные облигации со сроком обращения до одного года;
- государственные долгосрочные облигации со сроком обращения один год и более.

Облигации и акции имеют номинал и рыночную цену. Рыночная цена облигации, выраженная в процентах к ее номиналу, называется курсом облигации. Если рыночная цена облигации выше номинала, то говорят, что она продается с премией. Если цена меньше номинала, то новый владелец покупает ее с дисконтом. Если покупатель платит номинал, то имеет место паритет. Какова бы ни была рыночная цена облигации, процент по ней исчисляется к номиналу.

Кроме эмиссионной и рыночной цен, акции имеют и балансовую цену. Это так называемая бухгалтерская или "книжная" цена, определяемая на основе документов финансовой отчетности. Она исчисляется путем деления чистой стоимости активов (активы корпорации минус ее пассивы) на количество размещенных акций, т.е. величиной принадлежащего акционерам капитала, приходящейся на одну акцию.

Первичный и вторичный фондовый рынок

Любой фондовый рынок делится на первичный и вторичный.

Первичный рынок объединяет фазу конструирования нового выпуска ценных бумаг и их первичное размещение. Вторичный рынок - это рынок, на котором обращаются ранее эмитированные на первичном рынке ценные бумаги.

Важнейшей чертой первичного рынка является полное раскрытие информации для инвесторов, позволяющее сделать обоснованный выбор ценной бумаги для вложения денежных средств. Вся деятельность на первичном рынке служит для раскрытия информации: подготовка проспекта эмиссии, его регистрация и контроль государственными органами с позиций полноты представленных данных, публикация проспекта и итогов подписки и т.д.

Существует две формы первичного рынка ценных бумаг:

- частное размещение;
- публичное предложение.

Частное размещение характеризуется продажей (обменом) ценных бумаг ограниченному количеству заранее известных инвесторов без публичного предложения и продажи. Публичное предложение - это размещение ценных бумаг при их первичной эмиссии путем публичных объявления и продажи неограниченному числу инвесторов.

Соотношение между публичным предложением и частным размещением постоянно меняется и зависит от типа финансирования, который избирают предприятия в той или иной экономике, от структурных преобразований,

которые проводит правительство, и других факторов. Публичная подписка или публичное размещение ценных бумаг применяется тогда, когда корпорация принимает решение превратиться из частной в публичное акционерное общество с большим количеством акционеров. Разница не просто в количестве эмитируемых акций: речь идет о контроле над предприятием, который может в этих условиях перейти от учредителей к владельцам контрольного пакета акций. Публичное предложение большого количества тиражированных акций дает эмитенту огромные средства, которые открывают возможности расширения, модернизации, диверсификации деятельности, делает компанию известной, она переходит на новый, более высокий уровень престижности. Крупнейшие американские публичные акционерные компании типа AT&T - Америкен Телефон Энд Телеграф Компани. Первичные рынки отдельных видов ценных бумаг имеют свои особенности организации. Так, в США первичный рынок для правительственных вновь эмитированных облигаций закреплен за 41 компанией, зарегистрированных в качестве первичного дилера по правительственным бумагам.

Относительно небольшая доля ценных бумаг после первичного распределения остается в портфелях держателей до истечения срока облигаций или в течение всего срока существования предприятия, если речь идет об акциях. Ценные бумаги в большинстве случаев приобретаются для извлечения дохода не столько из процентных выплат, сколько от перепродажи.

По организации торговли ценными бумагами различают биржевой и внебиржевой рынки.

Биржевой рынок - это организованный рынок ценных бумаг, операции, по купле-продаже которых осуществляются на бирже в строгом соответствии с установленными правилами. На биржевом рынке ведется торговля ценными бумагами наиболее надежных эмитентов, которые допускаются на биржу только после прохождения определенной процедуры отбора, и за их деятельностью ведется постоянный контроль со стороны биржи. Биржевая торговля проводится в специально оборудованном помещении (бирже) по строгому графику в течение биржевых (торговых) сессий и по жестким правилам, установленным биржей, которые обязательны для исполнения участниками торгов.

Внебиржевой рынок - это рынок, на котором операции купли продажи ценных бумаг осуществляются вне помещений биржи. В зависимости от наличия установленных правил торговли различают организованный и неорганизованный внебиржевые рынки. По принципу возвратности денежных средств инвестору различают рынок долговых финансовых инструментов и рынок прав собственности (рынок долевых ценных бумаг).

На рынке долговых финансовых инструментов обращаются временно свободные финансовые ресурсы, т.е. предприятия получают денежные средства на определенный период времени, по истечении которого они подлежат возврату. Долговой финансовый рынок представлен рынком облигаций и векселей.

4.3. Фондовые индексы

Фондовые индексы призваны помочь определить в какой фазе (роста или падения) сейчас находится рынок.

Индекс Доу-Джонс (DJI)

Существует 4 индекса Доу-Джонса.

Промышленный индекс Доу-Джонса (TheDowJonesIndustrialAverage- **DJIA**) - простой средний показатель движения курсов акций 30 крупнейших промышленных корпораций. Промышленный индекс Доу-Джонса является самым старым и самым распространенным среди всех показателей фондового рынка. Его состав не является неизменным: компоненты его могут изменяться в зависимости от позиций крупнейших промышленных корпораций в экономике США и на рынке, однако в современных условиях такие случаи довольно редки. В принципе на его составляющие приходится от 15 до 20% рыночной стоимости акций, котируемых на Нью-йоркской фондовой бирже. Этот индекс начисляется путем сложения цен включенных в него акций и деления полученной суммы на определенный деноминатор (который корректируется на величину дробления акций и дивидендов в форме акций, составляющих свыше 10% рыночной стоимости выпусков, а также на замещение компонентов и слияния и поглощения). Индекс Доу-Джонса котируется в пунктах. С недавнего времени на него появились фьючерсные контракты в Чикаго.

Транспортный индекс Доу-Джонса (TheDowJonesTransportationAverage - **DJTA**) - средний показатель, характеризующий движение цен на акции 20 транспортных корпораций (авиакомпаний, железнодорожных и автодорожных компаний).

Коммунальный индекс Доу-Джонса (TheDowJonesUtilityAverage - **DJUA**) - средний показатель движения курсов акций 15 компаний, занимающихся газа - и электроснабжением.

Составной индекс Доу-Джонса (TheDowJonesCompositeAverage - **DJCA**) - показатель, состоящий на базе промышленного, транспортного и коммунального индексов Доу-Джонса.

Индекс "Стэндард энд пауэрз" (S&P)

Этот индекс публикуется независимой компанией "Стэндард энд пауэрз". Он составляется в двух вариантах - по акциям 500 корпораций и по акциям 100 корпораций.

S&P - 500 представляет собой взвешенный по рыночной стоимости индекс акций 500 корпораций, которые представлены в нем в следующей пропорции: 400 промышленных корпораций, 20 транспортных, 40 финансовых и 40 коммунальных компаний. В него включены в основном акции компаний, зарегистрированных на Нью-йоркской фондовой бирже, однако присутствуют также акции некоторых корпораций, которые котируются на Американской фондовой бирже и во внебиржевом обороте. Индекс представляет около 80% рыночной стоимости всех выпусков, котируемых на Нью-йоркской фондовой бирже. Этот индекс более сложный по сравнению с индексом Доу-Джонса, но он считается также более точным в силу того, что в нем представлены акции большего числа корпораций и акции каждой корпорации взвешиваются на величину стоимости всех акций, находящихся в руках акционеров. Фьючерсы и опционы по нему продаются на Чикагской товарной бирже.

S&P - 100. Индекс исчисляется на той же основе, что и индекс по акциям 500 корпораций, но состоит из акций корпораций, по которым существует зарегистрированные опционы на Чикагской бирже опционов. В основном это промышленные корпорации.

Индекс Нью-Йоркской фондовой биржи (NYSE Index)

Данный индекс представляет собой взвешенный по рыночной стоимости показатель движения курсов акций всех корпораций, зарегистрировавших свои бумаги на Нью-йоркской фондовой бирже, то есть, по сути, это показатель представляет собой среднюю цену на акцию по всем компаниям на Нью-йоркской фондовой бирже, взвешенный по рыночной стоимости акций каждой корпорации (с соответствующими корректировками по факторам дробления акций, слияний и поглощений). В отличие от индекса Доу-Джонса, который выражается в пунктах, индекс NYSE выражается в долларах. Операции с опционами по этому индексу осуществляются на самой Нью-йоркской фондовой бирже. Операции с фьючерсными контрактами осуществляются на Нью-йоркской бирже фьючерсов, которая является подразделением Нью-йоркской фондовой биржи.

Индексы Американской фондовой биржи (AMEX)

Американская фондовая биржа публикует два основных индекса, которые исчисляются на совершенно разной основе.

Основной рыночный индекс Американской фондовой биржи (AMEX MajorMarketIndex) является простым средним показателем движения цен 20 ведущих промышленных корпораций. Он был задуман Американской

фондовой биржей в качестве своеобразного субститута промышленного индекса Доу-Джонса. Хотя он рассчитывается и публикуется Американской фондовой биржей, в его состав входят акции корпораций, зарегистрированных на Нью-йоркской фондовой бирже. Примечательно, что 15 из них являются также компонентами промышленного индекса Доу-Джонса. Операции с фьючерсами по этому индексу осуществляются на Чикагской торговой бирже.

Индекс рыночной стоимости Американской фондовой биржи (AMEX MarketValueIndex) исчисляется на принципиально иной основе: он является показателем, взвешенным по рыночной стоимости всех выпущенных акций тех корпораций, которые включены в него в качестве компонентов. Впервые он был опубликован в сентябре 1973 года. Он включает в себя в качестве компонентов более 800 выпусков акций, представляющих ценные бумаги корпораций всех крупных отраслевых групп, зарегистрированных на Американской фондовой бирже, включая, помимо обыкновенных акций, американские депозитные свидетельства и подписные сертификаты. С технической точки зрения он является уникальным в силу того, что при его расчете предполагается, что дивиденды в форме наличных, выплачиваемые по входящим в его состав акциям, реинвестируются, и на этой основе они отражаются в индексе. Опционы по этому индексу котируются на Американской фондовой бирже.

Индекс внебиржевого оборота (NASDAQ)

Национальная ассоциация фондовых дилеров исчисляет целый ряд индексов, представляющих как внебиржевой оборот в целом, так и бумаги корпораций отдельных отраслей. Основным является индекс NASDAQ, в который включены в качестве компонентов акции около 3500 корпораций (кроме котируемых на биржах). Этот индекс является показателем, взвешенным по рыночной стоимости его составляющих. Впервые он был рассчитан в феврале 1971 года.

Операции с опционами и фьючерсами по этому индексу осуществляются на Чикагской товарной бирже.

Падение фондовых индексов приводит к падению национальной валюты

4.4. Белорусская валютно-фондовая биржа

Открытое акционерное общество «Белорусская валютно-фондовая биржа» было образовано в 1998 году во исполнение Указа Президента Республики Беларусь от 20 июля 1998 г. № 366 «О совершенствовании системы государственного регулирования рынка ценных бумаг». Учредителями биржи стали Национальный банк Республики Беларусь (контрольный пакет акций),

Фонд государственного имущества Министерства экономики Республики Беларусь и ряд крупных банков Республики Беларусь.

Высшим органом управления ОАО «Белорусская валютно-фондовая биржа» является Общее собрание акционеров. В состав акционеров биржи, кроме учредителей входят банки, брокерско-дилерские компании республики и др. Руководство деятельностью биржи в период между Общим собранием акционеров осуществляется Наблюдательным советом.

На сегодняшний день ОАО «Белорусская валютно-фондовая биржа» – единственная в республике торговая площадка, на основе которой создана общенациональная система биржевых торгов на всех основных сегментах финансового рынка: валютном, фондовом и срочном. Кроме организации торгов, биржа выполняет функции расчетного депозитария на биржевом рынке негосударственных ценных бумаг, функции оператора расчетно-клиринговой системы по всем видам ценных бумаг и инструментам срочного рынка, а также осуществляет регистрацию сделок, заключенных на внебиржевом рынке с акциями открытых акционерных обществ и ИПЧ «Жилье».

Валютный рынок

В соответствии с Правилами биржевой торговли иностранными валютами, утвержденными постановлением Правления Национального банка Республики Беларусь 28.06.2001 № 165 (в ред. от 31.10.2003), ОАО «Белорусская валютно-фондовая биржа» наделена правом организации торгов иностранной валютой.

Торги иностранной валютой на бирже осуществляются в рамках Секции валютного рынка. Биржевые торги проводятся ежедневно с использованием электронной системы торгов. Основными котируемыми на бирже валютами являются: Доллар США, Евро, Российский рубль и Украинская гривна. Курсы, сформированные по итогам биржевых торгов, сегодня входят в разряд основных индикаторов валютного рынка. По итогам торгов Национальный банк Республики Беларусь устанавливает официальные курсы белорусского рубля по отношению к доллару США и рублю Российской Федерации.

Рынок ценных бумаг

В соответствии с законодательством Республики Беларусь для многих ценных бумаг биржа является единственным допустимым местом заключения сделок. К таким бумагам относятся: государственные эмиссионные ценные бумаги, облигации Национального банка Республики Беларусь, облигации местных займов и ценные бумаги открытых акционерных обществ, прошедшие оценку качества и надежности (листинг) и допущенные к обращению на бирже.

К участию в торгах ценными бумагами допускаются только члены Секции фондового рынка. Сделки с ценными бумагами совершаются в универсальной электронной торговой системе. Членам Секции фондового рынка предоставляется возможность участвовать в торгах с использованием автоматизированных рабочих мест, расположенных в торговых залах биржи, или через удаленные торговые терминалы. Торги ценными бумагами проводятся ежедневно в следующих режимах: «Непрерывный двойной аукцион», «РЕПО (фиксированное ценообразование)», «РЕПО (свободное ценообразование)», «Дискретный аукцион», «Форвардные сделки», «Простой аукцион», «Простой аукцион РЕПО». Данные режимы эффективно используются для первичного размещения ценных бумаг, организации их вторичного обращения и обеспечения процессов приватизации.

В секторе негосударственных ценных бумаг совершаются сделки с акциями и облигациями субъектов хозяйствования при первичном размещении и вторичном обращении, а также приватизационные сделки. Фонд государственного имущества Министерства экономики Республики Беларусь использует биржевые технологии для организации аукционов по продаже принадлежащих государству акций за иностранную валюту и белорусские рубли, осуществляет реализацию госпакетов акций в режиме «дискретный аукцион» и других доступных режимах торгов.

Участники торгов могут совершать сделки с негосударственными ценными бумагами со следующими условиями расчетов: T+0 (поставка денег и ценных бумаг в день совершения сделки), T+n (поставка денег и бумаг в день, определенный участниками в момент совершения сделки), а также сделки, совершаемые на условиях РЕПО.

В соответствии с законодательством Республики Беларусь биржа осуществляет обязательную регистрацию всех совершенных на внебиржевом рынке сделок с ценными бумагами открытых акционерных обществ, а также начиная с 25 января 2005 года сделок с именными приватизационными чеками «Жилье».

Срочный рынок

Начиная с октября 2004 года биржа приступила к проведению торгов финансовыми инструментами срочного рынка на постоянной основе. Биржевые торги инструментами срочного рынка проводятся в электронной торговой системе каждый рабочий день одновременно по всем инструментам в режиме «непрерывный двойной аукцион». Участниками торгов выступают члены Секции срочного рынка. Расчеты по совершаемым сделкам проводятся в единой расчетно-клиринговой системе, в которой функции расчетного банка выполняет Национальный банк Республики Беларусь, а функции клиринга – биржа.

Инструментарий данного рынка представлен фьючерсными контрактами на курсы иностранных валют и процентные ставки на рынке государственных ценных бумаг.

Фьючерсная сделка - сделка, которая заключается не с целью купли-продажи товара, а с целью страхования (хеджирования) сделок с наличным товаром и получения в ходе его перепродажи разницы от возможного колебания цен в будущем.

Фьючерсный контракт - торговые соглашения, где объектом сделок является не товар, а биржевой контракт на товары.

Опционная сделка (или сделка с премией) - сделка при которой уплата противоположной стороне известной премии дает право купить или продать товар по установленной при заключении сделки цене в любой день в течение определенного периода, либо вообще отказаться от сделки без возмещения убытков. Если право оказалось невостребованным покупателем, то сделки прекращаются.

Опционный контракт - это двухсторонний договор о передачи права на покупку или продажу определенного базисного актива по определенной цене в определенное время. В контракте принимают участие покупатель, имеющий право на покупку или продажу актива, и продавец, предоставивший право поставить или принять актив по требованию покупателя. За полученное право покупатель опциона уплачивает продавцу некоторое вознаграждение, называемое премией.

БЕКАС - информационно-котировочная система, функционирующая на базе Интернет-технологий, предназначенная для поиска контрагента для совершения сделок с различными видами ценных бумаг, а также обслуживающая процессы обязательной регистрации на неорганизованном рынке сделок с акциями открытых акционерных обществ и именных приватизационных чеков «Жилье», совершенных на внебиржевом рынке. На сегодняшний день система является единственным в республике полноценным источником информации о состоянии внебиржевого рынка акций белорусских предприятий.

Кроме этого, биржа выступает поставщиком информации для республиканских информационных агентств, а также ведущих СМИ, ориентированных на освещение мировых экономических процессов.

4.5. FOREX

FOREX(ForeignExchangeMarket) – глобальный валютный рынок по обмену определенной суммы валюты одной страны на валюту другой по

согласованному курсу на определенную дату. FOREX не имеет какого-либо определенного места торговли. Это огромная сеть, соединенных между собой посредством телекоммуникаций валютных дилеров, сосредоточенных по всем ведущим мировым финансовым центрам и круглосуточно работающим как единый механизм. Основными участниками валютного рынка являются: коммерческие банки, валютные биржи, центральные банки, фирмы, осуществляющие внешнеторговые операции, инвестиционные фонды, брокерские компании, частные лица. Т.е. практически весь финансовый рынок.

Главными валютами, на долю которых приходится основной объем всех операций на рынке FOREX, являются сегодня доллар США (USD), евро (EUR), японская йена (JPY), швейцарский франк (CHF) и английский фунт стерлингов (GBP). Ежедневный объем конверсионных операций в мире составляет около 2-4 триллионов долларов США. На Лондонский рынок приходилось порядка 30% оборота, на долю рынков США - 20%, Германии - 10%. Операции с участием доллара США составляют 70%. На долю электронных брокеров сегодня приходится 15% оборота рынка FOREX.

Типичные объемы сделок в межбанковской торговле составляют 10 миллионов долларов, но благодаря системе маржевой торговли, выход на рынок доступен и лицам, располагающим небольшим капиталом. Брокеры, предоставляющие услуги маржевой торговли, требуют внесения залогового депозита и дают возможность клиенту совершать операции купли-продажи валют на суммы, в 100 раз большие, чем внесенный депозит. Риск потерь возлагается на клиента, депозит служит обеспечением, страхующим брокера.

ТЕМА 5: АВТОМАТИЗАЦИЯ РЫНКА ЦЕННЫХ БУМАГ

5.1 Место рынка ценных бумаг в финансово-кредитной структуре республики Беларусь. Задачи рынка ценных бумаг.

Рассмотрим основные термины и определения, которые необходимо нам знать в данной теме.

Депозитарная деятельность - оказание услуг по хранению сертификатов ценных бумаг и/или учету и переходу прав на ценные бумаги.

Депозитарий — юридическое лицо, которое занимается депозитарной деятельностью.

Счет «ДЕПО» - Государственные облигации имеют бездокументарную форму и представлены в виде записей на специальном счете по учету приобретенных и проданных ценных бумаг — счет «ДЕПО».

Сделки «РЕПО» — это сделки купли-продажи ГКО/ГДО, заключаемые на определенный срок с обязательством:

- для покупателя — последующей продажи (обратная продажа);
- для продавца — последующего выкупа (обратный выкуп).

Инфраструктуру любого рынка ценных бумаг можно представить в виде четырех основных составляющих.

- **Торговая организация (Биржа).** Организация, устанавливающая правила и осуществляющая торговлю ценными бумагами в соответствии с действующим законодательством и нормативными актами.
- **Клиринговая организация.** Организация, осуществляющая клиринг по всем сделкам, совершенным участниками торгов через организатора торговли.
- **Расчетный депозитарий.** Депозитарий, осуществляющий проведение всех операций по счетам депо участников рынка ценных бумаг при исполнении сделок, совершенных через организаторов торговли на рынке ценных бумаг.
- **Расчетная организация.** Организация, ведущая счета участников клиринга и осуществляющая расчеты по денежным средствам по результатам клиринга на основании поручений и (или) иных документов.

Клиринговая организация выполняет следующие функции:

- определение обязательств участников клиринга по итогам сделок клирингового пула;
- учет обязательств каждого участника клиринга;
- формирование и передача в расчетный депозитарий и расчетную организацию документов на проведение операций по счетам участников сделок;
- осуществление контроля над исполнением в расчетной организации и расчетном депозитарии операций по обязательствам участников;
- формирование отчетов по результатам клиринга по каждому участнику (в разрезе участников);
- архивное хранение информации о сделках в течение определенного времени;
- создание гарантийного фонда и разработка системы мер снижения рисков клиринговой деятельности.

Модель РЦБ РБ показана на рисунке 1.

Задачи рынка ценных бумаг:

- учет и хранения ценных бумаг;
- первичное размещение (аукцион) ценных бумаг;
- обращение (купля/продажа) ценных бумаг;
- расчеты по сделкам с ценными бумагами;
- информационная поддержка участников (сайт БВФБ – итоги торгов, аукционов, котировка ЦБ «БЕКАС»).

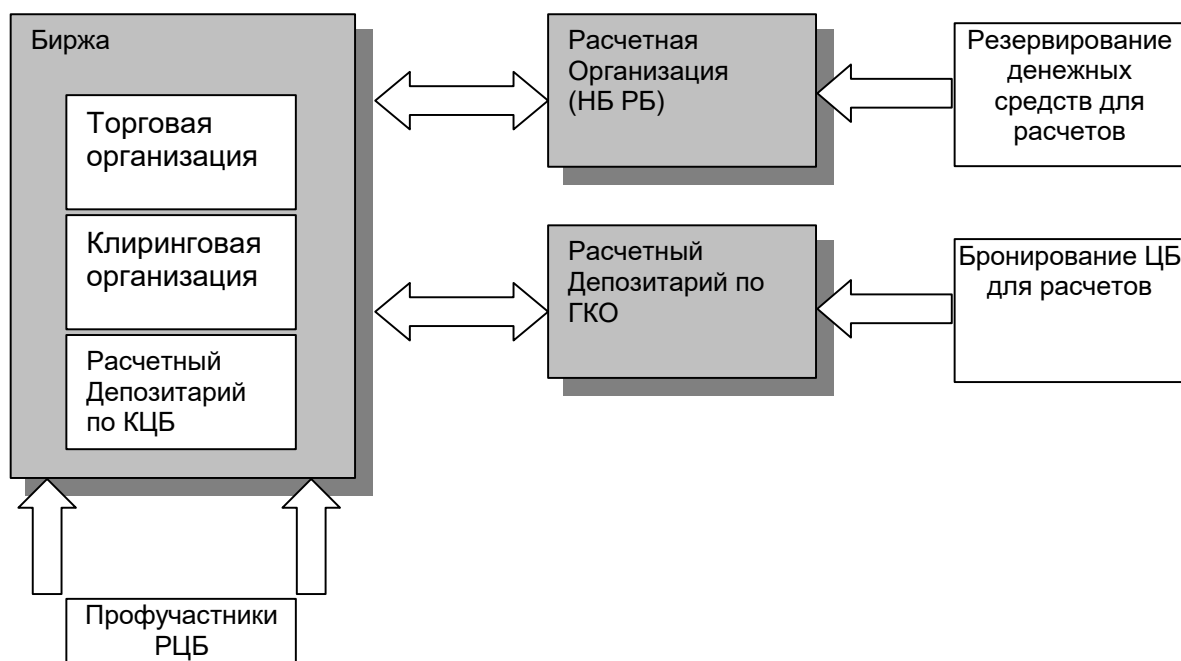


Рисунок 1. – Модель РЦБ РБ

5.2 Процесс эмиссии акций предприятия

Решение о выпуске акций принимается учредительной конференцией или общим собранием акционеров. Производится подписка на акции. - этап учреждения акционерного общества. Если подписка не покрывает определенной в уставе величины уставного фонда, то АО считается несостоявшимся.

Издается проспект эмиссии, который содержит сведения о предприятии (название, адрес, цель использования фин. ресурсов)

Акции выпускаются при создании акционерного общества либо при увеличении его уставного фонда. Выпуск акций создаваемым открытым акционерным обществом включает в себя проведение открытой подписки, регистрацию акций и их фактическое размещение на условиях и по итогам подписки. Порядок проведения открытой подписки на акции создаваемого открытого акционерного общества определяется законодательством.

Решение о выпуске акций должно содержать сведения, определяемые центральным органом, осуществляющим контроль и надзор за рынком ценных бумаг.

Акции выпускаются в размере оплаченного уставного фонда создаваемого акционерного общества и размещаются среди инвесторов на условиях и по итогам подписки.

Дополнительный выпуск акций, осуществляемый в связи с увеличением уставного фонда путем подписки, возможен только после полной оплаты акций и их государственной регистрации. Решение о дополнительном выпуске акций принимается общим собранием акционеров по окончании подписки.

Размещение дополнительного выпуска акций открытого акционерного общества возможно в форме распределения между участниками общества открытой продажи либо по итогам подписки.

Подписка на акции либо их продажа первому владельцу по цене ниже номинальной стоимости не допускается. При этом номинальная стоимость акций должна быть выражена только в национальной денежной единице. Открытая продажа дополнительного выпуска осуществляется на основе договора купли-продажи путем внесения инвестором вклада на расчетный счет эмитента в учреждении банка. Инвестор приобретает право владельца на акции после их полной оплаты, а на их отчуждение -- в порядке, предусмотренном законодательством.

5.3 Структура рынка ценных бумаг. Торговые автоматизированные системы.

Рынок ценных бумаг включает сегменты:

- ГКО
- ГДО
- КЦБ
- векселя
- инструменты срочных сделок

Каждый сегмент отличается своим регламентом и технологией.

Аукционы, сделки купли-продажи ЦБ проводятся в автоматизированной торговой системе БВФБ.

Автоматизированная торговая система включает торговую систему и расчетную систему.

Торговая система – автоматизированное рабочее место администратора (руководителя торгов), автоматизированное рабочее место трейдера (участника торгов) и ядро системы.

Основные функции торговой АС:

- ведение торговых счетов профучастников (по денежным средствам и ЦБ);
- прием, контроль и регистрация заявок на покупку-продажу ЦБ и сделок с ними;
- проведение биржевых торгов по купле-продаже ЦБ;
- определение цены по сделкам;
- контроль и регистрация сделок купли-продажи ЦБ;
- представление расчетных документов в расчетно-клиринговую службу БВФБ;
- заключение и регистрация внесистемных сделок.

Расчетная система (ПТК расчетно-клиринговой службы).

До начала торговой сессии – получает на счет Биржи денежные средства для использования во время предстоящей торговой сессии.

По окончании торговой сессии – по результатам заключенных сделок с облигациями производит взаимозачет требований и обязательств участников по денежным средствам.

Перед торговой сессией – получает на счет ДЕПО Биржи в ЦД ЦБ для использования во время предстоящей торговой сессии.

По окончании торговой сессии – по результатам заключенных в торговой системе сделок с ЦБ производит взаимозачет требований и обязательств участников по ЦБ.

5.4 Расчетно-клиринговая система, как инструмент клиринга и расчетов по итогам торгов и аукционов ценных бумаг. Автоматизированные системы РКС ЦБ и их взаимодействие.

Расчетно-клиринговая система по ценным бумагам Республики Беларусь предназначена для реализации автоматизированного процесса клиринга и расчета сделок с ценными бумагами.

Основные принципы:

- поставка против платежа;
- минимизация расчетных рисков (резервирование денег и бронирование ЦБ);

Процесс клиринга и расчета сделок с ценными бумагами состоит из нескольких этапов:

- подтверждение условий сделки прямыми участниками рынка;
- расчет обязательств сторон, вытекающих из подтвержденных условий сделки, известный как клиринг;
- окончательная передача ценных бумаг (поставка) в обмен на окончательный перевод средств (платеж) для расчета обязательств.

Подтверждение условий сделки осуществляется в АС торговой системы.

Клиринг и окончательная передача ценных бумаг (поставка) в обмен на окончательный перевод средств (платеж) для расчета обязательств осуществляется РКС ЦБ.

Расчетно-клиринговая система по ценным бумагам Республики Беларусь (далее – РКС ЦБ) не является как таковой автоматизированной системой, а представляет собой совокупность самостоятельных автоматизированных систем и подсистем, взаимодействующих в целях реализации части технологических процессов рынка ценных бумаг.

Взаимодействующие системы и подсистемы:

- программный комплекс расчетно-клиринговой службы автоматизированной системы «Биржа» БВФБ (далее – ПК РКС «Биржа»);
- автоматизированная банковская система «Учетно-операционные работы» Национального банка Республики Беларусь (далее – АБС «УОР»);
- система междепозитарных переводов Центрального депозитария Национального банка Республики Беларусь «Депо – Центр» (далее – система «Депо – Центр») и Расчетного депозитария БВФБ;
- система валовых расчетов в режиме реального времени (далее – система BISS);
- программный комплекс «Управление расчетами в АС МБР» Национального банка Республики Беларусь (далее – ПК «Управление расчетами в АС МБР»);
- программные комплексы участников расчетов в РКС ЦБ (банков, уполномоченных депозитариев), осуществляющих формирование, передачу, прием и обработку файлов и сообщений с информацией для расчетов по ценным бумагам (далее – ПК участников расчетов).

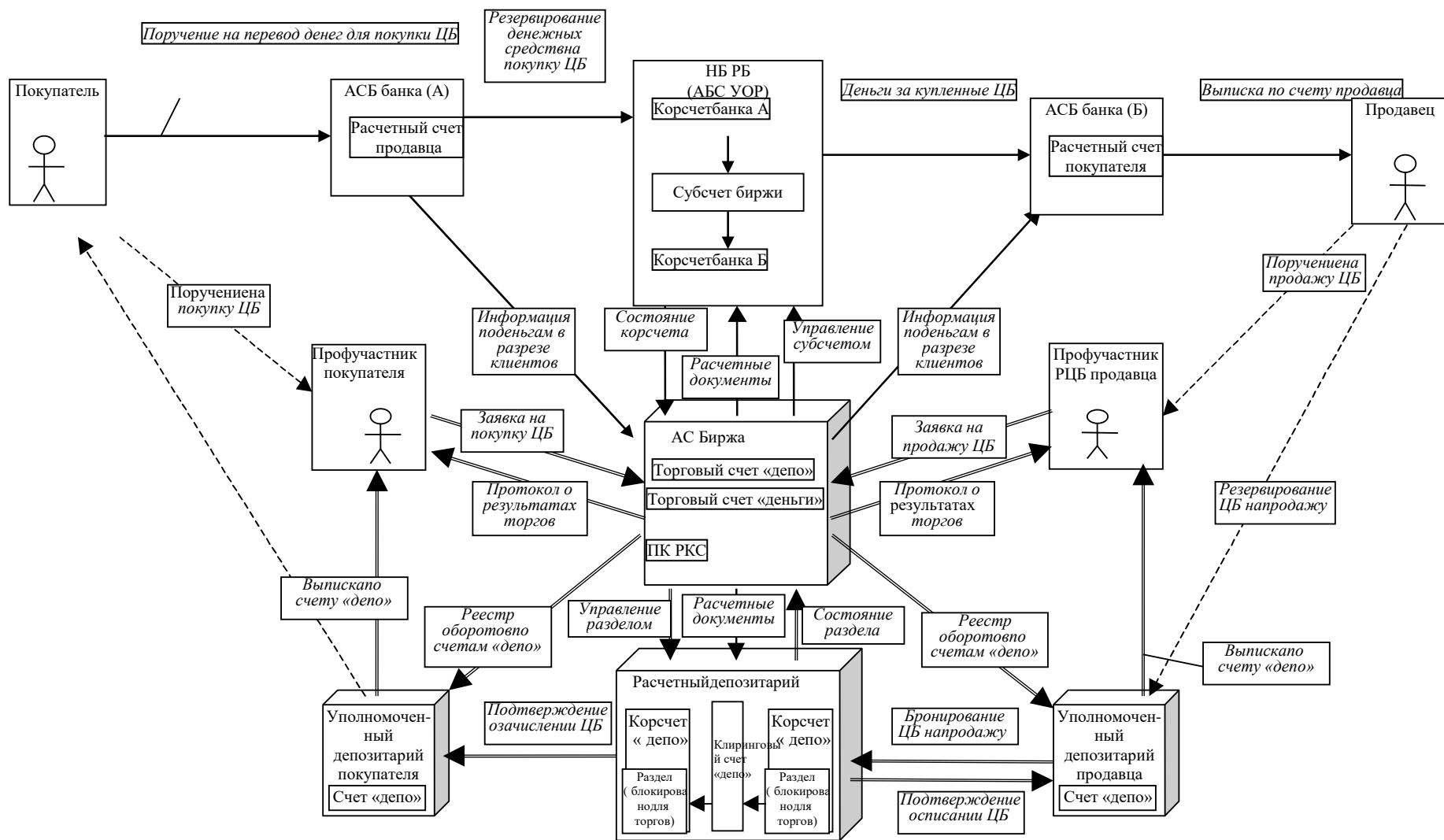


Рисунок 3 – Взаимодействие компонент инфраструктуры рынка ценных бумаг

ТЕМА 6: ПЛАТЁЖНЫЕ СИСТЕМЫ. КЛЮЧЕВЫЕ ПРИНЦИПЫ ПОСТРОЕНИЯ ПС

6.1. Общие положения

Платежная система – это совокупность банковских и финансовых институтов, платежных инструментов, банковских правил и процедур, а также межбанковских систем перевода денежных средств, обеспечивающих обращение денежных средств внутри страны и взаимодействие с зарубежными платежными системами.

Платежные инструменты, используемые при безналичных расчетах в Республике Беларусь:

- платежные поручения
- платежные требования
- чеки
- требования-поручения
- аккредитивы
- банковские пластиковые карточки

Что входит в понятие «платёжная система»?

Проектные решения платежных систем в различных странах мира различаются в значительной степени. Определяющими элементами платежной системы является «совокупность инструментов, банковских процедур и, как правило, межбанковские системы переводов средств, обеспечивающие обращение денежных средств». В центре внимания находится система перевода средств, то есть ядро платежной системы. Это, как правило, связано с соглашением между определенной группой участников системы и системным оператором, в котором определяются правила и процедуры, касающиеся перевода средств между участниками. Участники могут быть прямыми или косвенными. Банк международных расчетов (далее БМР) признается, что главным назначением платежных систем является обслуживание экономики, но их специфическое предназначение означает, что они не связаны непосредственно с правами и обязанностями каких-либо иных сторон, кроме системных операторов, участников систем и центральных банков. Так, например, при обсуждении правовой основы окончательности расчета, в центре внимания находится расчет между участниками систем.

Платежные системы находятся в сердце финансового сектора. Вместе с быстрыми технологическими переменами на национальном и международном уровнях, а также конкуренцией в этой области, государственная политика должна постоянно уделять внимание поддержке безопасности и эффективности платежных систем обоих уровней.

6.2. Определение системно значимых платежных систем

Важнейшим шагом в применении Ключевых принципов является разграничение платежных систем, являющихся системно значимыми, от иных. В стране может быть несколько платежных систем, которые являются важными для пользователей и для непрерывной и эффективной работы экономики в целом. Отличительной чертой системно значимой платежной системы является то, что она способна вызывать или передавать потрясения (шоки) в собственной или даже международной финансовой системе. Большинство стран имеют по крайней мере одну такую систему.

Главным фактором при оценке потенциальной возможности платежной системы вызвать или спровоцировать системные сбои является сумма обрабатываемых системой платежей в совокупном или индивидуальном выражении, по отношению к ресурсам участников системы и в контексте всей финансовой системы в целом.

Еще одним фактором при определении системной значимости системы является характер обрабатываемых платежей. Система, предназначенная для расчетов по иным платежным системам (например, если в ней обрабатываются платежи чистых сумм для расчетов по многосторонней неттинговой расчетной системе) или система для обработки платежей для расчета по транзакциям финансового рынка (например, транзакций на денежных рынках или рынках валют, или по переводам денег для операций на рынке ценных бумаг) обычно рассматривается как системно значимая платежная система.

Считается, что система является системно значимой, если к ней применимо хотя бы одно из следующих условий:

- она является единственной платежной системой в стране или главной системой с учетом совокупной величины платежей;
- в ней обрабатываются в основном крупные платежи;
- она используется для расчета транзакций финансового рынка или для расчета иных платежных систем.

Ключевые принципы предназначены для внедрения во всех странах в разумные временные сроки, независимо от того, является ли их экономика развитой, переходной или развивающейся. Конкретное применение Ключевых принципов зависит от экономического уровня развития страны, от институциональной структуры экономики и инфраструктуры в целом. При этом Ключевые принципы могут быть полезными при первоначальной оценке платежных систем, при постоянном контроле за их безопасностью и эффективностью, а также при разработке проектов модернизации.

Ключевой принцип I – Система должна иметь хорошо проработанную правовую базу во всех соответствующих юрисдикциях

Ключевой принцип II – Правила и процедуры системы должны давать участникам четкое представление о влиянии системы на каждый из финансовых рисков, которые они несут в силу их участия в системе.

Ключевой принцип III – Система должна иметь четко определенные процедуры управления кредитными рисками и рисками ликвидности, устанавливающие ответственность оператора системы и участников, а также содержащие надлежащие стимулы для управления этими рисками и их сдерживания.

Ключевой принцип IV – Система должна обеспечивать быстрый окончательный расчет в день валютирования, предпочтительно в течение дня или, как минимум, на конец дня.

Ключевой принцип V – Система, в которой осуществляется многосторонний неттинг, должна быть, как минимум, в состоянии обеспечить своевременное завершение ежедневных расчетов в случае неспособности участника произвести расчет по самому крупному расчетному обязательству.

Ключевой принцип VI – Средства, используемые для расчета, должны быть предпочтительно в форме требований к центральному банку; если используются иные средства, они должны иметь незначительный или нулевой кредитный риск или риск ликвидности.

Ключевой принцип VII – Система должна обеспечивать высокую степень безопасности и операционной надежности, а также должна иметь запасные процедуры для нештатных ситуаций, позволяющих своевременно завершить обработку данных за день.

Ключевой принцип VIII – Система должна предлагать такие средства для проведения платежей, которые являются практичными для пользователей и эффективными для экономики.

Ключевой принцип IX – Система должна иметь объективные и публично объявленные критерии для участия, обеспечивающие справедливый и открытый доступ.

Ключевой принцип X – Процедуры управления (руководства) системой должны быть эффективными, подотчетными и прозрачными.

Для обеспечения точности и целостности транзакций, система должна использовать целесообразные с экономической точки зрения стандарты безопасности. Стандарты, относящиеся к использованию информации, должны анализироваться на их соответствие имеющейся на данный момент технологии. Для завершения дневного цикла обработки, система должна поддерживать высокую степень операционной гибкости. Это вопрос не только наличия надежной технологии и резервирования всего программно-технического и сетевого комплекса. Кроме этого, необходимо иметь в наличии эффективные производственные процедуры и хорошо обученный и компетентный персонал, который умеет надежно и эффективно эксплуатировать систему и обеспечивать

исполнение всех процедур. Степень надежности зависит также от наличия альтернативных механизмов проведения платежей в чрезвычайных ситуациях.

Критерии оценки

В системе должны быть решены следующие вопросы.

Разработчики и операторы платежных систем должны рассмотреть следующие вопросы в отношении безопасности и операционной надежности системы:

Общие вопросы

а) Система должна отвечать принципам безопасности и уровням качества операционных услуг, согласованным между системным оператором и участниками, а также соответствующим правовым нормам, системным правилам, процедурам управления риском, производственным требованиям и международным, национальным или отраслевым стандартам.

б) Безопасность системы и операционная надежность зависят как от центральной системы, так и от системных компонентов участников; участники также несут ответственность за безопасность и операционную надежность. Система должна осуществлять официальный контроль над соблюдением соответствующего уровня качества услуг.

с) Принципы безопасности и уровни качества операционных услуг со временем должны изменяться в соответствии с развитием рынка и технологий; система должна проектироваться и работать в соответствии с этими изменениями.

д) Система требует адекватного числа хорошо обученных, компетентных и надежных сотрудников для безотказной и эффективной эксплуатации системы в нормальных и чрезвычайных ситуациях.

Безопасность

е) Задачи и политика безопасности должны определяться во время проектирования системы и периодически пересматриваться. Они должны подходить системе, учитывать ее конкретную архитектуру и форму собственности.

ф) Безопасность системы должна соответствовать экономически разумным стандартам, например, стандартам конфиденциальности, целостности, аутентификации, безотказности, операционной надежности, доступности и подконтрольности. Характеристики безопасности должны регулярно тестироваться.

г) Система должна регулярно подвергаться анализу на предмет рисков безопасности. Системный оператор должен постоянно следить за технологическим прогрессом и проводить анализ рисков безопасности системы на самом современном уровне.

Операционная надежность

h) Угрозы операционной надежности возникают не только при сбое центральной системы и компонентов участников, но также и при выходе из строя обслуживающей инфраструктуры и в случае природных катастроф.

i) В системе должны присутствовать всеобъемлющие, строгие и хорошо документированные операционные и технические процедуры.

j) Изменения в системе должны быть хорошо документированы, санкционированы, подконтрольны, протестированы и подвергнуты контролю качества.

k) Система должна быть спроектирована с достаточным запасом мощности, которая должна контролироваться и наращиваться в предвидении изменений производственных объемов.

Непрерывность производственного процесса

l) Системный оператор обязан осуществлять официальное планирование непрерывности производственного процесса. При разработке мероприятий для аварийных обстоятельств, следует учитывать принципы простоты и практичности.

m) Мероприятия по обеспечению непрерывности производственного процесса должны быть документированы и регулярно тестироваться. Они должны включать процедуры управления кризисными ситуациями и процедуры оповещения.

Мероприятия по обеспечению непрерывности производственного процесса могут включать в себя:

- перенос обработки платежей в другую платежную систему,
- создание второго центра обработки данных,
- введение режима «обслуживания на минимальном уровне».

Кроме этого, следует произвести оценку следующих аспектов:

Операционная надежность

n) Должны быть внедрены внутренние принципы и процедуры контроля, включая меры безопасности, предназначенные для ограничения операционного риска.

o) Все аспекты вычислительной системы должны быть документированы и обновлены. Следует иметь процедуру проведения аудита независимым специалистом по безопасности и возможность отслеживать обработку отдельной транзакции с начала до конца процесса.

p) Внутренний аудит должен проверять меры контроля операционного риска на регулярной основе.

q) Должен периодически проводиться внешний аудит систем информационных технологий.

Непрерывность производственного процесса

г) В случае выхода из строя основного вычислительного комплекса, следует иметь в наличии резервные средства.

с) В случае необходимости перехода на резервную систему следует иметь специальные процедуры сохранения всех данных по транзакциям. Резервная система должна находиться на достаточном расстоянии от места расположения главного центра обработки данных и использовать другие телекоммуникации и линии электропитания.

т) В случае выхода из строя основных систем, следует иметь планы действий в чрезвычайных ситуациях (включая план действий при природных катастрофах и план восстановительных мероприятий).

у) Отчеты о мониторинге производительности системы и о показателях качества должны составляться не реже раза в квартал. Системный оператор должен иметь план моделирования производительности важнейших систем, которые должны периодически тестироваться под пиковой нагрузкой.

в) Старший персонал, включая лиц, не несущих ответственность за соответствующие операции, должен регулярно изучать вопросы безопасности и высказывать свое мнение.

w) Система должна использовать отказоустойчивое или дублирующее оборудование и телекоммуникационные средства.

х) Документация процедур системы должна быть ясной и периодически обновляемой; она должна быть в наличии как на основном, так и резервном центрах. Следует иметь процедуры для копирования данных и ПО при их изменении. Следует также иметь процедуры обмена физическими данными на бумаге или дисках в ситуациях выхода из строя основных телекоммуникаций.

Пояснения и замечания

а) Полезной информацией для оценки операционной надежности системы является следующая:

- Сколько раз за прошлый год система давала сбои?
- Сколько времени потребовалось на восстановление обработки?
- Какими были масштабы потерь данных (транзакции и контролируемые служебные данные) и каким образом они были восстановлены?

б) Для оценки соответствия КП VII, эксперт должен провести беседы в центральном банке со специалистами департамента ИТ, аудиторами ИТ, специалистами платежных систем, органами надзора и системным оператором. Если центральный банк не является оператором и не производил оценку системы, такие беседы следует провести с частным оператором, его специалистами ИТ и аудиторами ИТ. Кроме этого, следует поговорить с произвольно выбранными участниками, особенно с их служащими, ответственными за вопросы ИТ.

с) Для управления безопасностью, операционными рисками и непрерывностью производственного процесса существуют разные способы, и приведенные выше критерии являются примерами таких механизмов. Для соответствия КП не обязательно соответствовать всем критериям оценки. Эксперт

должен проанализировать, достаточны ли средства, используемые системой для управления этими рисками, или необходимо предпринять дополнительные меры.

d) Взаимосвязь с другими Ключевыми принципами: Выбор принципов политики, используемых для решения вопросов безопасности и операционной надежности, должен производиться с учетом таких аспектов, как практичность и эффективность, рассматриваемых в КП VIII.

Системно значимая платежная система должна проектироваться и эксплуатироваться с высокой степенью безопасности и операционной надежности, что соответствует, учитывая ее особенность, ее назначению и требованиям пользователей. Специфические факторы могут значительно различаться в системах. Более того, технологический процесс в мире развивается очень быстро, меняя как характер требований пользователей, так и возможности их выполнения. В связи с этим в данном разделе говорится только в общем смысле о тех факторах, которые следует рассмотреть. Системно важная платежная система как правило, но не обязательно, является технически сложной, и именно этот случай рассматривается в данном разделе. Однако многие из этих учитываемых факторов распространяются и на иные аналогичные системные проектные решения.

■ Политические решения должны базироваться на рассмотрении вопросов безопасности и операционной надежности, а также практической целесообразности и эффективности, рассматриваемые в Ключевом принципе VIII. Этот выбор является как правило предметом консультаций между системным оператором и участниками, результат которых выливается в соглашение о принципах и уровнях услуг. Такое соглашение достигается как правило на высшем уровне руководства. Это делается для того, чтобы лица, разрабатывающие принципы и уровни услуг, были теми же лицами, кто несет ответственность за поддержку соответствующего равновесия между расходами на внедрение принципов и уровней услуг и выгодами, получаемыми от надежности системы и бесперебойного предоставления услуг. При проектировании системы и ее эксплуатации следует также проанализировать любые правовые ограничения, системные правила, процедуры управления риском и соответствующие операционные требования, имеющие отношение к безопасности и операционной надежности.

■ Операционная надежность системы зависит от операционной надежности всех ее компонентов (включая оборудование, ПО, телекоммуникационную сеть, энергоснабжение, служащих). Разработчики и операторы платежной системы обязаны заниматься вопросами безопасности и операционной надежности компонентов центральной системы, но также и компонентов систем участников (включая, если требуется, косвенных участников). Такое вмешательство может выходить за пределы первоначального интерфейса с системой и включать операции участников, которые могут оказать отрицательное воздействие на работу платежной системы. Вот почему участники системы несут ответственность за безопасность и операционную надежность всей платежной

системы в целом, что должно быть отражено во всех соответствующих правилах и контрактах.

■ Оператор платежной системы должен контролировать и определять, отвечает ли система принципам безопасности и операционным уровням услуг. Это должен быть постоянный и всеобъемлющий процесс с привлечением внутренних и/или внешних аудиторов. Сюда же входит мониторинг безопасности и операционной надежности участников, например, рабочая готовность их компонентов в течение обычных рабочих часов. Если участники создают излишний риск платежной системы или иных участников, системный оператор обязан, например, поставить в известность старших руководителей участника или, в особо серьезных случаях, предупредить системный надзор.

■ Система должна иметь соответствующее количество хорошо обученных, компетентных и надежных служащих. Они должны быть способны надежно и эффективно управлять системой и обеспечивать выполнение процедур операционного управления и управления риском в нормальных и чрезвычайных ситуациях. Некоторые служащие должны действовать как операционные администраторы и администраторы безопасности и иметь соответствующий уровень знаний, опыта и полномочий для выполнения своих задач. Обучение персонала должно включать углубленное понимание системы и ее назначения, чтобы операционные решения принимались на фоне имеющихся знаний. Персонал, ответственный за техническую поддержку всех компонентов системы, должен быть на рабочем месте по мере надобности (включая вне рабочих часов) для исправления ошибок и решения проблем.

■ Политика безопасности платежной системы и уровни операционных услуг со временем меняются в ответ на изменения на рынке платежных услуг (таких, как рост спроса и новые участники или клиенты), а также в ответ на технологические изменения, которые дают возможность осуществлять более надежную, быструю, эффективную или более эффективную с точки зрения цены обработку. Это проходит менее болезненно, если проектная разработка и эксплуатация системы обладают достаточной гибкостью, чтобы приспособиться к имеющимся изменениям.

■ Современные тенденции системного проектирования уделяют особое внимание безопасности и операционной надежности использования технологий «открытых систем» (часто называемых «интернет-технологиями» или «веб-технологиями»). Последние являются чрезвычайно популярными, поскольку они упрощают доступ и совместное использование данных и вычислительных ресурсов, однако их использование для системно значимых платежных систем ставит серьезные проблемы при создании соответствующей операционной целостности. Использование Интернета, в частности, поднимает особые вопросы, поскольку эта сеть не имеет четко определенного владельца или оператора, в связи с чем нет надежности (например, гарантии) качества услуг. В более общем плане, использование технологий открытых систем требует пристального внимания к возможным проникновениям или иным типам попыток нарушения защиты ресурсов со стороны киберов (например, проникновение в электронное хранилище, искажение базы данных, подделка кода или отмена услуги). При использовании таких технологий в системно значимых платежных системах

большую роль должен играть план мероприятий в аварийных ситуациях. Так, например, может потребоваться, чтобы система имела возможность реагировать на событие в масштабах всей системы, включая способность быстро и систематически привлекать соответствующие технические, производственные и человеческие ресурсы, а также юридическую базу. Кроме такого планирования чрезвычайных мероприятий, система могла бы, например, разработать собственные возможности для выявления и учета попыток нарушения защиты. Кроме этого, особое внимание должно быть уделено порядку использования коммерческого ПО, имеющегося в готовом виде, для системно значимых платежных систем, поскольку эти системы требуют высокого стандарта безопасности и операционной надежности.

Безопасность

- Цели и политика безопасности должны быть четко определены и документированы. Их конкретное содержание зависит от конкретной платежной системы, ее контекста и требований ее пользователей, но они должны быть достаточно строгими для оператора системы, участников, пользователей и органов надзора, чтобы обеспечивать доверие к системе. Цели и политика безопасности системно значимых платежных систем затрагивают системного оператора, участников и, возможно, клиентов с прямым доступом к системе или ее данным. Они должны устанавливаться в период проектирования системы и периодически пересматриваться, особенно, если в системе и ее компонентах происходят значительные изменения. Характеристики безопасности должны регулярно тестироваться.

- Цели и политика безопасности зависят от архитектуры системы и типа собственности на нее. Например, высоко централизованная система (в которой центральные компоненты, сеть и даже производственные комплексы участников принадлежат или эксплуатируются единым органом) могут иметь высоко централизованные цели и политику безопасности. С другой стороны, среда с распределенной обработкой (где системные компоненты могут иметь различных операторов и владельцев) требует, чтобы процесс обработки имел общие цели и принципы безопасности, четкое распределение ответственности за их внедрение, хорошую координацию участников, что позволит обеспечить логическое объединение общего операционного управления и контроль за системой.

- При выработке целей и политики безопасности следует учитывать экономически целесообразное соответствие стандартам, например, конфиденциальности, целостности, аутентификации, безотказности, операционной готовности и возможности аудиторского отслеживания операций. Они должны включать четкие принципы контроля как за физическим, так и логическим доступом к системе, ее оборудованию, ПО и сети для защиты системы и ее данных от несанкционированных действий как внутренних, так и внешних сторон. Вполне нормально строго ограничивать доступ к платежной

системе лишь теми лицами, кто имеет правомерное разрешение на доступ, и ограничивать его теми функциями, которые имеет данное лицо.

■Важная роль принадлежит проведению регулярного анализа риска безопасности с использованием признанных и структурированных методологий. Такой анализ должен, например, проводиться в период проектирования системы, а в последствие, когда меняется производственная среда или предлагается существенно изменить проектное решение системы; кроме этого, следует проводить периодический анализ (например, ежегодно) во время всего жизненного цикла системы. Со временем технологический прогресс может привести к росту угроз в системе, а также к появлению новых или усовершенствованию старых методов защиты и контроля. Системный оператор должен в связи с этим активно отслеживать технологические новшества, чтобы анализ риска безопасности системы всегда был на современном уровне. Типичные элементы анализа риска безопасности показаны в Комментарий 14.

Комментарий 14

Типичные элементы анализа риска безопасности

- Установить или пересмотреть цели и политику безопасности системы
- Определить функции системы, компоненты, границы и области ответственности
- Определить возможные угрозы и их масштаб (возможные воздействия и вероятность их возникновения)
- Определить существующие и потенциальные защитные средства (такие как физические устройства, ПО безопасности и организационные или операционные процедуры)
- Определить все остаточные риски и уязвимые места
- Повторять последние два шага до тех пор, пока остаточные риски и уязвимые места не будут находиться на приемлемом уровне с учетом целей и политики безопасности системы
- Внедрить в систему меры безопасности, определенные в ходе проведения анализа риска.

Операционная надежность

■Стандарты операционной надежности, необходимые для платежной системы, должны быть определены формально и документированы системным оператором и участниками как “соглашение об уровне услуг”. Уровни услуг могут отличаться, например, в зависимости от скорости расчета системы. В системе с расчетом в реальном времени на валовой основе уровни услуг могут определять максимальный период незапланированного «простоя», в то время как в системе с расчетом в конце дня они будут относиться к периоду расчета. Уровень требуемой операционной надежности также может зависеть от наличия

альтернативного механизма проведения платежей (такого, например, как иная платежная система) в случае серьезного сбоя системы или ее участников.

■Операционная надежность платежной системы связана не столько с компонентами центральной системы и участников, а с операционной надежностью инфраструктуры, от услуг которой она зависит, например, телекоммуникаций, энергоснабжения и транспорта (предоставляемых частным или государственным сектором). Угрозы прерывания услуг могут возникнуть не только из-за сбоя этих отдельных компонентов и услуг, но также и в связи с внешними событиями, например, происшествиями, затрагивающими всю отрасль, событиями общего плана, например, пожар, землетрясение или наводнение. Большое внимание в период проектирования системы следует уделить устранению ситуации, при которой выход из строя любого конкретного компонента системы приводит к выходу из строя всей системы («одна аварийная точка»). Все компоненты и угрозы должны быть учтены в мероприятиях по обеспечению непрерывности производственного процесса

■Системный оператор обязан разработать и внедрить в практику всеобъемлющие, строгие и хорошо документированные операционные и технические процедуры. Сюда должны войти процедуры по регистрации, отчетности и анализу всех операционных происшествий. После каждого значительного нарушения работы платежной системы оператор и, если требуется, участники должны предпринять «посмертное» расследование для выявления причин, а также провести модернизацию, требующуюся для нормальной работы или для обеспечения непрерывного производственного процесса.

■Любое значительное изменение системы и ее компонентов, включая компоненты, принадлежащие ее участникам, должны быть хорошо документированы, санкционированы, контролируемы, протестированы и подвергнуты процедурам приемки на качество соответствующими сторонами. Разработка и тестирование всех изменений должны проводиться без влияния на работу системы; этого можно достичь, используя для разработки иную систему, которая как можно точнее повторяет производственную и имеет те же уровни безопасности и контроля, что и производственная система. Если возможно, внедрение изменений должно проводиться так, чтобы внесенные изменения можно было при необходимости отменить, вернув систему в первоначальное состояние.

■Проектное решение системы должно обеспечивать наличие достаточной мощности для обработки предполагаемого объема платежей с требуемой скоростью, особенно в пиковое время и дни. Системный оператор должен регулярно контролировать и тестировать имеющуюся на данный момент мощность системы и ее производительность и тщательно планировать изменения объемов или производственную конфигурацию, чтобы поддерживать необходимые уровни пропускной способности и скорости прохождения платежей.

■Для платежной системы критичными считаются операционная надежность телекоммуникационных средств. Резервные или альтернативные телекоммуникационные средства и маршрутизация (например, использование коммутируемых телекоммуникационных линий как альтернативы выделенным линиям) могут сыграть здесь свою положительную роль. В большинстве случаев

платежная система зависит от одного или более поставщиков телекоммуникационных услуг, а также от надежности государственной телекоммуникационной инфраструктуры. По возможности оператор платежной системы должен в контрактах с телекоммуникационными компаниями определить требуемые уровни услуг и запасные маршруты, разработать аварийные планы.

Непрерывность производственного процесса

■Целью мероприятий по обеспечению непрерывности производственной деятельности является стремление обеспечить предоставление согласованных уровней услуг даже в ситуации, когда выходят из строя один или более компонентов системы. Оператор платежной системы, а если требуется, то и участники и провайдеры услуг инфраструктуры, должны предпринять совместные действия по созданию плана мероприятий по обеспечению непрерывности обслуживания в самых разнообразных возможных сценариях. Эти сценарии должны включать выход из строя центральных компонентов, компонентов участников и используемой инфраструктуры. Следует рассмотреть как внутренние, так и внешние угрозы, а также последствия каждого сбоя. Затем следует разработать мероприятия для предупреждения, смягчения и/или реагирования на каждый тип аварии. (Некоторые примеры мероприятий по обеспечению непрерывности производственного процесса приведены в Комментарий 15). Простота и практичность – ключевые моменты при проектировании резервных систем и процедур действий во внештатных ситуациях. Они должны активизироваться во время нештатных ситуаций и несмотря на обучение и тестирование, естественно, менее знакомы персоналу, который сталкивается лишь с повседневными операционными процедурами.

■Все аспекты мероприятий по обеспечению непрерывности производственного процесса должны быть четко и полно документированы. Сотрудники оператора платежной системы и участников должны получить надлежащее обучение и тренировку в их применении. Все элементы должны регулярно тестироваться с привлечением участников системы и иных сторон, кто будет привлечен к таким мероприятиям.

■Процедуры по быстрому формированию разносторонней группы для разрешения кризисных ситуаций являются важным элементом таких мероприятий, включая, если требуется, процедуры консультаций с участниками, органами надзора и иными заинтересованными сторонами. Мероприятия могли бы включать, например, процедуры по оперативному и регулярному информированию участников, их клиентов, иные финансовые службы, органы надзора и средства массовой информации об инцидентах и их влиянии на платежные услуги.

■Если мероприятия по обеспечению непрерывности производственного процесса включают переключение на обработку критически важных платежей в иную платежную систему, эта возможность должны быть оговорена, согласована и протестирована заранее с оператором этой системы, чтобы предупредить негативное влияние, которое может оказать поступление этих платежей на производительность резервной платежной системы.

■ Зачастую мероприятия по обеспечению непрерывности производственного процесса включают в себя создание запасного процессингового центра. Проектное решение такого центра должно учитывать время, необходимое для его запуска и для начала обработки платежей на новом месте. Что касается системы платежа в реальном времени на валовой основе, резервный центр должен содержаться в режиме «горячего резерва» с постоянным поступлением данных с основного центра, чтобы обработка могла возобновиться на новом месте в течение нескольких минут. Что касается системы с расчетом в конце дня, то время возобновления ее работы может быть более поздним (скорее определяемое в часах, а не в минутах). Второй процессинговый центр, как правило, проектируется с аналогичным ПО, оборудованием и телекоммуникациями, что и основной (для упрощения контроля, сопровождения и тестирования). Впрочем, идентичное ПО, вряд ли будет надежной защитой в случае сбоя ПО на основном центре. Место нахождения второго процессингового центра зависит от характера угроз, от которых он предназначен предохранять. Типичным здесь является защита от выхода из строя одной из инфраструктурных систем (например, электроснабжения или сети телекоммуникаций), оказывающей негативные последствия на основной и резервный центры. Системный оператор должен также принять решение о том, обязаны ли участники иметь резервный процессинговый центр; такая возможность может быть обеспечена двусторонним соглашением между участниками об использовании их процессинговых центров; можно также предусмотреть плановые аварийные меры использования центрального процессингового центра участником, имеющим серьезную аварию.

■ Мероприятия по обеспечению непрерывности производственного процесса платежной системы могут включать возможность использования при серьезном сбое «минимального уровня услуг» для обработки небольшого количества критичных платежей (например, относящихся к расчетам для другой платежной и расчетной системы, рыночной ликвидности или монетарной политике). Этот минимальный уровень услуг, может быть, достигнут, например, посредством ручной обработки документов на бумажном носителе, отправку аутентифицированных факсимильных сообщений или использование системы на базе ПЭВМ с применением физических носителей для передачи данных.

Комментарий 15

Примеры мероприятий для обеспечения непрерывности производственного процесса

- Использование отказоустойчивого или дублирующего оборудования.
- Регулярное профилактическое обслуживание всех вычислительных и телекоммуникационных комплексов.
- Наличие на месте запасных частей для оборудования и телекоммуникационных компонентов.
- Производство электроэнергии на месте или применение источников непрерывного питания, а также независимая подача воды.
- Системы обнаружения огня и противопожарные системы.

- Ведение простой и постоянно обновляемой процедурной и технической документации на основном и запасном центрах.
- Процедуры по копированию текущих данных, копированию ПО при его изменении, причем критичные его компоненты должны храниться вне основного центра.
- Процедуры обмена данными на основе физических носителей (дискеты, лента, бумага) в случае телекоммуникационных сбоев.
- Процедуры отключения некоторых системных функций или участников и запуска или остановки некоторых процессов, безотносительно их производственной последовательности.
- При введении нового компонента ПО, оборудования или телекоммуникаций, предусмотреть возможность сохранения в течение некоторого времени способности к возврату на прежнюю технологию.

ТЕМА 7: ПЛАТЕЖНАЯ СИСТЕМА РБ. АС МБР.

7.1. Исторический аспект

Денежная система Советского Союза к концу 1993 года прекратила свое существование. Все государства бывшего СССР, включая Республику Беларусь, начали создавать собственные денежные системы во главе с центральными (национальными) банками, образованными на базе учреждений Госбанка СССР. Национальный банк Республики Беларусь (далее – НБ РБ) был образован в 1991 г. С этого момента ведется работа по созданию двухуровневой банковской системы. С 1 июля 1992 г. в платежный оборот вводится белорусский рубль – национальная валюта, которая стала законным платежным средством.

Появление стремительно развивающейся сети коммерческих банков, прекращение функционирования системы учета Госбанка СССР, который гарантировал осуществление межбанковских расчетов, потребовало принятия неотложных мер по созданию эффективной платежной системы республики.

До 1993 г. межбанковские расчеты осуществлялись через счета банков и их филиалов в Главных управлениях НБ РБ по областям. Однако, увеличение сети филиалов не позволило банкам достаточно оперативно управлять своими ресурсами. В целях поддержания банками текущей ликвидности, обеспечения контроля со стороны НБ РБ за состоянием корреспондентских счетов банков с января 1993г. введен механизм осуществления межбанковских расчетов через единый корреспондентский счет банка, открытый в Национальном банке.

В мае 1995 г. введен единый расчетный час для межбанковских расчетов через государственное предприятие «Белорусский межбанковский расчетный центр» (сегодня – Расчетный Центр НБ РБ); БМРЦ также начал обеспечивать банки информацией в электронном виде о состоянии корреспондентского счета после каждого расчетного сеанса.

В 1995 г. Правлением НБ РБ утверждены требования к проекту развития и модернизации платежной системы. В основу этих требований положено осуществление межбанковских расчетов по крупным и срочным платежам на валовой основе в реальном режиме времени (на принципах RTGS), сокращение сроков документооборота, повышение сохранности и защищенности информации по платежам на всех стадиях ее обработки, более эффективное использование банками средств за счет получения ими информации о состоянии корреспондентских счетов в реальном режиме времени, безотзывность платежного сообщения и окончательность межбанковского расчета, дематериализация платежного оборота.

В качестве ядра национальной платежной системы проектом было предусмотрено создание автоматизированной системы межбанковских расчетов по крупным и срочным платежам (BISS), построенной на принципах расчетов на валовой основе в режиме реального времени (RTGS).

В платежной системе платежный поток был разделен на два: на крупные и срочные платежи, обрабатываемые в системе BISS, и на прочие платежи (несрочные), проводимые в клиринговой системе.

Платежи, совершаемые через систему BISS с помощью электронных расчетных документов, насчитывают более 90 % от их общей суммы.

7.2. Юридический аспект

Платежная система Беларуси регулируется двухъярусной законодательной структурой.

Первый ярус включает в себя законы и Указы Президента Республики Беларусь. **Законом Республики Беларусь «О Национальном банке Республики Беларусь»** (ст.16) установлено, что в число основных функций Национального банка входят: организация межбанковских расчетов, определение и утверждение порядка, форм и правил организации безналичных расчетов в народном хозяйстве республики и ответственности за их нарушение.

Место и роль коммерческих банков в организации безналичных расчетов определены **Законом Республики Беларусь «О банках и банковской деятельности Республики Беларусь»** (ст. 19, 21), который устанавливает, что расчеты между банками осуществляются через корреспондентские счета, а отношения банков с клиентами строятся на договорной основе. Клиенты самостоятельно выбирают банки для кредитно-расчетного обслуживания.

В настоящее время действует **Банковский кодекс Республики Беларусь** (далее – Банковский кодекс) от 25 октября 2000г. (с изменениями и дополнениями от 17 июля 2006 г.), который регулирует все аспекты банковской деятельности в стране.

Законом Республики Беларусь «Об электронном документе» определены основные требования, предъявляемые к электронным документам и их защите, а также права, обязанности и ответственность участников правоотношений, возникающих в сфере обращения электронных документов.

Второй ярус структуры, регулирующей платежи, охватывает нормативные документы, принятые НБ РБ в соответствии с предоставленным ему Банковским кодексом правом. Порядок осуществления безналичных расчетов в национальной валюте между банками Республики Беларусь закреплен в **Правилах осуществления межбанковских расчетов** от 28.09.2000 №2.3, в которых

приведены основные термины и определения, используемые в платежной системе Республики Беларусь, а также общие положения и принципы проведения межбанковских платежей через систему валовых расчетов и клиринговую систему расчетов.

Общий порядок и основные правила проведения межбанковских расчетов в автоматизированной системе межбанковских расчетов (далее – АС МБР), а также функции, полномочия и ответственность Национального банка, БМРЦ, банков и небанковских кредитно-финансовых организаций закреплены в **Инструкции по осуществлению межбанковских расчетов через АС МБР НБ РБ** от 10.03.2005 № 37. Данная Инструкция определяет форматы сообщений, а также порядок обмена сообщениями и технологию проведения платежей через АС МБР.

Правоотношения, возникающие между Национальным банком и банками, между банками при проведении межбанковских расчетов, а также между банками и клиентами в рамках заключенных договоров на расчетно-кассовое обслуживание, регулируются **Положением об ответственности за нарушение расчетных операций** № 759, 1996 г. Положение предусматривает материальную ответственность банка за задержку оплаты платежных документов, за задержку в зачислении средств на счета субъектов хозяйствования свыше одного рабочего дня с момента их поступления на корреспондентский счет банка, а также ответственность клиента за неуведомление банка в течение десяти календарных дней после получения выписки со счета об ошибочно зачисленных на его счет суммах.

7.3. Общие положения

В соответствии со статьями 25, 32 Банковского кодекса Республики Беларусь от 25 октября 2000 г. № 441–3 одной из основных целей деятельности Национального банка Республики Беларусь (далее – Национальный банк) является организация эффективного, надежного и безопасного функционирования платежной системы.

В рамках достижения этой цели Национальный банк осуществляет управление функционированием платежной системы Республики Беларусь и надзор за ней посредством установления правил осуществления платежей, тарифной политики, управления ликвидностью, а также посредством сбора, накопления и анализа показателей, характеризующих состояние платежной системы Республики Беларусь.

Национальный банк определяет правила, сроки и стандарты проведения в Республике Беларусь расчетов в безналичной и наличной формах и ответственность за их нарушение.

Национальный банк ведет ведомственный архив данных и документов по межбанковским расчетам. Национальный банк вправе использовать этот архив для статистической и иной обработки, а также для подтверждения операций, осуществленных при проведении межбанковских расчетов.

Межбанковские расчеты в Республике Беларусь осуществляются в системе BISS, являющейся основным функциональным компонентом автоматизированной системы межбанковских расчетов Национального банка (далее – АС МБР). BISS (BelarusInterbankSettlementSystem) – система межбанковских расчетов, функционирующая на валовой основе, в которой в режиме реального времени осуществляются расчеты по срочным и несрочным денежным переводам, а также расчеты по результатам клиринга в смежных системах (по сделкам купли–продажи ценных бумаг и финансовых инструментов срочных сделок, по операциям с использованием банковских пластиковых карточек). Обязательным условием для осуществления расчетов через систему BISS является установление корреспондентских отношений с Национальным банком путем заключения договора и открытия корреспондентского счета в Национальном банке.

Функции оператора АС МБР выполняет Расчетный центр Национального банка Республики Беларусь (далее – Расчетный центр). Расчетный центр имеет право электронной цифровой подписи электронных сообщений, создаваемых в результате проведения межбанковских расчетов, а также право дополнительного удостоверения электронной цифровой подписью исполненных электронных платежных документов.

Режим работы системы BISS определяется графиком приема и обработки системой BISS электронных платежных документов и электронных сообщений (далее – график системы BISS). С декабря 2009 года в соответствии с графиком системы BISS продолжительность операционного дня системы BISS установлена с 9.00 до 17.30 часов. При этом продолжительность операционного времени для приема клиентских платежей составляет период с 09.00 до 16.30. В выходные и праздничные дни система BISS не работает.

Межбанковские расчеты в системе BISS осуществляются с учетом следующих принципов:

- разделение платежного потока на электронные платежные документы Национального банка, срочные электронные платежные документы и несрочные электронные платежные документы;
- обработка электронных платежных документов в режиме реального времени;
- проведение межбанковских расчетов по срочным электронным платежным документам, включая электронные платежные документы Национального банка на дебетование корреспондентских счетов банков в соответствии с

законодательством Республики Беларусь, на валовой основе в пределах денежных средств на корреспондентских счетах банков;

- проведение межбанковских расчетов по несрочным электронным платежным документам с использованием взаимозачета с учетом суммы резерва, устанавливаемого банками для осуществления расчетов по несрочным электронным платежным документам.
- отражение суммы каждого электронного платежного документа по корреспондентскому (межфилиальному) счету банка (Национального банка) индивидуально в полном размере платежа;
- наличие технологической возможности комплексного управления состоянием корреспондентских счетов, включая мониторинг состояния расчетов и использование предоставляемых Национальным банком инструментов поддержания ликвидности.

Банк–отправитель на основании оформленных в соответствии с законодательством Республики Беларусь платежных документов от своего имени формирует электронные платежные документы и передает их в систему BISS. Передача электронных платежных документов в АС МБР производится банками и Национальным банком равномерно в соответствии с графиком системы BISS непосредственно после списания денежных средств со счетов клиентов либо со счетов по учету собственных платежей. В формируемых для передачи в систему BISS электронных платежных документах банками–отправителями указывается статус: "Срочный" или "Несрочный".

При отсутствии (недостаточности) денежных средств на корреспондентском счете банка–отправителя срочные электронные платежные документы помещаются в очередь ожидания средств. Очередь ожидания средств по срочным электронным платежным документам формируется в зависимости от времени их поступления и с учетом приоритетов. В случае недостаточности суммы резерва и (или) отсутствии встречных электронных платежных документов несрочные электронные платежные документы помещаются в очередь ожидания средств для обработки в следующем сеансе взаимозачета. Обработка несрочных электронных платежных документов из очереди ожидания средств осуществляется независимо от времени их поступления. Банк–отправитель может отозвать электронный платежный документ из очереди ожидания средств по срочным и несрочным электронным платежным документам путем передачи в систему BISS электронного сообщения.

В системе BISS допускается перевод несрочных (срочного) электронных платежных документов в срочные (несрочный) посредством направления банком–отправителем в систему BISS соответствующих электронных сообщений на присвоение им приоритета.

Межбанковский расчет в системе BISS является окончательным и не подлежит аннулированию после изменения состояния корреспондентских (межфилиального) счетов банков (Национального банка).

Банки–получатели на основании электронных платежных документов банков–отправителей, дополнительно удостоверенных электронной цифровой подписью Расчетного центра, отражают операции по корреспондентскому счету банка и субкорреспондентским счетам филиалов (отделений) банка Республики Беларусь, зачисляют денежные средства на счета клиентов либо на счета по учету собственных средств банка–получателя в кратчайшие сроки в течение текущего операционного дня банка.

В настоящее время программно–технический комплекс АС МБР соответствует требованиям руководящих документов и стандартов Республики Беларусь по обеспечению технической возможности проведения межбанковских расчетов. Случаев несанкционированного доступа в платежную систему не допущено. Параметр доступности клиентов к АС МБР (с нарастающим итогом от начала года) на 01.09.2011 составил 100 процентов дневного фонда рабочего времени (при нормативе не ниже 99 процентов).

В соответствии с требованиями Национального банка Республики Беларусь банками проводится работа по повышению надежности своих автоматизированных систем, взаимодействующих с АС МБР. О положительных результатах работы говорит тот факт, что время продления работы АС МБР сверх установленного регламента по причине сбоев автоматизированных и обеспечивающих систем (энергоснабжение, связь) банков значительно снизилось.

Первоочередные задачи в развитии платежной системы страны нашли отражение в Концепции развития национальной платежной системы Республики Беларусь до 2015 года с учетом мировых тенденций. Концепцией очерчена среднесрочная стратегия развития национальной платежной системы, направленная на дальнейшее повышение ее эффективности, надежности и безопасности на основе совершенствования организационной структуры системы межбанковских расчетов, развития и совершенствования систем стандартизации и сертификации, использования накопленного отечественного и международного опыта в области организационного, нормативно–правового и технологического обеспечения.

В настоящее время при совершении безналичных расчетов в Республике Беларусь используются следующие платежные инструменты:

- платежные поручения;
- платежные требования;
- чеки;
- требования–поручения;
- аккредитивы;
- банковские пластиковые карточки.

7.4. Программно-технический комплекс АС МБР

Основными компонентами программно-технической инфраструктуры АС МБР являются программно-технические комплексы (далее – ПТК), включающие технические средства и системное программное обеспечение (далее – ПО), а также прикладное ПО АС МБР.

Совокупность взаимосвязанных ПТК и прикладного ПО образует системы:

- центральный вычислительный комплекс (далее – ЦВК) АС МБР;
- межбанковская телекоммуникационная сеть (далее – МБТС);
- система передачи информации (далее – СПИ);
- система управления ПТК АС МБР;
- автоматизированная система Центрального архива электронных документов Национального банка;
- системы жизнеобеспечения (электроснабжения, теплоснабжения и т.д.).

На ЦВК функционируют следующие информационные системы или их подсистемы:

- ядро системы межбанковских расчетов по крупным и срочным денежным переводам на валовой основе в режиме реального времени (далее – ядро системы BISS);
- ядро центрального узла системы передачи финансовой информации (далее – ядро ЦУ СПФИ), включающее в себя менеджер MQSeries, средства ведения оперативного архива на основе системы управления базами данных (далее – СУБД) DB2 и входные маршрутизаторы;
- клиринговая система расчетов по прочим (мелким несрочным) денежным переводам (далее – КСР);

Функционирование ядра системы BISS осуществляется на ЦВК резервного вычислительного центра НБ РБ (далее – ЦВК РВЦ) в среде операционной системы OS/390 под управлением монитора транзакций CICS. Для доставки сообщений на обработку и посылки ответных сообщений используется средство доставки сообщений MQSeries. Для хранения входящих и исходящих сообщений и оперативных данных, необходимых для расчетов, используется база данных, управляемая СУБД DB2.

Функционирование ядра ЦУ СПФИ осуществляется на ЦВК РВЦ в среде операционной системы OS/390. Взаимодействие с банками осуществляется через средство доставки сообщений MQSeries по протоколу TCP/IP. Для протоколирования работы ядра ЦУ СПФИ используется база данных, управляемая СУБД DB2. Входные маршрутизаторы – пакетные задания –

обеспечивают перемещение сообщений между очередями согласно заданным правилам.

Функционирование КСР осуществляется на ЦВК основного вычислительного центра (далее – ЦВК ОБЦ) в среде операционной системы OS/390 путем выполнения комплекса пакетных заданий. С целью осуществления мониторинга КСР данные расчетов КСР помещаются в базу данных, управляемую СУБД DB2, и в очереди средства доставки сообщений MQSeries.

7.5. Структура центрального вычислительного комплекса

ЦВК является пространственно – распределенным вычислительным комплексом, состоящим из ЦВК ОБЦ и ЦВК РВЦ.

Программно – технические средства ЦВК РВЦ обеспечивают функционирование ядра системы BISS и ядра ЦУ СПФИ, ЦВК ОБЦ –Клиринговой системы и тестовой системы.

В состав технических средств ЦВК ОБЦ входят:

- ЭВМ IBM 9672 R14;
- телепроцессор IBM 3745/3746-900;
- маршрутизатор CISCO 7513;
- дисковая подсистема ESS 2105 ОБЦ;
- ленточная подсистема IBM 3490;
- дисковая подсистема RAMAC 2;
- дисковая подсистема RAMAC 3;
- терминальный контроллер IBM 3174 11L;
- дисплеи InfoWindow;
- устройства управления дисплеями ЕС – 7922;
- дисплеи ЕС – 7927;
- АЦПУ ЕС – 7040.

В состав технических средств ЦВК РВЦ входят:

- ЭВМ IBM 9672 R16;
- дисковая подсистема ESS 2105 РВЦ;
- ленточная подсистема IBM 3490;
- терминальный контроллер IBM 3174 11L;
- дисплеи InfoWindow;
- устройства управления дисплеями ЕС – 7922;
- дисплеи ЕС – 7927;
- АЦПУ ЕС – 7040.

Каждая из ЭВМ поделена на 2 раздела:

- ЭВМ IBM 9672 R14 имеет раздел KLIR для функционирования Клиринговой системы;
- ЭВМ IBM 9672 R16 имеет раздел BISS для функционирования ядра системы BISS и раздел DEBUG – для ядра ЦУ СПФИ.

Описание критичных ресурсов

При функционировании ЦВК критичными являются следующие ресурсы:

- ЭВМ 9672 R14, на которой функционирует Клиринговая система;
- ЭВМ 9672 R16, на которой функционируют ядро системы BISS и ядро ЦУ СПФИ;
- сетевая карта OSA/2 ЭВМ 9672 R14, обеспечивающая взаимодействие данной ЭВМ с АРМами, расположенными в сети АС МБР и в технологической сети;
- сетевая карта OSA/2 ЭВМ 9672 R16, обеспечивающая взаимодействие данной ЭВМ с АРМами, расположенными в технологической сети;
- сетевые карты OSA/E ЭВМ 9672 R16, обеспечивающая взаимодействие данной ЭВМ с АРМами, расположенными в сети АС МБР, а также с банками – участниками СПФИ;
- дисковые подсистемы ESS 2105 ОВЦ и РВЦ, на которых расположены резидентные тома операционных систем и тома с оперативными данными;
- ленточные подсистемы IBM 3490, предназначенные для создания резервных копий оперативных данных по концу операционного дня, а также для восстановления данных на этапе подготовки их загрузки в Центральный архив электронных документов Национального банка Республики Беларусь (далее – ЦА ЭД НБ РБ);
- рабочие места операторов ЦВК.

7.6. Резервный вычислительный центр Национального банка

Национальный банк большое внимание уделяет модернизации программной и технической базы осуществления безналичных расчетов, позволяющей оставаться на рубеже самых современных информационных технологий в данной области. Развитие программно-технической инфраструктуры проводится поэтапно в соответствии с разработанным и утвержденным Советом директоров Национального банка планом.

Современная АС МБР должна обеспечивать высокую степень операционной надежности, позволяющую сформировать окончательные расчеты за день, в том числе возможность обработки трафика в таких критических и нештатных ситуациях как стихийные бедствия, техногенные катастрофы и террористические акты, сбои энергопитания, разрыв коммуникаций.

В связи с этим были начаты работы по созданию на территории Республики резервного вычислительного центра Национального банка. Его необходимость обусловлена тем, что в настоящее время все функционально необходимые вычислительные и технические средства АС МБР расположены в одном здании на территории основного вычислительного центра. При этом в случае крупных аварий и стихийных бедствий в районе расположения этого вычислительного центра межбанковские расчеты могут быть прерваны на достаточно длительный срок, что вызовет дестабилизацию экономики республики. Создание резервного вычислительного центра позволяет возобновить межбанковские расчеты в случае угроз любого характера в течении 4 часов, причем на технические мероприятия по переводу на резервные системы отводится 1 час.

В проект резервного центра заложены передовые технологии в области оптических телекоммуникаций, хранения, передачи и обработки больших объемов информации. Концепция предусматривает создание территориально удаленных хранилищ данных, полностью дублирующих друг друга в случае выхода из строя одного из них. Разнесение основного и резервного центров предполагается на расстояние порядка 15 км, что достаточно для сохранения работоспособности одного из них в случае техногенных катастроф или крупных аварий в районе размещения другого. Связь между центрами осуществляется по волоконно-оптическим линиям связи с использованием современных технологий сжатия данных на основе мультиплексирования.

Следующим этапом построения высоконадежной и безопасной платежной системы является реконструкция Основного вычислительного центра с целью повышения его операционной надежности и объектовой безопасности.

7.7. Центральный архив электронных документов

В целях обеспечения сохранности, учета и использования электронных документов в 2000 году в Национальном банке был создан первый в республике Центральный архив электронных документов.

Центральный архив электронных документов принимает на хранение электронные документы и информацию по межбанковским платежам, электронные документы структурных подразделений центрального аппарата Национального банка, которые используют автоматизированные системы для обработки и хранения документов в электронном виде.

В настоящее время в Центральном архиве электронных документов хранятся документы по межбанковским расчетам с 1998 года и по текущий день, электронные документы Центрального депозитария Национального банка Республики Беларусь по государственным ценным бумагам и ценным бумагам Национального банка Республики Беларусь за 2000-2011 годы, электронные документы по первичному размещению государственных ценных бумаг и ценных бумаг Национального банка Республики Беларусь (НБ РБ) за 2001- 2011 годы.

Объем ежедневно принимаемых на хранение в Центральный архив электронных документов НБ РБ электронных документов (ЭД) и сопутствующей информации по межбанковским платежам составляет от 14 до 17 Мб или от 130 до 160 тысяч документов.

С конца 2002 года создана и успешно функционирует автоматизированная подсистема документальной синхронизации архивов участников межбанковских расчетов, которая обеспечивает взаимодействие Центрального архива ЭД с архивами банков-участников межбанковских расчетов и позволяет осуществлять ежедневную сверку электронных платежных документов, подлежащих архивному хранению. Кроме обеспечения гарантии целостности и полноты хранимого фонда электронных документов система дала возможность дублирования информации на случай ее потери и аудита архивов банков Национальным банком.

Центральный архив электронных документов Национального банка Республики Беларусь работает в тесном взаимодействии с органами государственного контроля республики. В сроки установленные регламентом правомочным структурным подразделениям Комитета государственного контроля в электронном виде передается информация о всех межбанковских платежах, проводимых за операционный день.

Правовые основы применения электронных документов, основные требования, предъявляемые к ним, а также права, обязанности и ответственность участников правоотношений, возникающих в сфере обращения электронных документов, установлены Законом Республики Беларусь “Об электронном документе и электронно-цифровой подписи”.

В данном Законе устанавливается, что программные и технические средства, используемые для создания, обработки, передачи и хранения электронных документов, подлежат сертификации в органе по сертификации при Национальном банке Республики Беларусь.

В рамках реализации положений Закона при Национальном банке на базе УП БМРЦ и УП «Центр банковских технологий» (ЦБТ) в составе Национальной системы сертификации были созданы орган по сертификации программно-технических средств в области банковских услуг и технологий и аккредитованы на независимость и компетентность две испытательные лаборатории.

7.8. Расчетный центр

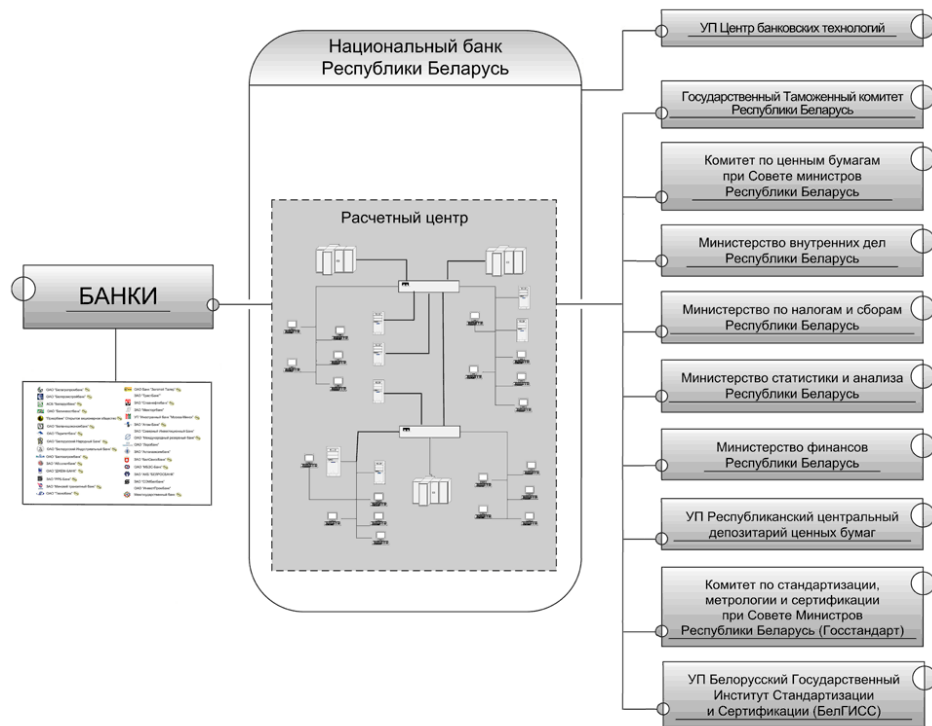


Рисунок 1 – Роль расчетного центра

ТЕМА 8: ЕРИП.

8.1. Введение

14 марта 2005 г. было принято постановление Совета Министров Республики Беларусь и Национального банка Республики Беларусь 5 «О создании межведомственной комиссии по формированию на территории Республики Беларусь единого расчетного и информационного пространства для оплаты услуг через банки, небанковские кредитно-финансовые организации, организации почтовой и электрической связи».

8.2. Основные понятия:

- *Единое расчетное и информационное пространство (ЕРИП)* - совокупность единых правил и процедур, определяющих порядок осуществления платежей с использованием различных платежных инструментов для осуществления расчетов по розничным платежам за услуги в пользу исполнителей услуг.
- *Участник ЕРИП* — юридическое или физическое лицо, участвующие в информационном взаимодействии посредством АИС ЕРИП.
- *Потребитель услуг (плательщик)* – физическое или юридическое лицо, потребляющее услуги производителей услуг и производящее оплату за потребленные услуги через расчетных агентов.

- *Производитель услуг (исполнитель услуг, поставщик услуг, ПУ)* - юридическое лицо, оказывающее услуги юридическим и физическим лицам и получающее за эти услуги оплату на свои расчетные (текущие) счета через расчетных агентов.
- *Расчетный агент (РА)* – банк, небанковская кредитно-финансовая организация, организация почтовой и электрической связи, осуществляющая роль посредника при приеме платежей от потребителей услуг в пользу производителей услуг.
- *Центральный узел (ЦУ)* - структурное подразделение Национального банка Республики Беларусь, осуществляющее взаимодействие с региональными узлами и расчетными агентами.
- *Региональный узел (РУ)* - структурное подразделение Национального банка Республики Беларусь (в составе Главных управлений Национального банка Республики Беларусь по областям), осуществляющее взаимодействие с производителями услуг в регионе и Центральным узлом.
- *Банк производителя услуг* – банк, в котором открыт расчетный (текущий) счет ПУ, на который поступают денежные средства за оказанные услуги, и с которым заключен договор на расчетно-кассовое обслуживание.
- *Автоматизированная система межбанковских расчетов (АС МБР)* – часть национальной платежной системы в Беларуси, включающая совокупность процедур и программно-технических комплексов, позволяющих осуществлять межбанковские расчеты по денежным обязательствам между банками Республики Беларусь
- *Автоматизированная информационная система единого расчетного и информационного пространства (АИС ЕРИП, Система)* – Совокупность программно-технических комплексов, баз данных и информационно-коммуникационных систем, функционирующих на основе общих принципов и обеспечивающих взаимодействие участников информационного обмена в процессе осуществления платежей за услуги.
- *Расчетная система ЕРИП (РС ЕРИП)* – обеспечивает прием и гарантию перечисления денежных средств за оказанные услуги от потребителя этих услуг производителю услуг.
- *Биллинговая система* - программный комплекс, осуществляющий учет объема потребляемых абонентами услуг, расчет и списание денежных средств в соответствии с тарифами компании.
- *Нормативно-справочная информация (НСИ)* – условно-постоянная часть всей информации, включает в себя словари, справочники и классификаторы, данные из которых (термины, единицы измерения, коды, наименования материалов, контрагентов и т.п.) используются при формировании текущей (workflow) информации. НСИ представляет собой информационное описание объектов, обладающих общим признаком и сведенных в группы, то есть в справочники, для каждого из которых структура описания информации об этих объектах заранее определена.

8.3. Основные сведения об АИС ЕРИП

Автоматизированная информационная система единого расчетного и информационного пространства предназначена для обеспечения комплексного обслуживания потребителей услуг, снижения затрат на обработку операций оплаты услуг, предоставления возможности оплатить услуги через любого расчетного агента в любом регионе.

Основные задачи АИС ЕРИП:

- обеспечение расчетных агентов информацией, необходимой для приема платежей за услуги, оказанные исполнителями услуг;
- контроль прохождения принятых платежей для обеспечения своевременности и полноты поступления на текущие (расчетные) счета исполнителей услуг денежных средств, уплаченных потребителями услуг;
- предоставление исполнительным комитетам необходимой статистической и учетной информации.
- обеспечить возможность единообразной и повсеместной оплаты услуг, в том числе с учетом социальных льгот, посредством использования наличных денежных средств и банковских пластиковых карточек через пункты приема оплаты (ППО) отделений расчетных агентов, системы мобильных и Интернет платежей.
- в систему должны подключаться исполнители услуг, потребление услуг которых носит постоянный характер (коммунальные службы, операторы связи, обслуживающие радиовещание, телевидение, охрану квартир и т.д.).
- система должна обеспечивать защиту информации исполнителей услуг.

Участники АИС ЕРИП:

- производители услуг;
- банки производителей услуг;
- расчетные агенты;
- региональные узлы ЕРИП;
- центральный узел ЕРИП;
- телекоммуникационный оператор;
- местные органы власти;
- потребители услуг.

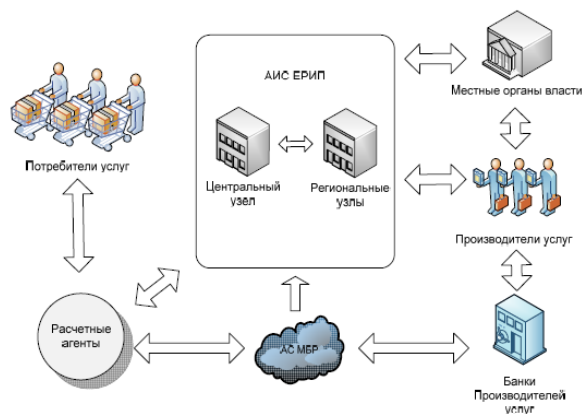


Рисунок 1. Схема взаимодействия участников

Взаимодействие всех участников в рамках АИС ЕРИП образует несколько взаимосвязанных процессов:

- процесс подготовки, сбора, консолидации и распространения информации, необходимой для выполнения операций оплаты услуг (в том числе и НСИ);

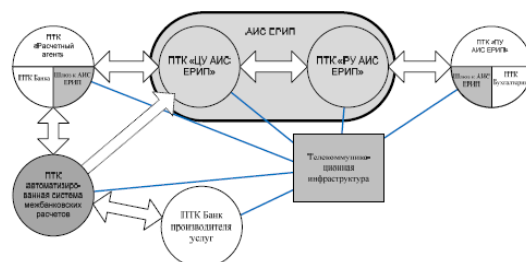


Рисунок 2. Схема взаимодействия программно-технических комплексов участников

- процесс выполнения потребителями услуг операций оплаты в пользу производителей услуг в пунктах приема платежей расчетных агентов;
- процесс проведения расчетов между расчетными агентами и производителями услуг за выполненные потребителями услуг операции оплаты услуг;
- процесс проведения расчетов между расчетными агентами и узлами ЕРИП по комиссионным вознаграждениям за услуги АИС ЕРИП;
- процесс предоставления аналитической, статистической и учетной информации по оплате услуг заинтересованным участникам.

8.4. Нормативно-справочная информация аисерип

Нормативно-справочная информация (НСИ) – условно-постоянная часть всей информации, включает в себя словари, справочники и классификаторы, данные из которых используются при формировании текущей информации. НСИ представляет собой информационное описание объектов, обладающих общим признаком и сведенных в группы, то есть в справочники, для каждого из которых структура описания информации об этих объектах заранее определена.

Состав и структура

Нормативно-справочная информация (НСИ) подразделяется на внешнюю и внутреннюю.

К внешней НСИ относятся справочники, которые формируются и ведутся другой (смежной) системой, и используются путем прямого доступа к таблице БД или предоставляются в виде файла данных для дальнейшей загрузки в таблицы БД. При размещении в БД данные внешних справочников могут (при необходимости) приводиться к виду необходимому для использования, и таким образом справочник из внешнего переходит в статус внутреннего.

К внутренней НСИ относятся:

- справочники, которые формируются и ведутся в БД Системы ее средствами (осуществляется ручной ввод, корректировка и удаление информации).
- справочники, которые формируемые на основании внешних справочников (дополняется средствами Системы автоматически или вручную);
- справочники, которые «защиты» как константы непосредственно в тексты программных модулей.

«Защиты» справочники представляют собой стандартные значения (константы), которые формируются, как правило, один раз на момент внедрения Системы и жестко связаны с программным обеспечением. Значения таких справочников при необходимости могут быть изменены только с привлечением специалистов разработчика программного обеспечения.

Формирование нормативно-справочной информации, необходимой для функционирования Системы осуществляет Центральный узел в консолидированной БД ЕРИП в рамках модулей «АРМ администратора» и «АРМ оператора», привлекая (при необходимости) соответствующие министерства и ведомства. НСИ подлежит использованию в АИС ЕРИП, только после ее внесения в консолидированную БД ЕРИП.

Цепь взаимодействия:

- информация о производителях услуг и их требованиях к оплате услуг (извещения на оплату услуг) предоставляется производителями услуг в соответствующий Региональный узел.
- Региональные узлы взаимодействуют с производителями услуг и Центральным узлом.
- изменения НСИ в автоматизированном режиме рассылаются в Региональные узлы ЕРИП.

Учетные данные производителей услуг включают:

- реквизиты производителя услуг;
- реквизиты расчетного счета производителя услуг;
- реквизиты услуг производителя услуг;
- процент комиссии с производителя услуг по конкретной услуге;
- сценарий оплаты и параметры платежа для конкретной услуги;
- параметры доступа к биллинговой системе производителя услуг (если таковая есть)

Указанные данные регистрируются в базе данных Регионального узла один раз - при заключении договора. Далее эти данные передаются в Центральный узел, где размещаются в консолидированной базе данных. На основании этих данных формируется справочная информация о производителе услуг однозначно определяющая его в рамках Системы и необходимая для ее функционирования.

8.5. Взаимодействия программно-технических комплексов

Потоки информации между ПТК могут быть двух типов:

- Off-line – поток возникает с определённой периодичностью по расписанию;
- On-line – поток возникает сразу же, при появлении необходимости обновления информации передаваемой в данном потоке.

Использование различных типов потоков между ПТК, участвующих в работе АИС ЕРИП, позволяет оптимизировать нагрузки на всю систему АИС ЕРИП в целом.

При взаимодействии ПТК происходит обмен информацией, для описания которого можно выделить следующие потоки информации:

- поток нормативно-справочной информации – поток сообщений, которые содержат реквизиты используемых в АИС ЕРИП справочников.
- поток данных о производителях услуг – поток сообщений, которые содержат реквизиты собственно производителя услуг и список услуг производителя услуг и их реквизиты;
- поток данных описания дерева услуг – поток сообщений, которые содержат информацию об узлах дерева услуг и привязку конкретных услуг к узлам дерева;
- поток требований к оплате – поток сообщений, которые содержат данные о задолженностях потребителей услуг;
- поток реестров совершенных платежей – поток сообщений, которые содержат данные об операциях оплаты услуг, совершенных потребителями услуг в пользу производителя услуг, но по которым расчетный агент еще не перечислил средства на расчетные счета производителя услуг;
- поток реестров сторнированных платежей – поток сообщений, которые содержат данные о сторнированных операциях оплаты услуг;
- поток реестров оплаченных платежей – поток сообщений, которые содержат информацию об операциях оплаты услуг, совершенных потребителями услуг, по которым расчетный агент перечислил средства на расчетные счета производителя услуг;

Взаимодействие между ПТК «ЦУ АИС ЕРИП» и ПТК «РУ АИС ЕРИП»

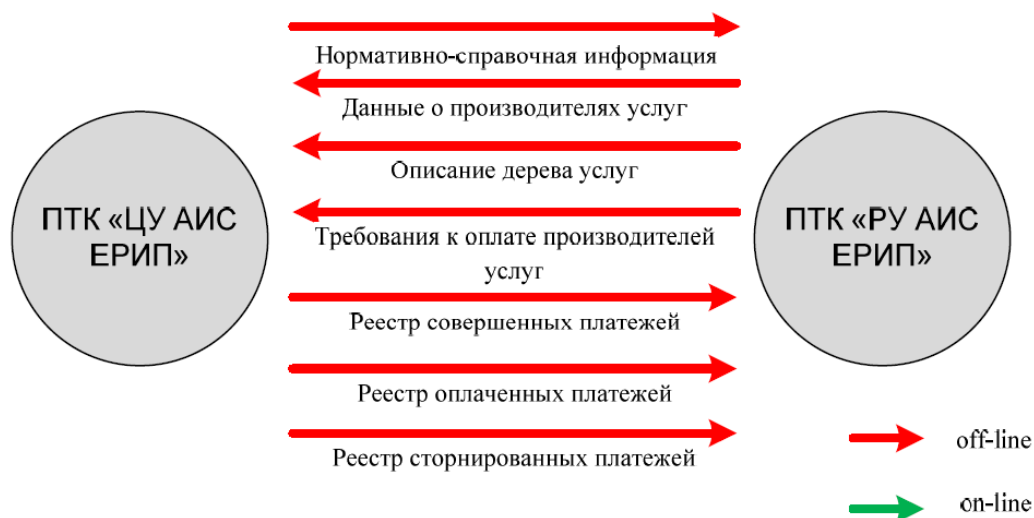


Рис. 2. Потоки между ПТК «ЦУ АИС ЕРИП» и ПТК «РУ АИС ЕРИП»

Направление обмена указывает, какой ПТК в данном обмене является клиентом (инициатором соединения), и какой из них в данном обмене является сервером (ожидающим соединение).

Взаимодействие между ПТК «Расчетного агента» и ПТК «ЦУ АИС ЕРИП»

Т.к. у каждого расчетного агента, в общем случае, могут использоваться различные ПТК «Расчетного агента», то для организации взаимодействия ПТК «Расчетного агента» с АИС ЕРИП, необходимо использовать модуль «Шлюз к АИС ЕРИП» предназначенный для работы с конкретным ПТК «Расчетного агента».

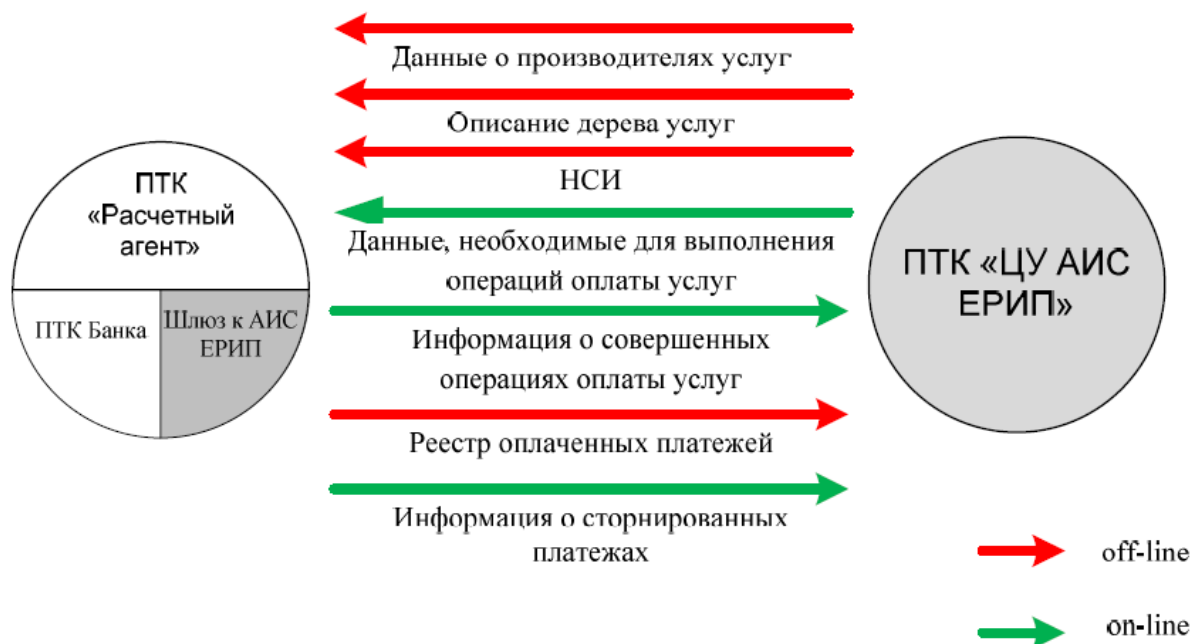


Рис. 4. Потоки между ПТК «Расчетного агента» и ПТК «ЦУ АИС ЕРИП»

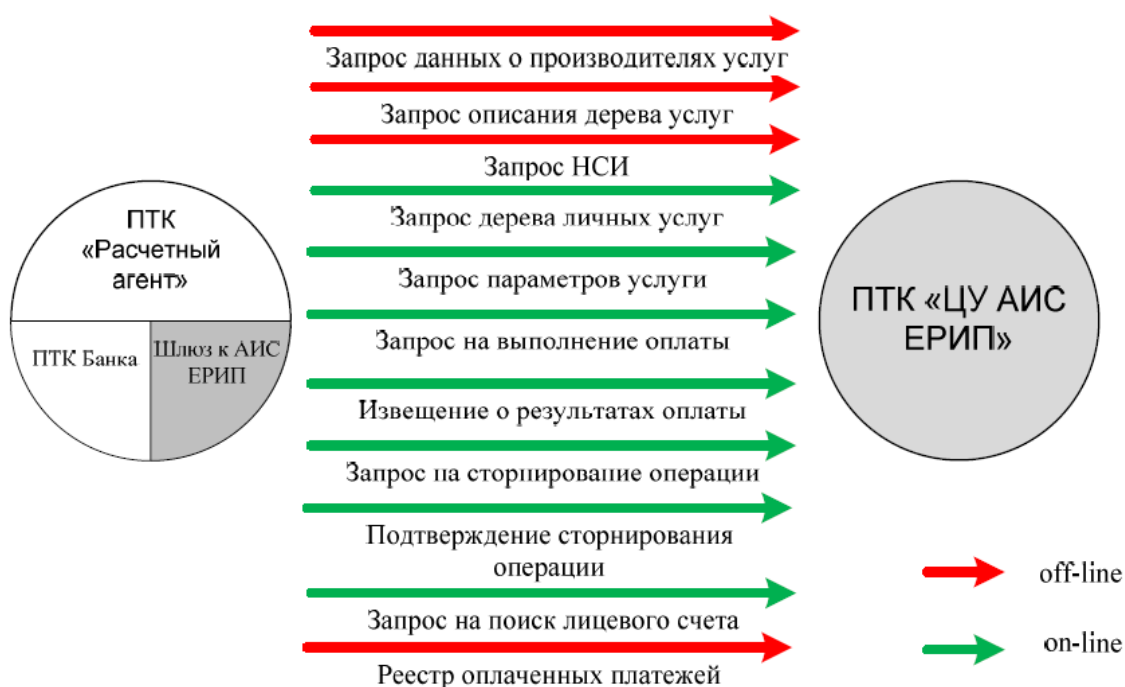


Рис. 5. Обмен информации при взаимодействии ПТК «Расчетного агента» и ПТК «ЦУ АИС ЕРИП»

Взаимодействие ПТК «Региональный узел АИС ЕРИП» и ПТК «Производителя услуг»

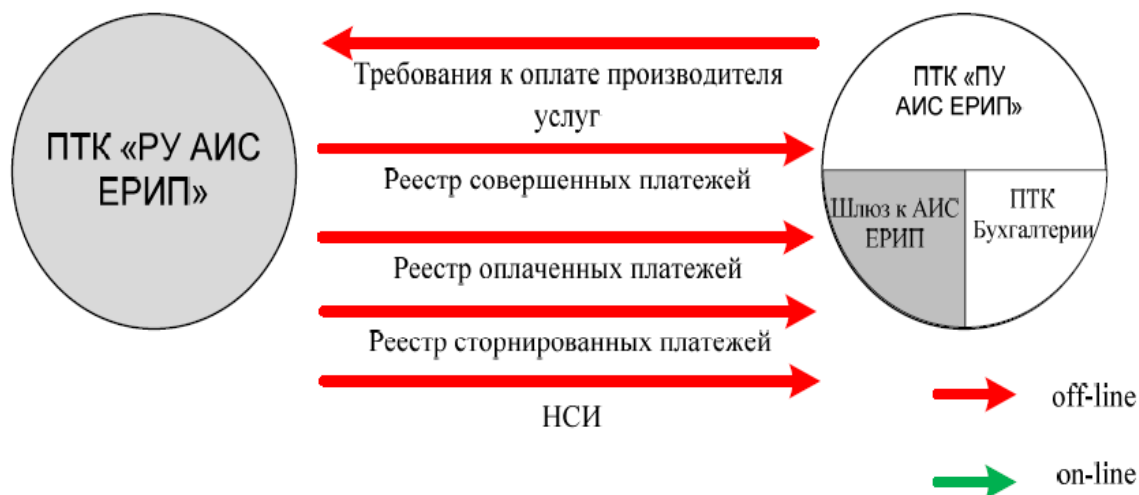


Рис. 6. Потоки между ПТК «Производителя услуг» и ПТК «РУ АИС ЕРИП»

В случае, когда производитель услуг предоставляет доступ к своей билинговой системе, ПТК «Производителя услуг» взаимодействует с ПТК «ЦУ АИС ЕРИП» по следующей схеме:

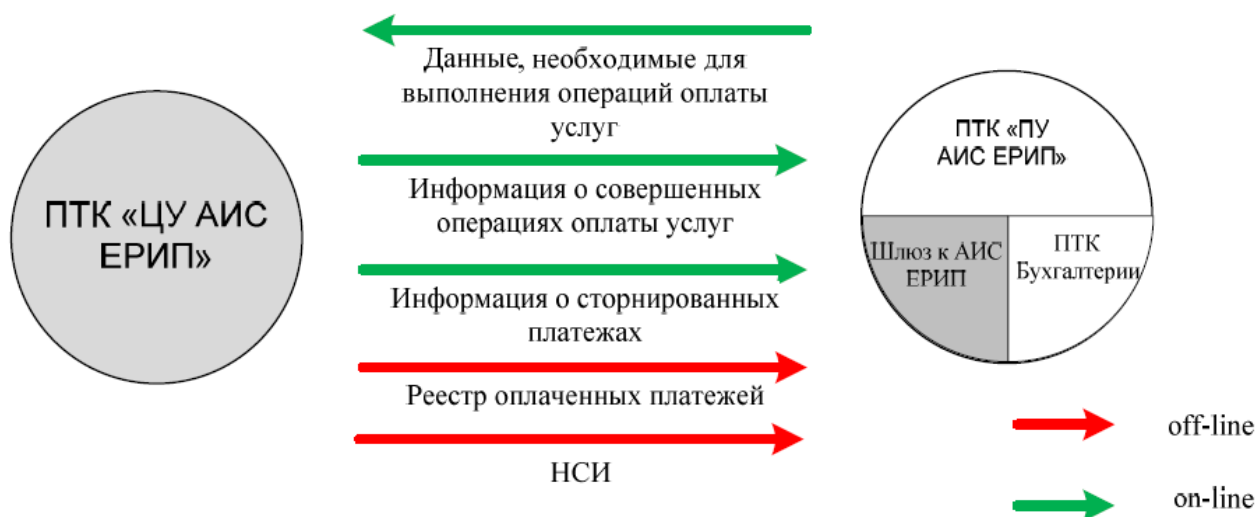


Рис. 8. Потоки между ПТК «Производителя услуг» и ПТК «ЦУ АИС ЕРИП»

ТЕМА 9: ПЛАСТИКОВЫЕ КАРТЫ И ИНФРАСТРУКТУРА ИХ ОБСЛУЖИВАНИЯ.

9.1. Пластиковые карты — новый инструмент организации безналичных расчетов

Пластиковая карта - обобщающий термин, который обозначает все виды карточек, различающихся по назначению, по набору оказываемых с их помощью услуг, по своим техническим возможностям и организациям, их выпускающим.

Важнейшая особенность всех пластиковых карт, независимо от степени их совершенства, состоит в том, что на них хранится определенный набор информации, используемый в различных прикладных программах. Карта может служить пропуском в здание, средством доступа к компьютеру, средством оплаты телефонных переговоров, водительским удостоверением и т. д. В сфере денежного обращения пластиковые карты являются одним из прогрессивных средств организации безналичных расчетов. В системе безналичных расчетов они составляют особый класс орудий платежа, которые могут обладать качествами как дебетовых, так и кредитных инструментов.

9.2. История развития пластиковых карт и платежных систем

Первое теоретическое упоминание об использовании карт как платежного средства появилось в Англии и относится к концу прошлого века. Идею кредитных карт выдвинул в своей книге Джеймс Беллами «Глядя назад» (J.Bellami. Lookingbackwards, 1880 г.).

На практике пионерами в этой области оказались США. Первая кредитная карта была выпущена в 1914г. фирмой GeneralPetroleumCorporationofCalifornia (ныне MobilOil). Карточки использовались для оплаты в процессе торговли нефтепродуктами. В этом качестве они быстро завоевали популярность. Владелец карты получал значительные удобства в обслуживании и скидки при покупке товара. Фирма-эмитент получала постоянных клиентов и стабильные доходы.

С увеличением числа пользователей встал вопрос об учете и регистрации продаж по каждой эмитированной карте, это вызвало к жизни процесс эмбоссирования карт (теснение номера карты, данных клиента, срока действия карты). Практически без изменений эмбоссирование сохранилось до наших дней и широко используется, в том числе и на смарт-картах. Первые карты с эмбоссированием изготавливались из металла, но затем они были вытеснены пластиковыми картами, так как последние оказались более практичными.

Эти карты не были еще платежным средством. Это были так называемые клубные карты, которые подтверждали принадлежность пользователя к той или иной системе учреждений сферы обслуживания. Эти карты имели строго ограниченное

распространение как по видам услуг, так и географически. Использование клубных карт широко распространено и в настоящее время.

Первые карты, являющиеся полноценным платежным средством, были выпущены не банковскими гигантами, а DinersClub (1950 г.), AmericanExpress и HiltonCredit (1959 г.). В отношении изготовления они мало чем отличались от предыдущих, но по своим функциям это были совершенно новые карты. Фактически эти годы можно считать моментом рождения нового инструмента организации безналичных расчетов.

Первая банковская карта была выпущена в 1951 г. маленьким нью-йоркским банком LongIsland, и с тех пор началось бурное развитие этого вида услуг. Первая универсальная карта большого банка BankofAmerica прошла испытания в Fresco, California, в 1956 г. С 1966 г. BankofAmerica начал продажу лицензий на использование карточной технологии другим банкам.

В ответ на это несколько крупных банков-конкурентов BankofAmerica (14 нью-йоркских банков) учредили свою **Межбанковскую карточную ассоциацию - МКА (InterbankCardAssociation)**, а в 1969 г. эта ассоциация купила права на карты MasterCharge (Мастер Чадж), выпускавшиеся карточной ассоциацией банков западных штатов (4 калифорнийских банка), а большинство банков - членов МКА перешли на выпуск MasterCharge.

Вначале выпуск карт часто оказывался нерентабельным для банков, и это приводило к многочисленным финансовым потерям. Для того чтобы карточная технология стала рентабельной, банк-эмитент должен был быть признанным широким коммерческим сектором. Однако для того, чтобы это стало возможным, банк должен был иметь большое число клиентов, принявших новые банковские услуги. Для достижения поставленной цели огромное количество карточек было разослано по почте, хотя на практике это привело к многочисленным злоупотреблениям. Такой массовый запуск нового продукта происходил в США 1960-1965 гг. Причем, некоторые банковские учреждения предлагали карты своим клиентам бесплатно, однако по истечении года или двух иногда без всякого предупреждения накладывали на их счета годовую пошлину.

Положение, при котором BankofAmerica имел доминирующие позиции на рынке банковских карт, быстро перестало устраивать лицензированные им банки, и в 1970 г. BankofAmerica передал контроль над бизнесом карт новой организации банков - **NationalBankAmeriCard, Inc. (NBI)**, в которой он был лишь одним из членов.

Таким образом, к началу семидесятых годов в Соединенных Штатах сформировались два основных конкурента на рынке универсальных банковских карт: НБИ и МКЛ.

Обе организации с момента учреждения внесли в устав решения не принимать в свои ряды банки - члены организации конкурента, и потребовалось 10 лет (с 1966 по 1976 гг.) и несколько судебных процессов, чтобы двойное членство было разрешено.

Параллельно с развитием американского рынка шла и интернационализация карточных операций. Она началась еще в 1951 г., когда компания DinersClub выдала первую лицензию на использование своего имени и схемы в Великобритании. Примерно в это же время Британская ассоциация отелей и ресторанов начала выпускать кредитную карту BHR, которая, не являясь банковской, была все же универсальной картой. В 1965 г. эта система, объединившись со своим шведским конкурентом Rikskort, владельцем которой являлась семья Валленбергов, учредила компанию EuroCardInternational (Еврокард Интернэшнл) со штаб-квартирой в Швеции.

В 1974 г. МКА подписала соглашение с британской системой Access (ЭксессКард), которая входила в Ассоциацию Еврокард. С этого момента началось сотрудничество EuroCard и американской Межбанковской карточной ассоциации, выпускающей MasterCharge.

В 1977 г. наименование NBI было изменено на VISA USA Inc. Изменение имени имело огромное значение, так как это событие открыло дорогу широкому распространению карт VISA в США и за рубежом. По данным годового отчета VisaInternational в 2005г. находились в обращении более 1,3 млрд. карт VISA. По карточкам Visa за 2005г. всего было произведено операций розничных продаж и обналичивания денег на общую сумму **3,7 триллиона долларов**.

В 1980 г. Межбанковская карточная ассоциация дала своей карте «более международное» название MasterCard (Мастеркард).

EuroCard, расширяя свое сотрудничество с MasterCard, по мере появления новых технологий заключила соглашения с компаниями Cirrus и Maestro, что позволило расширить ассортимент предлагаемых клиентам видов услуг за счет карт для получения наличных в банкоматах. В конце 1992 г. произошло слияние EuroCardInternational с платежной системой Eurocheck. Новая организация стала называться EuropayInternational.

Конкурентная борьба между платежными системами разворачивалась не только в Европе. В Японии, например, несмотря на активные попытки завоевания этого рынка VISA и MasterCard проигрывали картам JCB (Джей-Си-Би).

Японская компания кредитных карт JCB была основана в 1961 г. JCB является лидером на рынке кредитных карт Японии и активно развивает свою экспансию в качестве транснациональной компании. На конец марта 1993 г. (т. е. на конец финансового года в Японии) количество карт в обращении составило 27,6 млн,

количество ассоциированных предприятий торговли и услуг (т. е. принимающих карты JCB) - 2,9 млн, в том числе 660 тыс. в 139 странах мира.

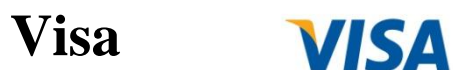
JCB ориентируется главным образом на высший и высший средний класс потребителей с высоким уровнем дохода и дифференцированным спросом.

С одной стороны, JCB - единственная в Японии компания, чьи карты являются международными. С другой стороны, JCB отличается от других международных платежных систем (VISA, Europa-MasterCard, AmericanExpress - все они гораздо крупнее JCB) усиленным акцентом на развитие своих карт не только и не столько в качестве средства платежа, сколько в качестве средства доступа к услугам в области туризма и развлечений.

В бывшем СССР карты международных систем появились еще в 1969 г. Но это были карты, эмитированные зарубежными компаниями и банками. В Советском Союзе началась создаваться сеть предприятий, принимающих эти карты в качестве платежного средства. Именно в 1969 г. было подписано первое соглашение такого рода с компанией DinersClub.

В 1974 г. на советском рынке появилась AmericanExpress, в 1975 г. -- VISA (тогда еще BankAmeriCard) и EuroCard, в 1976 г. - японская JCB. С советской стороны все соглашения подписывались Всесоюзным акционерным обществом (ВАО) «Интурист», которое и организовывало расчеты по пластиковым картам в валютных магазинах «Березка» и гостиницах.

Первым советским эмитентом международных карт был Внешэкономбанк, выпустивший в 1989 г. «золотые» карты EuroCard. Однако до сих пор точно неизвестно, сколько их было выпущено и кому именно они были выданы. Ясно только, что их было очень ограниченное количество и предназначались они для узкого круга лиц. С коммерческой точки зрения, это можно считать не более чем относительно удачным экспериментом.



Visa – это электронная платежная система, которая, являясь некоммерческой ассоциацией, объединяет более 22,000 банков-членов по всему миру. Visa выполняет посредническую роль между банками и занимается организацией расчетов и обеспечивает техническое взаимодействие между участниками системы.

Для оперативного и эффективного управления Visa разделена на 6 региональных подразделений:

- Азиатско-Тихоокеанский регион (AsiaPacific)

- Канада (Canada)
- Центральная и Восточная Европа, Ближний Восток и Африка (CEMEA)
- Европа (Europe)
- Латинская Америка и страны Карибского бассейна (LatinAmericaandCaribbean)
- Соединенные Штаты Америки (United States of America)

VISA CEMEA

Visa CEMEA является одним из самых динамично и быстро развивающихся регионов, в который входит 84 страны. Штаб-квартира Visa CEMEA находится в Лондоне, а территориальные отделения - в России, Украине, Южно-Африканской Республике, Объединенных Арабских Эмиратах и Марокко. О культурном и географическом многообразии региона говорит различие уровней развития его рынков. В некоторых странах существуют устоявшиеся системы платежных карточек, в то время как в других все еще отсутствует эффективная платежная и телекоммуникационная инфраструктура. У каждой страны есть свои возможности и задачи, на которых сосредоточивает свое внимание Visa CEMEA.

В связи с вхождением ряда стран, ранее относившихся к региону CEMEA, в Европейский Союз, структура региона CEMEA изменилась. В настоящий момент регион CEMEA разбит на 11 субрегионов:

- Южная Африка
- Южно-Африканская Республика
- Африка (Алжир, Тунис и другие страны Африки)
- Марокко
- Египет
- Саудовская Аравия
- Объединенные Арабские Эмираты
- Ближний Восток
- Центральная и Восточная Европа
- Россия
- Страны СНГ

С переходом мирового сообщества к современным видам безналичных платежей посредством пластиковых карт, география распространения продуктов Visa стремительно растет. Visa International намерена продолжать расширять свое присутствие на мировых рынках с целью предоставления удобных, надежных и отвечающих всем требованиям потребителей инструментов для оплаты товаров и услуг.

Технологическое развитие пластиковых карт

Как уже отмечалось, первые карты изготавливались из картона или металла, а затем стали выпускать пластиковые карты. Основным аргументом для внедрения пластиковых карт являлось удобство для пользователя.

С появлением новых электронных средств регистрации и сбора информации появилась возможность заносить и считывать информацию на карту при помощи магнитного кодирования.

Начало применения пластиковых карт с магнитной полосой датируется 1969 г. В комбинации с эмбоссированием такие карты широко используются до сих пор. Следует помнить, что информация на первых двух дорожках предназначена только для считывания, она записывается при выдаче карты пользователю и в процессе использования не изменяется. Распространение и прием карт с магнитной полосой по всему свету стали возможным благодаря внедрению и соблюдению платежной индустрией единого глобального стандарта.

Следующим этапом в развитии пластиковых карт история обязана французскому журналисту Ролану Морено, который в 1974 г. предложил использовать карты с электронной микросхемой. Он запатентовал эту идею и основал компанию Innovation для производства таких карт. Четырьмя годами ранее аналогичную идею запатентовал в Японии Кунитака Аримура (Kunitaka Arimura), однако международного патента он не получил.

Пластиковые карты со встроенными в них микросхемами называют еще «интеллектуальными», чип (chip)- или смарт (smart)-картами.

Появление пластиковых карт со встроенной в них микросхемой оценивается западными специалистами как революционное. На сегодняшний день смарт-карты - наиболее динамично развивающийся тип пластиковых карт. Поэтому Visa, объединив усилия с Europay и MasterCard, разработала индустриальный стандарт EMV (Europay, MasterCard, Visa) для платежных чиповых карт с кредитно-дебетовыми приложениями. Использование стандарта EMV означает, что чиповые карты будут приниматься в торгово-сервисной сети и банкоматах во всём мире, и в дальнейшем получат такое же широкое распространение как и карточки с магнитной полосой.

Visa также выступила инициатором по созданию единого индустриального стандарта для поддержания нескольких приложений на одной карте с динамическим изменением параметров и количества размещенных приложений. Этот стандарт первоначально получил название Открытая Платформа (OpenPlatform). По мере подключения к работе над этим стандартом для многофункциональных карт все большего количества производителей и других платежных систем, включая AmericanExpress, JCB и MasterCardInternational, эта инициатива Visa переросла в международное объединение, получившее название Глобальная Платформа (GlobalPlatform). Это открытый стандарт, и им могут воспользоваться любые разработчики программного обеспечения, что позволит

увеличить конкуренцию в создании приложений, увеличить их разнообразие и, тем самым, стимулирует быстрое развитие еще большего разнообразия приложений.

VisaSmartDebit/Credit – это основное приложение Visa для чиповых карт. Поскольку это приложение соответствует стандарту EMV, карты с VisaSmartDebit/Credit могут быть использованы в любой стране, в которой есть инфраструктура EMV.

Одним из основных преимуществ использования VSDC заключается в новых расширенных возможностях, открываемых дополнительными приложениями. Это различные бонусные схемы (loyalty), идентификационные приложения (ID), страховки, накопительные схемы и многое другое.

Карты VSDC могут быть использованы при оплате товаров и услуг, при снятии денег в банкомате, совершении безопасных платежей в Интернете, для накопления очков и скидок в магазинах, а также при совершении платежей через мобильные телефоны, компьютер и другие технические устройства.

9.3. Классификация пластиковых карт

1. По материалу, из которого они изготовлены:

- бумажные (картонные);
- пластиковые;
- металлические.

В настоящее время практически повсеместное распространение получили пластиковые карты. Однако для идентификации держателя карты часто используются бумажные (картонные) карты, запаянные в прозрачную пленку. Это ламинированные карты. Ламинирование является довольно дешевой и легкодоступной процедурой и поэтому, если карта используется для расчетов, то с целью повышения защищенности от подделок применяют более совершенную и сложную технологию изготовления карт из пластика. В то же время, в отличие от металлических карт, пластик легко поддается термической обработке и давлению (эмбоссированию), что весьма важно для персонализации карты перед выдачей ее клиенту.

2. На основании механизма расчетов:

- двусторонние системы - возникли на базе двусторонних соглашений между участниками расчетов, при которых владельцы карт могут использовать их для покупки товаров в замкнутых сетях, контролируемых эмитентом карт (универмаги, бензоколонки и т. д.);

- многосторонние системы - предоставляют владельцам карт возможность покупать товары в кредит у различных торговцев и организаций

сервиса, которые признают эти карты в качестве платежного средства. Многосторонние системы возглавляют национальные ассоциации банковских карт, а также компании, выпускающие карты туризма и развлечений (например, AmericanExpress).

3. По виду проводимых расчетов:

- *кредитные* карты, которые связаны с открытием кредитной линии в банке, что дает возможность владельцу пользоваться кредитом при покупке товаров и при получении кассовых ссуд;

- *дебетовые* карты предназначены для получения наличных в банковских автоматах или для получения товаров с расчетом через электронные терминалы. Деньги при этом списываются со счета владельца карты в банке. Дебетовые карты не позволяют оплачивать покупки при отсутствии денег на счете. Преимущество дебетовой карты перед кредитной состоит в отсутствии ограничений на размер одного платежа.

Иногда выделяют в особую категорию платежные карты (chargecard) как разновидность кредитных карт. Отличие состоит в том, что общая сумма долга при использовании платежной карты должна погашаться полностью в течение определенного времени после получения выписки без права продления кредита.

4. По характеру использования:

- индивидуальная карта, выдаваемая отдельным клиентам банка, может быть «стандартной» или «золотой»; последняя выдается лицам с высокой кредитоспособностью и предусматривает множество льгот для пользователей;

- семейная карта, выдаваемая членам семьи лица, заключившего контракт, который несет ответственность по счету;

- корпоративная карта выдается организации (фирме), которая на основе этой карты может выдать индивидуальные карты избранным лицам (руководителям или ценным сотрудникам). Им открываются персональные счета, «привязанные» к корпоративному карточному счету. Ответственность перед банком по корпоративному счету имеет организация, а не индивидуальные владельцы корпоративных карт.

Выделяют иногда карточки туризма и развлечений (travelandentertainmentcards). Они выпускаются компаниями, специализирующимися на обслуживании указанной сферы, например AmericanExpress. Карточки принимаются сотнями тысяч торговых и сервисных предприятий во всем мире для оплаты товаров и услуг, а также предоставляют владельцам различные льготы по бронированию авиабилетов, номеров в гостиницах, страхованию жизни, скидки с цены товара и т. д.

Главные отличия этого вида карт от банковских кредитных карт заключаются, во-первых, в отсутствии разового лимита на покупки и, во-вторых, в обязанности

владельца карты погасить задолженность в течение месяца без права пролонгировать кредит. В случае просрочки платежа с владельца карты взимается повышенный процент.

Еще выделяют чековые гарантийные карты (chequeguaranteecards). Эти карты выдаются владельцу текущего счета в банке для идентификации чекодателя и гарантии платежа по чеку. Карта базируется на кредитной линии, которая позволяет владельцу счета пользоваться кредитом по овердрафту.

5. По способу записи информации на карту:

- графическая запись;
- эмбоссирование;
- штрих-кодирование;
- кодирование на магнитной полосе;
- чип;
- лазерная запись (оптические карты).

Самой ранней и простой формой записи информации на карту было и остается графическое изображение. Оно до сих пор используется во всех картах, включая самые технологически изощренные. Вначале на карту наносились только фамилия, имя держателя карты и информация о ее эмитенте. Позднее на универсальных банковских картах был предусмотрен образец подписи, а фамилия и имя стали эмбоссироваться (механически выдавливаются).

Эмбоссирование (emboss) - нанесение данных на карточке в виде рельефных знаков. Это позволило значительно быстрее оформлять операцию оплаты картой, делая оттиск на ней слипа. Информация, эмбоссированная на карте, моментально переносится через копировальную бумагу на слип. В целях борьбы с мошенничеством могут использоваться слипы и без копировального слоя, но способ переноса эмбоссированной на карте информации, в сущности, остался прежним - механическое давление. Эмбоссирование не вытеснило полностью графическое изображение.

Штрих-кодирование - запись информации на карту с помощью штрих-кодирования применялась до изобретения магнитной полосы и в платежных системах распространения не получила.

Магнитные карты имеют тот же самый вид, что и обыкновенные пластиковые карты, только на обратной стороне карты имеется магнитная полоса. Магнитная полоса может хранить около 100 байт информации, которая считывается специальным считывающим устройством. Информация, содержащаяся на магнитной полосе, совпадает с записями на передней стороне карты: имя, номер счета владельца карты и дата окончания действия карты. Магнитные карты обычно используются как кредитные карты (типа VISA, MasterCard, EuroCard,

AmericanExpress)), как банковские дебетовые карты, карты для банкоматов, а также как телефонные кредитные карты.

Магнитная запись является одним из самых распространенных на сегодняшний день способов нанесения информации на пластиковые карты. Но сейчас уже ясно, что магнитная полоса не обеспечивает необходимого уровня защиты от подделок. А это является критическим моментом в платежных системах, основанных на картах.

Карты памяти выглядят так же, как обычные пластиковые карты, за исключением того, что они имеют встроенную микросхему. Карты памяти часто называют смарт-картами, но само их название говорит о том, что микросхема карты содержит только запоминающее устройство. Объем памяти обычной карты составляет приблизительно 256 байт, но существуют карты с объемом памяти от 32 байт до 8 Кбайт. Уровень защиты этих карт не очень высок, поэтому они используются в прикладных системах, которые не требуют значительного уровня защиты информации, например для оплаты телефонных разговоров. Наибольшее распространение получили европейские телефонные карты типа используемых во Франции и Германии. Приобретаемая телефонная карта позволяет сделать определенное число звонков, соответствующее числу «единиц». Одна единица соответствует одному местному телефонному звонку. Карта вставляется в разъем телефонного аппарата, на диске которого показывается число оставшихся единиц. По мере использования карты число оставшихся единиц уменьшается. Когда карта полностью израсходована, ее выбрасывают. Телефонные карты используются для рекламы.

Смарт-карты внешне похожи на карты памяти, однако в микросхему смарт-карты включена «логика» (микропроцессор), что и делает эти карты «интеллектуальными». Название «смарт-карта» (smart - интеллектуальная, или разумная) связано с возможностью последней выполнять весьма сложные операции по обработке информации. Микросхемы смарт-карты представляют собой полные микроконтроллеры (микрокомпьютеры). В действительности смарт-карта представляет собой небольшой компьютер, способный выполнять расчеты подобно персональному компьютеру. Смарт-карты имеют различную емкость. Смарт-карты дороже карт памяти и их стоимость определяется стоимостью микросхемы, которая прямо зависит от размера имеющейся памяти.

9.4. Развитие рынка пластиковых карточек в РБ

Банковская пластиковая карточка в Республике Беларусь является платежным инструментом, обеспечивающим доступ к банковскому счету и проведение безналичных платежей за товары и услуги, получение наличных денежных средств и осуществление иных операций в соответствии с законодательством Республики Беларусь.

В соответствии с Банковским кодексом Республики Беларусь выпуск банковских пластиковых карточек в обращение осуществляется банками–эмитентами. Операции с использованием банковских пластиковых карточек проводятся банками–эмитентами в пределах полномочий, предоставленных имеющимися у них лицензиями Национального банка Республики Беларусь и в соответствии с Инструкцией о порядке совершения операций с банковскими пластиковыми карточками, утвержденной постановлением Правления Национального банка Республики Беларусь от 30.04.2004 № 74.

На 1 июля 2011 года 24 банка Республики Беларусь эмитируют банковские пластиковые карточки внутренних, международных и внутренних частных и международных частных платежных систем:

- ОАО "Белагропромбанк";
- ОАО "БПС–Банк";
- ОАО "АСБ Беларусбанк";
- ОАО "Белинвестбанк";
- "Приорбанк" ОАО;
- ОАО "Белвнешэкономбанк";
- ОАО "Паритетбанк";
- ОАО "БНБ–Банк";
- ОАО "Белгазпромбанк";
- ЗАО "РРБ–Банк";
- ЗАО "МТБанк";
- ОАО "Технобанк";
- "Франсабанк" ОАО;
- ЗАО "Трастбанк";
- ЗАО Банк ВТБ (Беларусь);
- ЗАО "Альфа–Банк";
- ОАО "Банк Москва–Минск";
- ЗАО "Дельта Банк";
- ЗАО "Кредэксбанк";
- ОАО "ХКБанк";
- ЗАО "БТА Банк";
- ЗАО "БелСвиссБанк";
- ЗАО "АКБ "БЕЛПРОСБАНК";
- Национальный банк Республики Беларусь
- (только для работников системы НБРБ)

Количество банковских пластиковых карточек, находящихся в обращении по состоянию на 1 июля 2011 года составило 9 672,0 тыс., в том числе 3 777,8 тыс. карточек системы "БелКарт", 5 894,4 тыс. карточек международных систем расчетов, 32 карточки внутренних частных систем расчетов и 530 карточек международных частных систем расчетов.

В Республике Беларусь установлено 3 192 банкомата, 3 015 инфокиосков и 83 импринтера, 21 799 организаций торговли (сервиса) оснащены 34 573 платежными терминалами.

За 2 квартал 2011 года на территории Республики Беларусь осуществлена 140 841 271 операция с использованием банковских пластиковых карточек в белорусских рублях на сумму 20 123 271 млн. рублей. Удельный вес безналичных операций в общем количестве операций с использованием банковских пластиковых карточек составил 55,4%, а в суммарном выражении – 14.2%.

Общее количество операций в иностранной валюте за 2 квартал 2011 года составило 1 137 807 операций на сумму 467 445,3 тыс. долларов США. Удельный вес безналичных операций в общем количестве операций с использованием карточек в иностранной валюте составил 18,03%, а в суммарном выражении – 8.8%.

Перечень систем расчетов с использованием банковских пластиковых карточек

1. Внутренняя система "БелКарт"
2. Международная система "MASTERCARD"
3. Международная система "VISA"
4. Международная система "UnionCard"
5. Международная система "DinersClub"
6. Международная система "JCB"
7. Внутренняя частная система "Трастбанк"
8. Международная частная система АО банк "Снорас"
9. Международная частная система "STBcard"
10. Международная частная система "Золотая корона"
11. Международная частная система "БелИнвестБанк-Ликард"

9.5. Инфраструктура приема карточек к обслуживанию

Опыт развития платежных систем на основе карточек в Европе показывает, что наибольшего эффекта от их внедрения в отдельном взятом государстве можно достигнуть только при создании единого в масштабе государства информационного пространства, использующего карточные продукты различных систем, как внутренних, так и международных.

Такие системы действуют в настоящее время во Франции, Дании, Испании, Португалии, Австрии, Финляндии и в стадии построения, практически, во всех странах Европы.

В европейских странах развитие платежных систем на основе пластиковых карточек имеет следующие тенденции:

- движение к совместимости и взаимному дополнению различных карточных продуктов для обеспечения безналичных форм расчетов во всем спектре потребительских сделок;
- интеграция традиционных и современных, основанных на новых технологиях, сегментов рынка карточных продуктов. Совмещение логотипов;
- построение в пределах государства единых платежных инфраструктур, обслуживающих клиентов (резидентов и нерезидентов) с помощью всего спектра карточных продуктов, обеспечивая максимальное удобство и минимальные риски для всех участников расчетов.

Банкоматы

Банкоматы - банковские автоматы для выдачи наличных денег при операциях с пластиковыми карточками. Банкомат позволяет держателю карточки получать информацию о текущем состоянии счета и проводить операции по перечислению средств с одного счета на другой (например, производить оплату коммунальных услуг и услуг операторов сотовой связи).

Первый банкомат (АТМ – Automatic teller machine) в мире был запущен банком Barclays Bank в Северном Лондоне 27 июня 1967 г. Он мог выдавать только десятифунтовые купюры. Лишь через два года банкоматы появились в Америке: в 1969 г. первый из них (производитель - корпорация Docutel) был установлен банком Chemical Bank в нью-йоркском районе Лонг-Айленд. На территории бывшего СССР первые банкоматы были установлены в системе "Дельта-Банк" сначала в Киеве (1991 г.), а затем (1993 г.) - в Коломенском и Мещанском отделениях Московского Сбербанка (производитель - фирма Olivetti, поставщик - фирма IBS).

Общая схема работы

Банкомат - это не только устройство для выдачи денег, но также устройство для обработки информации. На первый взгляд - у банкомата простейшие функции: считать карточку, выдать деньги, напечатать чек. Однако только перечень возможных операций банкомата показывает, что это далеко не так. Кроме того, банкомат должен быть запрограммирован так, чтобы быть абсолютно предсказуемым и абсолютно надежным. Компьютер банкомата не имеет права "зависать" или не обрабатывать каких-либо сигналов.

Любой фирмой-производителем поставляется специальное программное обеспечение к банкомату - библиотека базовых программных модулей для написания собственной прикладной системы или для непосредственного использования в банкоматах и (крайне редко) для использования в центральных компьютерах, управляющих банкоматами.

Сообщения, которые приходится обрабатывать компьютеру банкомата, весьма разнообразны. Соответственно различны и задачи, которые решаются компьютером в многозадачном режиме:

- идентификация и проверка правильности введенного PIN-кода,
- обработка сигналов от большого числа датчиков,
- постоянный автоматический контроль всех внутренних и внешних соединений,
- контроль расхода бумаги в принтере и купюр в депозитных кассетах,
- анализ на разрыв электрических соединений в момент выдачи купюр,
- реакция на "нештатные" механические воздействия,
- фиксация факта изъятия денег или "забывчивости" клиента,
- распознавание кодов разных платежных систем и переключение контуров обработки клиентских сообщений,
- сеансовый и внеплановый вызов центрального компьютера.

Кроме того, компьютер банкомата постоянно генерирует некоторые важные команды: выбрать режим авторизации (ON-Line или OFF-Line в зависимости от запрашиваемой суммы и наличия необходимой информации в базе данных компьютера), выдать деньги, вывести информацию на пользовательский экран, послать запрос на центральный компьютер, арестовать карточку, находящуюся в стоп-листе (списке карточек, права пользования которыми аннулированы). Поэтому неудивительно, что внутренний компьютер в банкомате должен быть весьма мощным.

На сегодняшний день большинство моделей рассчитано на работу в on-line режиме с карточками с магнитной полосой, однако появились и устройства, способные работать со смарт-картами и в off-line режиме.

Любой банкомат, где бы он ни находился, соединен с вычислительным центром (процессингом), который осуществляет управление данной сетью банкоматов. Сеть может принадлежать как конкретному банку, так и независимому поставщику услуг.

Когда вы вставляете в банкомат карту, вводите свой пин-код и выбираете требуемую операцию, запрос посылается в процессинг, который перенаправляет его в соответствующий банк или финансовое учреждение, выпустившее вашу карточку. Если вы хотите снять деньги, то процессинг осуществляет электронный перевод требуемой суммы с вашего банковского счета на свой. Как только перевод осуществлен, вычислительный центр посылает банкомату команду на выдачу денег.

Таким образом, схема работы банкоматов в целом аналогична предоставлению услуг Интернета. Когда вы хотите получить доступ в Интернет, то соединяетесь с сервером провайдера, который, в свою очередь, перенаправляет вас на другие сервера, хранящие необходимую вам информацию.

Для связи банкомата с процессингом используются специально построенная сеть на основе оптоволокну, простые телефонные линии, подключение к которым производится через модем, выделенные линии. Кроме того, есть банки, которые используют в качестве средства связи радиомодемы.

В вычислительный центр банкомат передает не только запросы клиентов, но и все сведения о своей работе, которые отслеживаются оператором. Во-первых, банкомат заблаговременно предупреждает процессинг о необходимости обслуживания - скажем, в машине закончились деньги или произошел сбой в работе системы. Во-вторых, в вычислительный центр поступают все сообщения об ошибках. В этом случае процессинг определяет, носит ли ошибка фатальный характер и работу банкомата следует немедленно прекратить, или же неисправность можно "обойти". Например, если сломался чековый принтер, то банкомат может вывести на экран сообщение об отсутствии бумаги и предложить клиенту продолжить выполнение операции.

Правила получения наличных в банкоматах имеют общие принципы. Тип банкомата и банк, установивший АТМ, лишь предлагают свою вариацию последовательности действий при получении денег.

Внутреннее устройство

Банкомат состоит из двух основных частей: верхней, пользовательской, и нижней, сейфа. По назначению, банкоматы делятся на офисные, уличные, черезстенные и автострадные. Офисные банкоматы устанавливаются в помещениях, уличные предназначены для использования на улице, а черезстенные могут устанавливаться через перегородку как внутри здания, так и снаружи. В случае с черезстенной моделью, клиент видит перед собой банкомат или целиком, или ему доступна только лицевая панель. Подобное разграничение произведено по соображениям безопасности: если бы на улице банкоматы размещали целиком, потенциальному злоумышленнику было бы проще получить доступ к сейфу. Кроме того, замена денег сопрягалась бы с большой опасностью. Автострадные банкоматы должны выдерживать лобовой наезд тяжелого грузовика.

Обязательными элементами каждого банкомата являются:

- IBM-совместимый компьютер с многозадачной операционной системой,
- специальное или комбинированное устройство считывания магнитных, оптических или интеллектуальных карточек,
- устройство выдачи купюр.

Все эти составные элементы заключены в единый сейфовый корпус.

В устройствах выдачи купюр вначале появились вакуумные механизмы. Затем компания DeLaRue применила принципиально новый фрикционный механизм

работы с купюрами. Практика показала, что фрикционные механизмы DeLaRue отличаются более высокой точностью обработки денежных знаков.

Предназначенные для выдачи купюры хранятся в специальных кассетах. Эти кассеты хотя не так защищены, как сейфы, но могут быть вскрыты только на специальном оборудовании.

Кассет в банкомате может быть несколько, стандартно - от двух до пяти. Разные депозитные кассеты могут использоваться как для купюр разных номиналов, так и для разных валют.

Важное значение в банкоматах имеет так называемая "возвратная" или "отказная" кассета. Туда помещаются замятые или потертые купюры, неправильно отсчитанные, отбракованные в процессе выдачи, а также забытые клиентом. Если система "подозревает", что что-то не так, она автоматически сбрасывает купюры в отказную кассету и средства со счета клиента не списываются.

Банкоматы могут комплектоваться дополнительным оборудованием: принтер со специальной бумагой, фотокамера и мультимедиа-оборудование для прямых консультаций с банковским служащим с помощью экрана, клавиатура для программирования, блок автономного питания, криптопроцессор и многое другое.

В нижней части банкомата расположен диспенсер - устройство для выдачи денег (заметим, что диспенсером называют также и само окошко выдачи). Деньги загружаются в диспенсер в специальных кассетах. Объем кассеты колеблется от двух до трех тысяч банкнот. Как правило, кассеты заполняются валютой полностью, чтобы не приходилось слишком часто обслуживать банкомат. Диспенсеры могут иметь двух-, трех-, четырех- и пятикассетную конфигурацию. То, какими именно деньгами будут заполнены кассеты, зависит от банка, так как их можно настроить для банкнот любого типа посредством задания длины и ширины банкноты. Подчеркнем, что в одну кассету можно загрузить банкноты только одного номинала.

После того, как деньги загружены в кассету, она закрывается специальным ключом, пломбируется и выдается инкассаторам, которые выезжают на место, вынимают прежние кассеты и вставляют новые. Как правило, инкассация занимает от 15 минут до получаса: банкомат тестирует все свои устройства, проверяет, есть ли в кассетах деньги и имеется ли связь с процессингом. Только после этого на экран выводится приветственное сообщение.

Как только кассета вставлена в диспенсер, она приводится в рабочее положение: крышка откидывается, а деньги прижимаются к фидеру, устройству, предназначенному для "снятия" банкнот. У каждой кассеты свой фидер. Если банкнота идет из самой нижней кассеты, она проходит через все имеющиеся фидеры. В том случае, если за одной банкнотой случайно зацепилась вторая, фидер возвращает ее на место.

Затем банкнота проходит через устройство DoubleDetect, предназначенное для проверки поступающих банкнот на соответствие запросу: того ли они размера, правильная ли у них толщина, нет ли перекоса. Это осуществляется при помощи специальных датчиков. После этого банкноты попадают в дивертер, который, если все в порядке, отправляет их в накопительное устройство (стакер), а если что-то не так - сбрасывает в режект-кассету или, по-другому, диверт-кассету.

Режект-кассета специально предназначена для сброса денег. Туда поступают банкноты, по тем или иным причинам отбракованные диспенсером. Это рваные, истертые, слипшиеся банкноты или банкноты с загнутым краем. Во время выдачи денег может отключиться электричество или произойти какой-либо сбой - в этом случае набранная сумма денег также сбрасывается в режект-кассету. Наконец, клиент может просто забыть деньги в окошке выдачи или не взять их вовремя - некоторые модели банкоматов автоматически забирают деньги обратно через определенный промежуток времени. В современных банкоматах, по соображениям удобства, режект-кассета состоит из двух частей: в одну из них сбрасываются "хорошие" деньги, в другую - бракованные. Если диспенсер отбраковывает слишком много банкнот, это говорит о наличии неполадки.

Когда в стакере набирается запрашиваемая сумма, она поступает в собственно устройство выдачи денег.

Следует отметить, что датчики сопровождают банкноту на всем протяжении ее пути, от выхода из кассеты до выхода из диспенсера. Предположим, фидер зафиксировал, что банкнота вышла из кассеты. Если она вовремя не попадет в стакер, будет зафиксирована ошибка. Это обеспечивает принципиальную невозможность выдачи вам не той суммы денег.

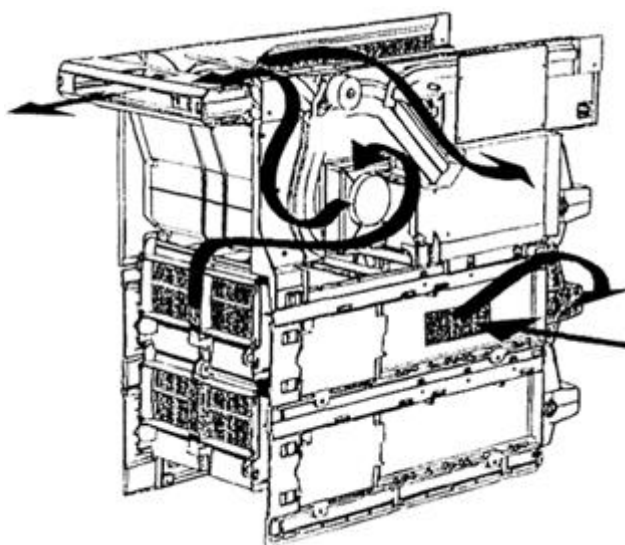


Рис. 1. Так происходит движение купюры в банкомате.

Теперь обратимся к верхней части банкомата, в которой расположена его электронная начинка. Главный компонент здесь, конечно же, компьютер. В современных банкоматах компьютеры работают под управлением современных операционных систем, таких как Windows, Linux . Кроме компьютера, в верхней части расположено устройство для приема и считывания кредитных карт (кард-ридер), чековый и журнальный принтеры. Первый принтер предназначен для выдачи вам чеков, а на ленте второго фиксируется все, что происходит с банкоматом.

Владелец банкомата обязан хранить эту информацию в течение двух лет. Если у клиента возникли какие-либо сомнения относительно произведенной операции, он всегда может запросить журнал за нужный период. Последние модели банкоматов оснащаются графическими принтерами, некоторые из которых позволяют даже распечатывать информацию на бумаге формата А4 - это позволяет широко использовать банкоматы при проведении маркетинговых акций.

Также в верхней части расположен защитный модуль, устройство, кодирующее информацию, так как передача пин-кода карточки в процессинговый центр осуществляется только в закодированном виде. Наконец, упомянем прочие, уже непосредственно видимые пользователю устройства: монитор, клавиатура, динамик и световые индикаторы.

В моменты простоя банкомата монитор обычно показывает рекламу. Современные банкоматы оснащаются плоскими цветными мониторами с антибликовым покрытием, что не только делает приятным работу с ними, но и повышает эффективность демонстрируемой рекламы. Экран монитора может быть сенсорным - в этом случае функциональная клавиатура устанавливается по желанию заказчика.

Кроме банкоматов, предназначенных только для выдачи наличных денег, существуют также полнофункциональные терминалы банковского самообслуживания, позволяющие не только снимать деньги со счета, но и зачислять их, производить переводы со счета на счет и выполнять другие операции.

Зачисление средств производится при помощи специального модуля - депозитора. Вы вводите необходимую информацию, депозитор выдает вам специальный конверт, в который вы кладете деньги, а затем бросаете конверт в окошко устройства. Ряд последних моделей позволяет принимать деньги уже без посредства конверта, автоматически проверяя их на подлинность. Кроме того, депозиторы могут обрабатывать чеки (интеллектуальные депозиторы).

Безопасность

Безопасность важна, прежде всего, для владельца банкомата. Во-первых, защиту денег от воров обеспечивает сейф, который имеет толстые металлические стенки

и кодовый замок. Обычно сейф весит где-то полтонны, а вес особо защищенных дорогих сейфов может достигать полутора тонн, что делает проблематичным не только их взлом, но и увоз при помощи миникрана (были и такие случаи). Одно время выпускались облегченные варианты сейфов с тонкими стенками, которые можно пробить отверткой, - они были дешевы, но обеспечивали минимальный уровень защиты.

Затем, банкоматы могут оснащаться сигнализацией и видеокамерой. В случае несанкционированного проникновения внутрь сейфа в кассете может происходить разбрызгивание чернил, окрашивающих купюры.

Чтобы обслужить банкомат, инкассаторы, кроме кода доступа к сейфу, должны иметь при себе специальный ключ (ключ оператора) для доступа к интерфейсной программе, так как вынуть и вставить кассеты, не дав соответствующей команды компьютеру, нельзя. Функции, доступные обслуживающему персоналу при наличии этого ключа, строго ограничены. Доступом собственно к операционной системе с возможностью менять настройки банкомата имеет только программист, обладающий своим собственным ключом.

Для клиентов также предусмотрены несколько уровней безопасности. Пин-код карточки разрешается вводить только три раза. Если введенный в третий раз пин-код неверен, карточка удерживается банкоматом и попадает в расположенный сзади кард-ридера контейнер. Остается в банкомате карточка и в том случае, если пропало электричество или произошел какой-нибудь другой сбой, хотя обычно устройства бесперебойного питания обеспечивают выполнение, по крайней мере, текущей операции.

Кроме того, некоторые модели банкоматов оснащаются зеркалами заднего обзора, чтобы клиент видел происходящее за его спиной, видеокамерами, специальным покрытием экрана, защищающим от подглядывания и шифрующей клавиатурой.

POS – терминалы и POS - системы

POS - терминалы (PointofSale) - это специальное электронное банковское оборудование, устанавливаемое рядом с кассовым аппаратом торгово-сервисного предприятия и позволяющее считывать информацию с магнитной полосы или чипа карточки и осуществлять связь с банком для проведения авторизации с целью осуществления операции по банковской карточке.

POS-терминалы, или торговые терминалы, предназначены для обработки транзакций при финансовых расчетах с использованием пластиковых карточек с магнитной полосой и смарт-карт. Использование POS-терминалов позволяет автоматизировать операции по обслуживанию карточки и существенно уменьшить время обслуживания. Возможности и комплектация POS-терминалов варьируются в широких пределах, однако типичный современный терминал снабжен устройствами чтения как смарт-карт, так и карт с магнитной полосой,

энергонезависимой памятью, портами для подключения ПИН-клавиатуры (клавиатуры для набора ПИН-кода), принтера, соединения с ПК или с электронным кассовым аппаратом.

Стоимость POS-терминалов в зависимости от комплектации, возможностей фирмы-производителя может меняться от нескольких сотен до нескольких тысяч долларов, однако обычно не превышает полутора - двух тысяч. Размеры и вес POS-терминала сопоставимы с аналогичными параметрами телефонного аппарата, а зачастую бывают и меньше.

В настоящее время инфраструктура на основе терминального оборудования довольно быстро развивается. Ведущие банки Республики Беларусь готовы предложить держателям платежных карт возможность рассчитываться за приобретаемые товары или услуги практически без использования наличных денег. Данная услуга постепенно привлекает к себе "осторожного" клиента, обращая на себя внимание своей простотой, надежностью и комфортом. Отсутствие дополнительного комиссионного сбора - еще один большой плюс для безналичных расчетов. Держатель пластиковой карточки одного банка может расплачиваться в магазине, где установлен POS-терминал другого банка. Эта услуга для него будет оказана без снятия дополнительного процента.

Фискальный регистратор (ФР) - это контрольно-кассовая машина, способная работать только в составе компьютерно-кассовой системы, получая данные через канал связи.

На базе фискального регистратора можно создать POS-систему рабочее место продавца-кассира, которое будет представлять собой компьютер с программным обеспечением для учета продаж и управления фискальным регистратором и набор дополнительного оборудования.

Фискальные регистраторы различаются принципом печати. Более популярный вид фискальных регистраторов ФР с термопечатью. Данный способ печати не требует красящего картриджа, он быстрее матричной печати и практически бесшумен. У многих ФР имеется встроенный автоматический резак, позволяющий разделять чеки.

POS-системы - это аппаратные комплексы для автоматизации работы кассиров на базе фискальных регистраторов. Обычно в состав POS-системы входит системный блок ПК, фискальный регистратор (ФР), POS-монитор кассира, денежный ящик, программируемая клавиатура, карт ридер (cardreader) и дисплей покупателя. Все эти составные модули, интегрированные вместе, представляют собой законченное рабочее место кассира. Одно из отличий POS-системы от POS-терминала состоит в том, что модуль фискальной памяти у POS-системы находится в печатающем устройстве, а именно, в фискальном регистраторе. У POS-терминала модуль фискальной памяти находится внутри корпуса компьютерного блока. С этим связана еще одна особенность применения POS-

систем и POS-терминалов. POS-терминалы могут продаваться только с определенными специализированными кассовыми программами. Для POS-систем не требуется сертификация программного обеспечения, т.к. все необходимое для фискального учета программное обеспечение (ПО) записано во внутренней памяти печатающего устройства - фискального регистратора.

Инфокиоски

Информационные терминалы (инфокиоски) - специальное банковское оборудование, предназначенное только для предоставления информационно-справочных услуг населению.

В разных отраслях экономики технологии самообслуживания получают все большее распространение — электронные информационно-справочные терминалы стали неотъемлемой частью информационной инфраструктуры современных аэропортов и вокзалов, а в крупнейших розничных магазинах уже давно применяются информационные терминалы, позволяющие покупателю по штрих-кодам товаров получить дополнительную информацию, рассчитать общую стоимость покупок и даже самостоятельно произвести оплату.

Основной причиной и целью внедрения технологий самообслуживания является снижение расходов на проведение операций по обслуживанию клиентов. Подсчитано, что в банках США, например, стоимость одной операции по выдаче наличных, осуществленной традиционно, через операциониста, в четыре раза дороже, чем такая же операция, произведенная в банкомате.

Все многообразие современных средств самообслуживания подчиняется общим правилам проектирования и изготовления. Любой терминал самообслуживания всегда имеет интерфейс с клиентом, как правило, это экран с текстовой и/или графической информацией. Для ввода запроса от клиента используется специальная клавиатура либо (особенно в современных устройствах) — тактильный (сенсорный) экран. Если от клиента необходимо получать не только запросы, но и данные (персональный код, фамилия, номер счета и проч.), то используется дополнительная клавиатура, в банковских устройствах — с шифрованием вводимой информации.

До недавнего времени, пока не существовало международных стандартов на устройства и программное обеспечение для оборудования самообслуживания, на рынке было представлено несовместимые друг с другом устройства различных производителей. При этом такие устройства способны были предложить только ведущие мировые компании, поскольку каждый терминал или банкомат проектировался и изготавливался практически «с нуля», что требовало существенных затрат. Все это неизбежно сказывалось на конечной стоимости самих устройств.

Сейчас, когда повсеместно приняты стандарты сопряжения модулей в устройствах самообслуживания и такие стандартизованные модули широко доступны на рынке, стало возможным проектировать и изготавливать оборудование самообслуживания с гораздо меньшими затратами при условии наличия развитой технологической и конструкторской базы, как, например, в нашей стране. Стоимость таких устройств в несколько раз меньше, чем у изделий мировых лидеров, а функциональность зачастую и выше.

В последнее время количество установленных АСБ "Беларусбанк" платежно-справочных терминалов самообслуживания (инфокиосков) превысило 200 устройств. Инфокиоски являются эффективным и удобным инструментом для предоставления держателям пластиковых карточек высококачественного банковского сервиса.

К настоящему времени в инфокиосках Беларусбанка с помощью пластиковой карточки можно всего за несколько секунд оплатить услуги операторов мобильной связи VELCOM, МТС, БелСел; услуги интернет-провайдера "Атлант Телеком", коммунальные услуги, услуги связи РУП "Белтелеком"; погасить задолженность по кредиту в белорусских рублях, выданному в любом учреждении АСБ "Беларусбанк"; услуги спутникового телевидения "Космос-ТВ"; зарегистрировать услугу SMS-банкинг.

Платежно-справочный терминал Cash-In

21 марта 2006 года Приорбанк впервые в Беларуси запустил в промышленную эксплуатацию платежно-справочный терминал с функцией приема наличных денежных средств (Cash-In) с последующим зачислением на карт-счета, открытые в "Приорбанк" ОАО.

Теперь держатели дебетовых и кредитных карточек Приорбанка имеют возможность внести средства в белорусских рублях или в долларах США на свой карт-счет. Денежные средства станут доступны им уже через 1 час после внесения.

В настоящий момент помимо внесения денег на карт-счет в терминале реализованы следующие функции: просмотр баланса по карточке, а также получение информации о размере платежа по кредитной карточке, который должен быть сделан в текущем месяце.

Первый платежно-справочный терминал с функцией Cash-In белорусского производителя ЗАО "Международный деловой альянс" установлен и функционирует в ЦБУ 115 по ул. Кропоткина, 91.

В конце марта был установлен второй терминал в городе Гомеле по ул. Красноармейская, 3а (здание ГФ по Гомельской области "Приорбанк" ОАО).

ТЕМА 10: НАЦИОНАЛЬНАЯ СИСТЕМА МЕЖБАНКОВСКИХ БЕЗНАЛИЧНЫХ РАСЧЕТОВ НА ОСНОВЕ ПЛАТЕЖНЫХ КАРТОЧЕК «БЕЛКАРТ»

10.1. Основные понятия и принципы построения системы

Основная задача системы «БелКарт» состоит в широком распространении среди населения республики карточек, как средства платежа и инструмента банковского обслуживания, с целью увеличения доли безналичных расчетов в платежном обороте и дополнительном привлечении средств населения в экономику государства.

Работа над созданием национальной платежной системы с использованием банковских пластиковых карточек по заданию банков началась в марте 1994 года. 26 сентября 1995 года проведена первая финансовая операция.

Органы управления системой "БелКарт":

- Общее собрание акционеров ЗАО "Платежная система "БелКарт";
- Наблюдательный совет ЗАО «Платежная система «БелКарт»;
- Дирекция ЗАО «Платежная система «БелКарт», возглавляемая Генеральным директором.

Членами системы «БелКарт» являются Национальный банк Республики Беларусь и 16 крупнейших коммерческих банков республики.

Основные функции банков-членов системы «БелКарт»:

- выпуск в обращение платежных карточек различных видов для физических и юридических лиц;
- обслуживание предприятий всех форм собственности по заработной плате с помощью карточек;
- обслуживание платежных терминалов предприятий торговли и сервиса, принимающих карточки к безналичной оплате товаров и услуг;
- обслуживание по карточкам клиентов своих и чужих банков по выдаче наличных денег, оплате коммунальных услуг и переводу средств;
- межбанковские расчеты с другими банками-членами системы «БелКарт»;
- информационное и сервисное обслуживание держателей карточек.

«БелКарт» - это комплексная система, включающая в себя все атрибуты платежных систем подобного типа: организационное, правовое, методологическое, информационное, финансово-экономическое и техническое обеспечение, инструменты и методы осуществления расчетов, управления рисками и обеспечения безопасности. «БелКарт» является составной частью национальной платежной системы страны.

Карточка «БелКарт» относится к категории банковских платежных пластиковых карточек и выпускается в обращение банком-членом системы.

Правовая, юридическая и нормативная основа системы «БелКарт» регулируется действующим законодательством Республики Беларусь, нормативными документами Национального Банка, а также документами системы:

1. «Инструкция о порядке совершения операций с банковскими пластиковыми карточками» от 30 апреля 2004 г. N 74. Утверждена Правлением Национального банка Республики Беларусь (рег.N 8/10996 от 19 мая 2004 г.)

2. «Инструкция по бухгалтерскому учету операций с банковскими пластиковыми карточками и электронными деньгами в банках Республики Беларусь» от 14 июля 2004 г. N 222. Утверждена Постановлением Совета директоров НБ РБ (рег.N 8/11301 от 29 июля 2004 г.).

3. «Положение о системе «БелКарт»». Протокол № 4 от 17.01.2005. Утверждено Наблюдательным советом ЗАО «Платежная система «БелКарт».

4. «Положение о процессинге и клиринге в системе «БелКарт». Протокол № 4 от 17.01.2005. Утверждено Наблюдательным советом ЗАО «Платежная система «БелКарт».

5. «Правила проведения операций с использованием банковских пластиковых карточек «БелКарт»» (редакция 26.12.2003).

6. Соглашения между участниками.

Создание единой межбанковской платежной системы обеспечивает следующие преимущества:

- использование единого торгового пространства предприятий торговли и сервиса, принимающих карточки к оплате, а также единой сети банкоматов для выдачи наличных денег;
- унификация карточек для расчетов за товары и услуги;
- нейтральный коммерческий характер сети процессинговых центров;
- единые нормы, правила, процессы и формы документов;
- сокращение рисков и обеспечение безопасности платежной системы;
- единая стратегия и технология взаимодействия с международными платежными системами;
- управляемость платежной системы;
- минимизация затрат на создание системы и поддержание ее в процессе эксплуатации.

Система построена на единой для всех банков - членов системы информационной технологии, включающей в себя инструмент платежа - пластиковую микропроцессорную карточку, специализированное терминальное оборудование, вычислительные комплексы, средства электронной передачи данных, а также необходимое организационное, методологическое, информационное и программное обеспечение.

10.2. Виды участников системы

1. Банки-эмитенты карточек (Issuer), их отделения и филиалы.
2. Банки, обслуживающие ПТС, ПВН (Acquirer), их отделения и филиалы.
3. Предприятия торговли и сервиса (ПТС).
4. Клиенты-держатели карточек.
5. ЗАО «Платежная система «БелКарт» - научно-технический центр, оператор и клиринговый центр платежной системы.
6. Национальный банк Республики Беларусь - участник и расчетный банк системы.

Банки-эмитенты размещают карточки среди населения, предоставляют клиентам услуги и осуществляют расчетные операции по карт-счетам.

Банки, обслуживающие ПТС, подключают к себе терминалы и обслуживают предприятия торговли и сервиса по основным базовым процессам (авторизация, блокировка, сбор и обработка платежей), взаимодействуя с ГКСЦ (РКСЦ) на договорной основе. Для этих целей банки могут организовать собственный банковский КартЦентр (БКЦ), а могут арендовать вычислительные мощности и ресурсы ГКСЦ или РКСЦ в ЗАО «Платежная система «БелКарт».

Предприятия торговли и сервиса (ПТС), оборудованные платежными POS-терминалами, принимают карточки «БелКарт» к оплате за товары и услуги.

Клиенты - держатели карточек - физические лица, члены их семей, а также юридические лица, пользующиеся услугами с помощью банковских карточек «БелКарт».

10.3. Общая структурная организация системы

В системе можно выделить следующие структурные элементы:

- объект управления (сами безналичные расчеты);
- органы управления (банки, процессинговые и расчетные центры, предприятия торговли и сервиса, предприятия разных форм собственности);
- механизм организации и проведения безналичных расчетов (документы организационного, правового, методического, информационного, программного, технического и других видов обеспечения).

Модель системы, отражающая функциональные и информационные связи, приведена на рис. 1.

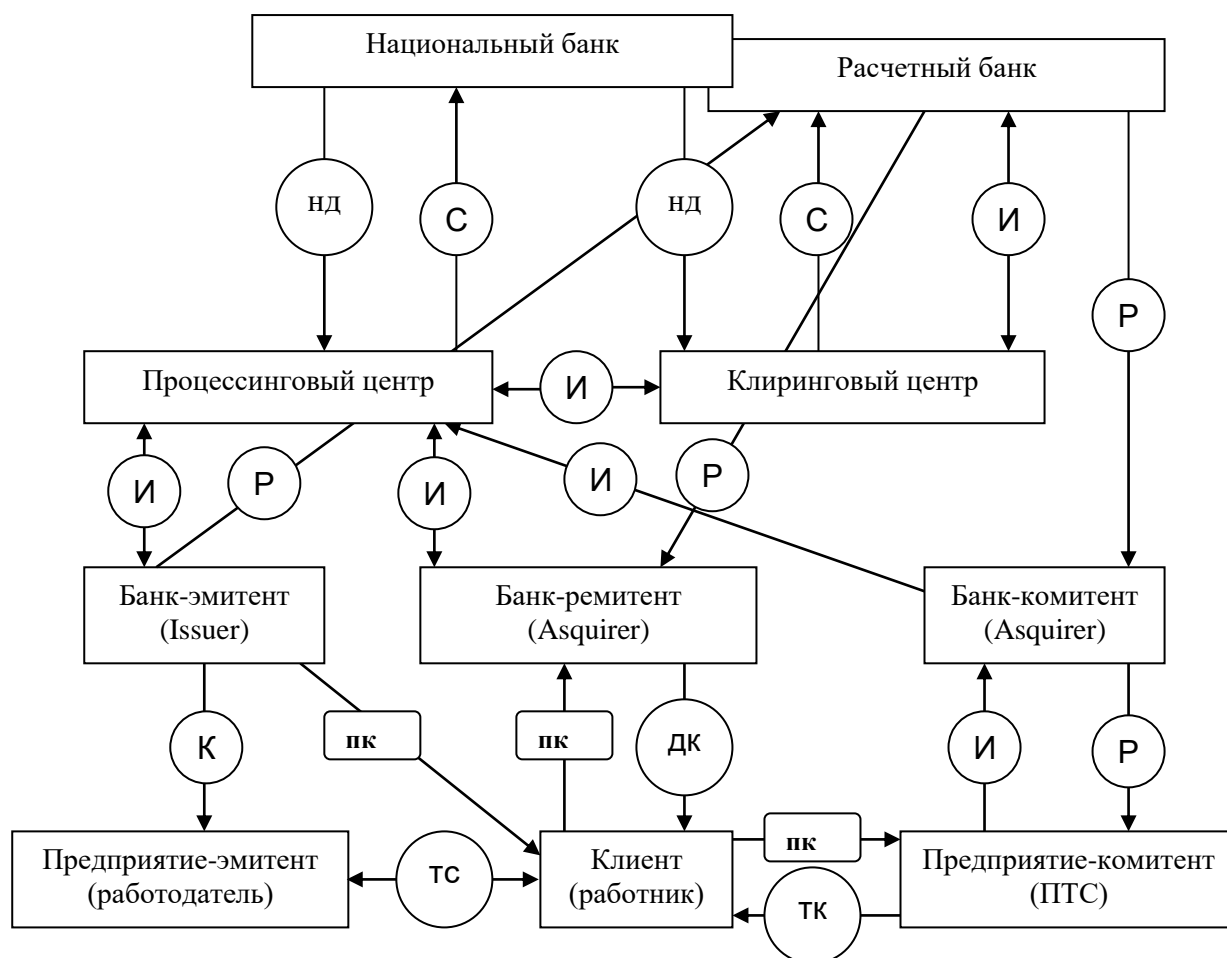


Рис. 1

НД- нормативные документы
карточка

С - статистика и отчетность

И - информация

Р – расчет

К – кредит

ТС - трудовое соглашение

ТК - товарный кредит

ДК - денежный кредит



- платежная

Клиент - платежеспособное или кредитоспособное лицо, получающее доходы от предприятия-эмитента и осуществляющее расчеты с предприятием-комитентом.

Предприятие-эмитент - источник денежных ресурсов клиента в виде заработной платы, стипендий, пособий и т.п.

Предприятие-комитент продает товар и (или) предоставляет услуги безналичными перечислениями со счета клиента в банке-ремитенте.

Банк-эмитент (Issuer) размещает карточки среди клиентов, осуществляет расчетно-кассовое обслуживание предприятий-эмитентов, выполняет безналичные зачисления и отчисления для клиентов от этих предприятий.

Банк-комитент (Acquirer) выполняет расчеты с банками-эмитентами и предприятиями-комитентами за товары и услуги и обслуживание предприятий-комитентов.

Банк-ремитент выполняет налично-денежные операции по карточкам.

Процессинговый центр - предприятие (подразделение), осуществляющее деятельность по организации оперативной работы системы.

Расчетный банк осуществляет расчеты между банками эмитентами, комитентами и ремитентами по операциям, выполненным с помощью банковских платежных карточек.

Структура «БелКарт» представляет собой многоуровневую систему, иерархическая организация которой отражает взаимодействия объектов системы, участвующих в процессе обслуживания по карточкам.

В системе выделяются следующие уровни:

- Первый (нижний) уровень, "Front-end" системы «БелКарт».

Терминалы и комплексы на их основе в ПТС, ПВН. Банкоматы, работающие в автономном режиме.

- Второй уровень, "Front-office" системы «БелКарт». Отделы вкладных операций, электронные кассы, расчетно-кассовые центры банков-эмитентов. Терминалы, работающие в линейном режиме (ППК, функция пополнения в АТМ).

- Третий уровень. "BackOffice" системы «БелКарт». Процессинговые центры. БКЦ, КЦФБ, РКЦ, ГКЦ.

Четвертый уровень. "BackOffice" Национальной Платежной Системы. Национальный банк, банки, ЗАО «Платежная система «БелКарт».

10.4. Информационная модель системы

Информационно-технологическая модель системы отражает основные структурные элементы системы, технологические процессы и процедуры, выполняемые в системе с помощью специальных технических и программных средств по согласованным в рамках единой технологической дисциплины правилам и регламенту. Схема взаимосвязанных процессов, процедур и функций, действующих в системе «БелКарт», приведена на рис. 2.



Рис. 2

Функционально-структурная схема системы представлена на рис.3.

Для организации выпуска карточек в обращение и обслуживания по ним в системе «БелКарт» реализованы объекты нескольких типов:

- ГКСЦ - головной КартСервисЦентр - главный процессинговый центр системы;
- РКСЦ - региональный процессинговый центр;
- БКЦ - банковский КартЦентр;
- КЦФБ - КартЦентр филиала банка;
- РКЦ или ЭК - расчетно-кассовый центр или «электронная касса» банка-эмитента;
- ПТС - предприятие торговли и сервиса с платежным POS-терминалом или ЕСК (электронным кассово-суммирующим аппаратом с функцией безналичной оплаты по карточкам «БелКарт»);
- ПВН - пункт выдачи наличных с POS-терминалом, работающим в операторном режиме или банкоматом (АТМ), работающим в безоperatorном режиме;
- ППК - пункт пополнения и изменения параметров карточек.

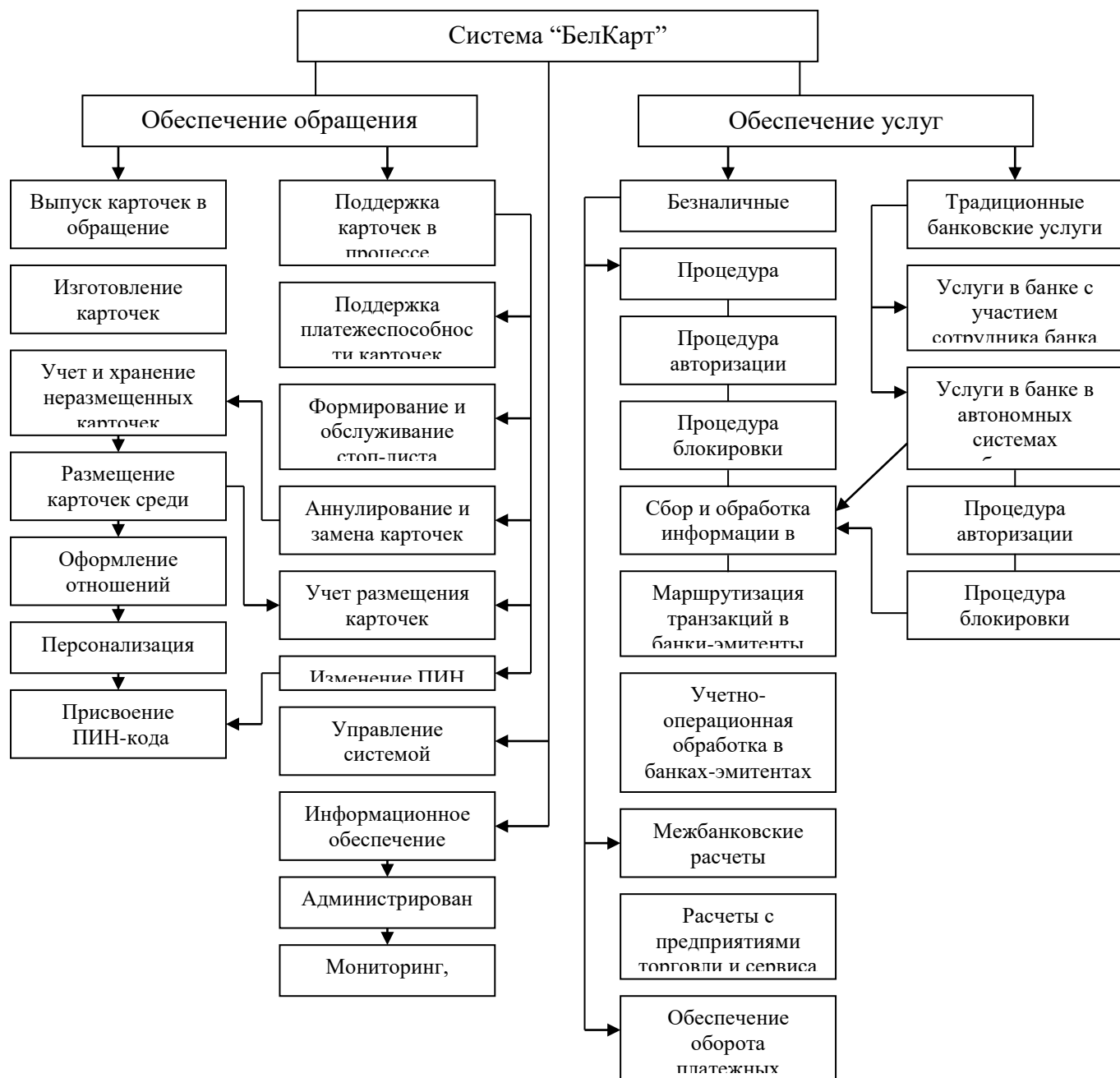


Рис. 3 - Функционально-структурная схема системы

В основе информационной структуры, модели и технологии в системе «БелКарт» лежит микропроцессорная карточка. Карточка «БелКарт» является персонифицированным средством, предназначенным для оплаты товаров и услуг, получения наличных денег и выполнения операций со счетом.

Система «БелКарт» обеспечивает работу с карточками дебетного, кредитного и дебетно-кредитного типа.

Карточка «БелКарт» позволяет клиенту самостоятельно контролировать свои расходы по карточкам, что очень важно, так как при ускоренных сделках держатель теряет ощущение владения денег.

Микропроцессорная карточка делает преимущественным в системе «БелКарт» автономный режим «off-line». Автономный режим предполагает, что терминалы или банкоматы в процессе выполнения операции не соединены с центральным процессором системы, а все действия в момент совершения операции происходят под управлением программного обеспечения микропроцессорной карточки и платежного терминала (банкомата). С использованием «off-line» технологии в системе «БелКарт» совершаются операции оплаты, получения наличных денег, сторнирования платежной операции, автопополнения, изменения ПИН, просмотра остатка средств на карточке. Операции с использованием «off-line» режима требуют связи терминалов с центральной компьютерной системой в режиме реального времени. Терминалы и банкоматы имеют непосредственный доступ к базе данных системы для выполнения запроса и изменения файлов в момент совершения каждой операции. С использованием «off-line» режима производится занесение средств на карточку, удаленное пополнение карточки, возврат средств с карточки на счет, операции выдачи наличных денежных средств в РКЦ клиентам этого же РКЦ, изменение параметров карточки, получение выписки о движении по счету.

Исходя из комбинированной «Off-On/line» технологии, последовательного и протяженного по времени характера подключения банков и их филиалов, постепенного наращивания масштабов эмиссии карточек и развития инфраструктуры, были применены относительно недорогостоящие системные и программно-технические решения, которые обеспечили эмиссию первых карточек в предельно короткие сроки с возможностью наращивания ресурсов (производительности, пропускной способности) по мере роста масштабов системы (числа участников, объектов, услуг и операций) без существенных изменений программно-аппаратной платформы. Принцип централизованной обработки транзакций через единый процессинговый центр не реализовывался ввиду относительно высокой стоимости первоначальных затрат на создание ГКСЦ и организации взаимодействия с объектами системы, проблем с наличием и качеством каналов связи, а также затрат на их эксплуатацию, что привело бы к высоким приведенным затратам на одну транзакцию.

В отличие от обычной, он-лайновой магнитной карточки, микропроцессорная карточка обеспечивает высокозащищенный способ хранения ПИН-кода на самой карточке, защиту данных на карточке от подделки и несанкционированного считывания, а также аудиторский след о сделках - запись результатов выполнения последних 14-ти операций с карточкой.

Карточка «БелКарт» имеет 4 отдельные платежные приложения, которые настраиваются с помощью ряда параметров. Каждая карточка клиента «БелКарт» имеет 3 общих настраиваемых параметра, а также по 20 параметров отдельно для каждого платежного приложения. Для достижения своих целей банк может устанавливать в договорах с клиентом размеры дневных, недельных и т.д. лимитов пополнения и расходования средств с помощью карточки, а также лимитов получения наличных денег. Программное обеспечение карточки позволяет устанавливать независимо для каждого из 4-х платежных приложений следующие параметры и ограничения: период времени действия ограничений (от 1 до 79 дней), количество операций в заданный период времени (от 1 до 99), максимальная сумма отдельной операции, максимальная сумма платежного приложения в целом.

Также может быть установлено ограничение на сумму операции без предъявления ПИН (для ускорения выполнения операций оплаты мелких покупок или услуг, например, оплаты обедов в столовой).

Гибкая система параметризации позволяет настраивать каждую конкретную карточку на ту или иную финансово-экономическую модель, например:

1. Платежное приложение 1 (обслуживание по заработной плате). Период времени - 30 дней, количество операций - 10, общая сумма платежного приложения - не более 500 тысяч рублей, сумма отдельной операции - не более 100 тысяч рублей. Разрешены операции получения наличных денег и оплаты товаров (услуг).

2. Платежное приложение 2 (доплата за питание в ведомственной сети столовых). Период времени - 7 дней, количество операций - 7, общая сумма платежного приложения - не более 50 тысяч рублей, сумма отдельной операции - не более 10 тысяч рублей. Разрешены только операции безналичной оплаты.

3. Платежное приложение 3 (доплата за медицинское обслуживание в ведомственном профилактории). Период времени - 30 дней, количество операций - 5, общая сумма платежного приложения - не более 100 тысяч рублей, сумма отдельной операции - не более 20 тысяч рублей. Разрешены только операции безналичной оплаты.

4. Платежное приложение 4 (средства в кредит под будущую заработную плату). Период времени - 30 дней. Сумма платежного приложения - не более среднего уровня заработной платы работника за последние 0,5 года, например, 150 тысяч рублей. Разрешена операция автопополнения .

В смарт-технологиях используется развитая и гибкая система параметризации самой карточки на уровне собственного прикладного программного обеспечения, которое поддерживает механизм управления рисками (банка, клиента, системы в целом) и обеспечивает оптимальную настройку экономических интересов клиента и банка.

Операционная система микропроцессорной карточки, прикладные и инструментальные программные средства «БелКарт» позволяют адаптировать карточку для новых функций (приложений).

В последние годы система «БелКарт» развивается в соответствии с государственной Программой, одобренной Постановлением Совета Министров Республики Беларусь и Национального банка Республики Беларусь.

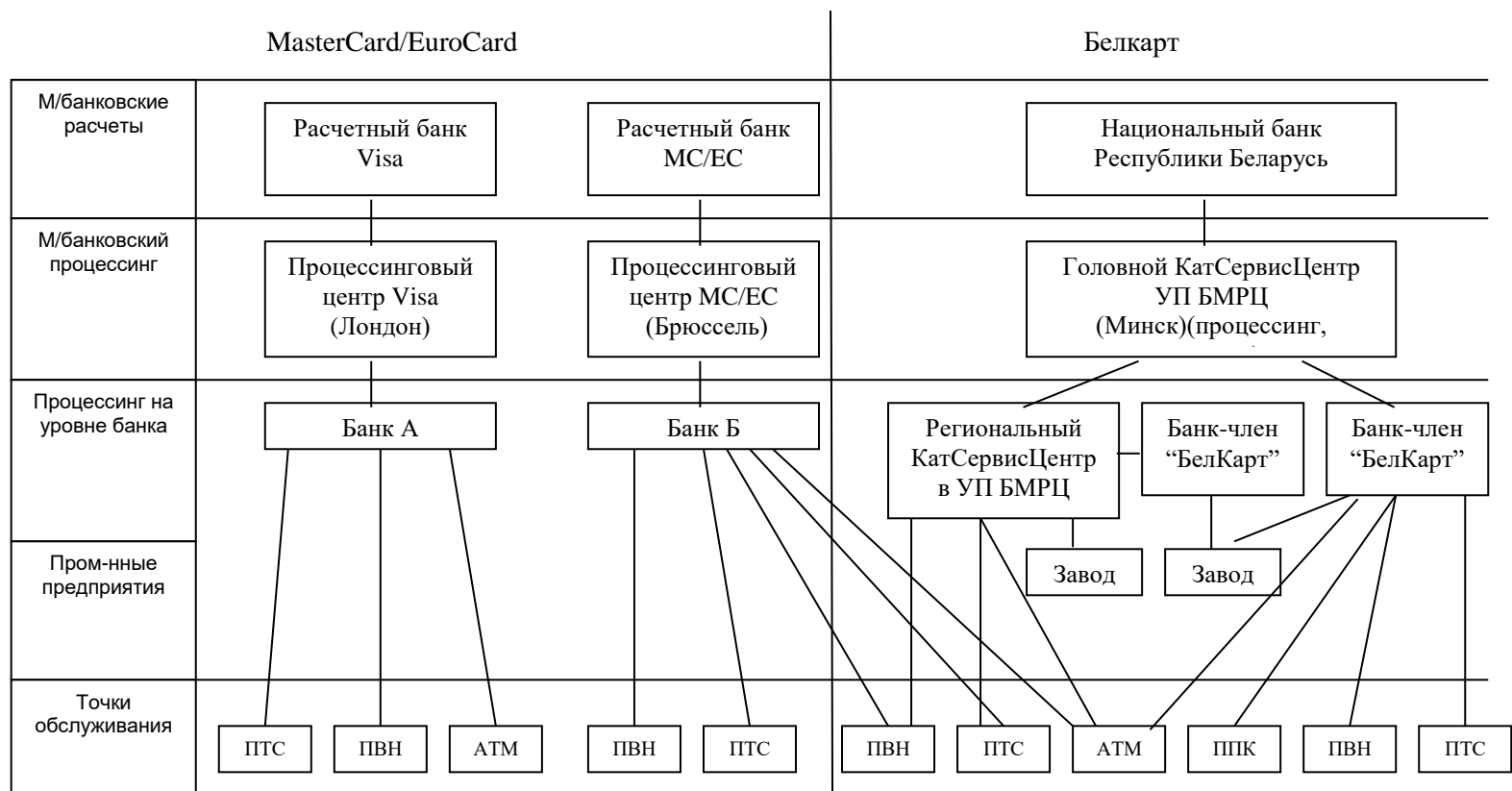


Рис. 5

БКЦ – КартЦентрБанка, АТМ – банкомат, ПТС – предприятие торговли и сервиса, ПВН – пункты выдачи наличных, ППК – пункт пополнения карточек.

11.1. Платежные карты и их место в финансовой индустрии

Трудно сегодня себе представить динамично развивающееся финансовое учреждение без работы с клиентами - физическими лицами. Несмотря на сложную организацию такой работы, довольно высокую затратную составляющую, именно в этом сегменте рынка находится «золотая жила», позволяющая банкам привлекать существенные средства и получать значительную прибыль, что особенно важно в условиях постоянно увеличивающейся конкуренции. При этом наиболее активно обслуживание физических лиц осуществляется с помощью пластиковых карт, о чем свидетельствуют многочисленные примеры - социальные программы банков Москвы и Возрождения, Альфабанк-Экспресс, кредитные линейки банков Русский Стандарт, Дельта-банк и т. д.

В последние годы рынок пластиковых карт в России переживает настоящий бум. Число карт только международных платежных систем каждый год практически удваивается. Неудивительно будет, если к 2007 году число банковских карт составит 50-70 миллионов. Следует также ожидать, что хотя большинство (до 60-70%) из этих карт будет принадлежать международным платежным системам VISA и MASTERCARD, востребованными останутся как российские, так и региональные и локальные (по территории и/или по принадлежности к одному банку-эмитенту) системы. А помимо банковских карт, существуют платежные небанковские карт - "бензиновые", предоплаченные и "скидочные" в сфере торговли, карты страховых компаний, и наконец, многофункциональные. Следует при этом отметить, что несмотря на многообразие использование карточек и размещаемых на них приложений, общие принципы построения карточных систем, требования к программно-аппаратным комплексам, используемое оборудование в достаточной степени унифицированы.

11.2. Общие принципы построения платежной системы

11.2.1. Участники системы

Участниками практически любой платежной системы с использованием пластиковых карт являются:

Таблица 1.1.

Участники	Основные функции
Координирующий орган	Решение организационно-технических вопросов по функционированию и развитию системы
Главный центр	Генерация и распределение ключей, сертификация

Эмиссионный центр (эмитент)	Регистрация и ведение владельцев карт (клиентов) Ведение счетов клиентов Ведение карт, включая стоп-листы, и их авторизация Персонализация карт
Эквайринговый центр (эквайер)	Регистрация и обслуживание (включая оплату предоставленных товаров и услуг) точек приема карт Регистрация и обслуживание торговых терминалов и банкоматов Выдача наличных по картам Прием и обработка транзакций устройств приема карт
Процессинговый центр (процессор)	Информационное взаимодействие между эмиссионными, эквайринговыми и процессинговыми центрами Обеспечение (информационное) взаиморасчетов Связь с внешними карточными системами
Точки приема карт	Отпуск товаров и оказание услуг по картам клиентов
Клиенты (владельцы карт)	Оплата за полученные товары и услуги по дебетным и кредитным счетам

Принципиальная схема платежной системы приведена на рис. 1.1.

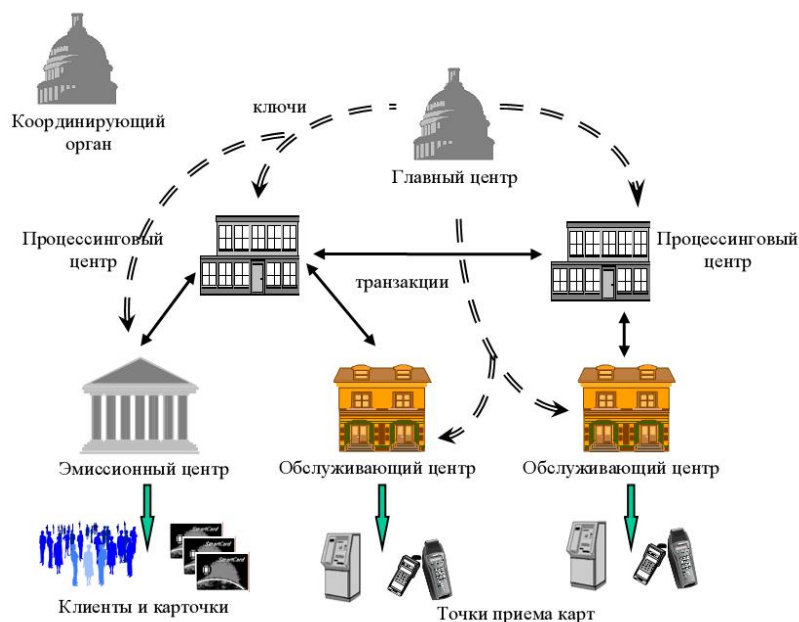
На организационно-информационные взаимосвязи, действующие в рамках одной платежной системы, накладываются следующие ограничения:

- имеется только один Координирующий орган,
- имеется только один Главный центр,
- каждый Эмиссионный центр связан только с одним Процессинговым центром,
- каждый Эквайринговый центр связан только с одним Процессинговым центром,
- каждая Точка обслуживания (магазин, АЗС, гостиница...) связана только с одним Эквайринговым центром,
- каждое карточное приложение, размещаемое на карте клиента, связано только с одним Эмиссионным центром.

В то же время допустимы иерархические (многоуровневые) взаимосвязи между процессинговыми центрами.

В общем случае все участники платежной системы, кроме владельцев карт, могут являться самостоятельными юридическими лицами, а владельцы карт - как физическими, так и юридическими лицами.

В зависимости от конкретной топологии системы, данная схема может изменяться. Например, эмиссионный, эквайринговый и процессинговый центры могут быть реализованы в рамках единой программно-технической установки у одного юридического лица. С другой стороны, как показывает практика, достаточно часто ряд технологических функций передается от эмиссионных и



эквайринговых центров центрами процессинговыми. Ниже рассматриваются ряд конкретных примеров подобных схем.

Рис 1.1. Принципиальная схема платежной системы

11.3. Варианты построения систем

11.3.1. Локальная одноэмитентная система

В зависимости от того или иного назначения системы, в качестве эмитента могут выступать - и действительно выступают - различные организации, например,

- финансовое учреждение (банк),
- сеть магазинов (или даже один магазин),
- топливная компания, сеть бензоколонок,
- крупное промышленное предприятие, обеспечивающее питание своих сотрудников и продажу им товаров в собственной торговой сети,
- гостиница или пансионат,
- университет.

В данном варианте реализации Координационный орган, Главный центр, Эмиссионный и Эквайринговый центр выступают в едином лице (все эти "участники" суть подразделения организации - владельца системы).

Процессинговый центр, как таковой - отдельный институт, в данной системе отсутствует.

11.3.2. Локальная многоэмитентная система одного банка

Владельцем системы является один банк. Карты выпускаются различными филиалами банка, расположенными на значительном расстоянии друг от друга, возможно, в различных городах. Во всех этих городах производится также и обслуживание карт, например, в сфере торговли, на АЗС, в банкоматах. В силу организационно-технологических причин (большие расстояния, отсутствие надежных мощных каналов связи между городами) невозможно или неудобно работать со счетами клиентов в единой он-лайновой сети с единой базой данных, а коммуникационная связь эквайрингового центра с устройствами приема карт работает неустойчиво и / или дорого из-за высоких тарифов на междугородные соединения.

В этом случае наиболее рациональным решением является организация на базе каждого филиала банка объединенного эмиссионного, эквайрингового и процессингового центра. Эти центры связаны между собой. При этом возможно обеспечение произвольной по топологии структуры, например, «каждый с каждым», «звезда» через головной офис банка, несколько отдельных «звезд», соединенных между собой и т. д.

Координационный орган и Главный центр, а также объединенные центры принадлежат банку и могут являться его подразделениями или самостоятельными дочерними структурами.

Карты обслуживаются во всей системе. При этом локальные авторизационные запросы и транзакции так и остаются локальными внутри данного филиала, а межфилиальные -направляются из соответствующего эквайрингового центра в соответствующий эмитентный.

При наличии устойчивых коммуникаций между отдельными филиалами и городами возможна реализация и производных архитектур. Так, например, если два и более филиалов или отделений банка расположены в одном городе и соединены между собой в единой локальной сети с одним сервером базы данных и удаленно распределенными автоматизированными рабочими местами операционистов, обслуживающих клиентские счета и карточки, то для этих филиалов используется один эмиссионный центр.

С другой стороны, возможно, подключение терминальных устройств к достаточно удаленному эквайринговому центру, который может находиться и в другом городе. В этом случае критерием может быть как технологическая, так и экономическая целесообразность.

На одной чаше весов - высокая стоимость междугородного трафика, на другой - стоимость организации дополнительного эквайрингового центра.

11.3.3. Региональная многоэмитентная система

Как правило, межбанковская система. Банки-участники присоединяются к уже существующей или организуют новую платежную систему. Чаще всего создается специальное юридическое лицо (например, процессинговая компания), обеспечивающее функционирование и развитие данной системы. Естественно, Координирующий орган и Главный центр принадлежат этой компании. В качестве эмиссионных и эквайринговых центров выступают банки-участники. Процессинговые центры могут принадлежать банкам, непосредственно платежной системе, быть самостоятельными организациями, надлежащим образом сертифицированными в рамках данной системы.

Общая же структура системы очень напоминает описанную в п.2.2.2. Однако довольно часто эмитенты и эквайеры перепоручают ряд функций процессинговым центрам. К числу таких функций относятся:

- персонализация карт, ведение лимитов и авторизация (для эмитентов),
- обслуживание терминальных устройств и сбор транзакций (для эквайеров).

Обычно это происходит при сравнительно небольшом числе клиентов и недостаточно развитой сети обслуживания (несколько банкоматов, несколько магазинов) у этих банков.

11.3.4. Международная платежная система

Прежде всего, к таким системам относятся Visa и Mastercard. Организационно и технологически в обеих системах очень много общего. Во-первых, руководство самих этих систем и выполняет роль Координирующего органа. Имеются в системах и центры сертификации, обеспечивающие генерацию и распространение ключей и криптографических сертификатов.

Во-вторых, именно усилиями этих систем создавались общие принципы функционирования «карточных» систем, в том числе и принципиальная схема (рис. 1.1).

В-третьих, близка политика развития систем и правила приема новых членов. Здесь наблюдается многоэтапность и постепенное принятие банками-участниками на себя все новых и новых функций.

В подавляющем большинстве случаев банки начинают свою работу в этих платежных системах в качестве банков-агентов, распространяющих чужие карты (карты банков-спонсоров) даже без собственного логотипа. Вся фактическая работа с картами ведется непосредственно в банках-спонсорах.

Затем банк вступает в платежную систему в качестве ассоциированного (или аффилированного) члена под патронажем тех же крупных банков-спонсоров. Ассоциированный член получает право эмиссии карт с собственным логотипом и даже может их самостоятельно персонализировать, однако авторизация осуществляется, как правило, у спонсоров или в сертифицированных процессинговых центрах (ThirdPartyProcessor - TPP у Visa или MemberServiceProvider - MSP - у Mastercard).

Поработав некоторое время в качестве ассоциированного (аффилированного) члена, банк получает возможность повысить свой статус до принципиального и стать полноправным эмитентом. Это позволяет не только выпускать карты, но и самостоятельно обеспечивать их авторизацию.

Банк - принципиальный член имеет возможность быть и эквайером. При этом его функции могут быть ограничены только финансовой составляющей (выдача наличных в отделениях банка, зарядка и инкассация кассет банкоматов, расчеты с торговой сетью) с передачей функций информационного обслуживания устройств приема карт другим банкам или процессинговым центрам. Наконец, он может выполнять самостоятельно все функции по обслуживанию карт. В этом случае он выполняет роль не только эквайрингового, но и процессингового центра, поскольку для авторизации карт других банков-эмитентов необходимо пересылать запросы в общую сеть платежной системы.

Естественно, на каждом этапе развития для выполнения принятых на себя функций банку необходимо иметь соответствующее оборудование и программное обеспечение.

11.4. Программное обеспечение платежной системы

11.4.1. Общая структура программного обеспечения

В соответствии с общими принципами построения платежных систем, изложенными в разделе 2, можно рассмотреть, модульное прикладное программное обеспечение (см. рис. 3.1), реализующее все необходимые функции как backoffice для работы с клиентами, счетами и картами, так и frontend для поддержки работы терминальных устройств и коммуникаций. При этом должны обеспечиваться эмиссия и обслуживание и традиционных карт с магнитной полосой, и карт с микросхемами. Такой программный комплекс должен быть построен на современной, отказоустойчивой и масштабируемой СУБД, например, Oracle. В соответствии с требованиями к размерности системы доступен широкий выбор рациональной программно-аппаратной платформы (в том числе ОС - Unix, Windows и др.).

В состав программного обеспечения входят три системы:

- Эмиссионный центр;
- Эквайринговый центр;
- Процессинговый центр.

Системы в свою очередь состоят из набора функциональных подсистем, обеспечивающих решение тех или иных задач. В зависимости от требований, выставляемых заказчиком, используются различные опции этих подсистем, определенная номенклатура внутрисистемных и внешних интерфейсов, коммуникационные модули.

В некоторых случаях, те или иные компоненты программного обеспечения могут устанавливаться у различных участников платежной системы. Например, если по поручению банка-эмитента ряд функций по ведению и персонализации

карт, а также их авторизации переданы некоторому юридическому лицу, обеспечивающему процессинг, то там помимо системы "Процессинговый центр" устанавливаются и необходимые компоненты системы "Эмиссионный центр". Аналогично, если банк-эквайер поручил процессинговому центру информационное обслуживание своих банкоматов или торговой сети, то там должны быть установлены и компоненты системы "Эквайринговый центр". С другой стороны, если банк является эмитентом и эквайером в некоторой распределенной системе, причем все функции по эмиссии и обслуживанию сети приема карт выполняет самостоятельно, то в банке устанавливается и система "Процессинговый центр".

11.4.2. Программное обеспечение эмиссионного центра

Основные функции системы "Эмиссионный центр" следующие: работа с клиентами, счетами, картами.

Эта система может устанавливаться в банках-эмитентах и процессинговых компаниях. Она содержит три основные подсистемы:

- "Обслуживание клентов и счетов";
- "Управление картами";
- "Авторизация в режиме on-line".

Подсистемы и основные функциональные, интерфейсные и коммуникационные модули с перечнем выполняемых функций и реализованных функциональных автоматизированных рабочих мест представлены в таблице 3.1.

Таблица 3.1. Система "Эмиссионный центр"

NN	Подсистема/Модуль	Функции	Тип АРМ
1	Подсистема "Обслуживание клиентов и счетов"		
1.1	Базовый модуль - ведение клиентов и счетов	безопасность и администрирование; регистрация и обслуживание клиентов - физических и юридических лиц; ведение текущих счетов клиентов (тип - "до востребования"); обработка финансовых	Администратор системы Операционист банка Бухгалтер
1.2	Сберегательная касса.	ведение счетов различного типа; работа со сберкнижками; коммунальные платежи	Операционист банка
1.3	Интерфейсный модуль к системе ОВД (заказной)	Передача интегрированных данных в "Операционный банковский день"	Автомат
2	Подсистема "Управление картами"		
2.1	Базовый модуль	ведение карт и их состояний	Операционист по работе с пластиковыми картами

2.2	Ведение карточных приложений на смарт-картах	особенности эмиссии смарт-карт, том числе: ведение "электронных кошельков"; пополнение "кошельков" и т. д.	Операционист по работе с пластиковыми картами
2.3	Генерация карт	генерация ключей эмитента; генерация карт и карточных приложений; генерация ПИН и печать ПИН-конвертов	Оператор по выпуску карт
2.4	Персонализация карт	Управление процессом персонализации карт в различных устройствах	Оператор по выпуску карт
2.5	Интерфейс к системе ведения клиентов и счетов	обмен данными с системой ведения клиентов и счетов (заказной или в рамках данного решения - п. 1.1)	Автомат
2.6	Модули передачи данных для генерации карт Процессору	передача данных для генерации карт Процессору, если ему поручена данная функция (заказная или в рамках данного решения)	Оператор по работе с пластиковыми картами / Автомат
2.7	Модули передачи данных для управления карт-счетами у Процессора	передача данных для управления карт-счетами у Процессора, если ему поручена данная функция (заказная или в рамках данного решения)	Оператор по работе с пластиковыми картами / Автомат
2.8	Модули передачи стоп-	передача стоп-листов (заказная	Оператор по работе с
		или в рамках данного решения)	пластиковыми картами / Автомат
2.9	Модули пакетного приема финансовых операций (протоколов транзакций)	пакетный прием протоколов транзакций (заказная или в рамках данного решения)	Оператор по работе с пластиковыми картами / Автомат
3	Подсистема "Авторизация"		
3.1	Базовый модуль авторизации	on-line авторизация карт с использованием базы данных п. 2.1; настройка параметров, работа с протоколами, оперативное управление	Автомат Инженер по коммуникациям
3.2	Интерфейс к системе ведения карт и карточных	интерфейс к системе ведения карт и карточных счетов (п.	Автомат
3.3	Модули приема авторизационных запросов	прием авторизационных запросов от различных платежных систем	Автомат

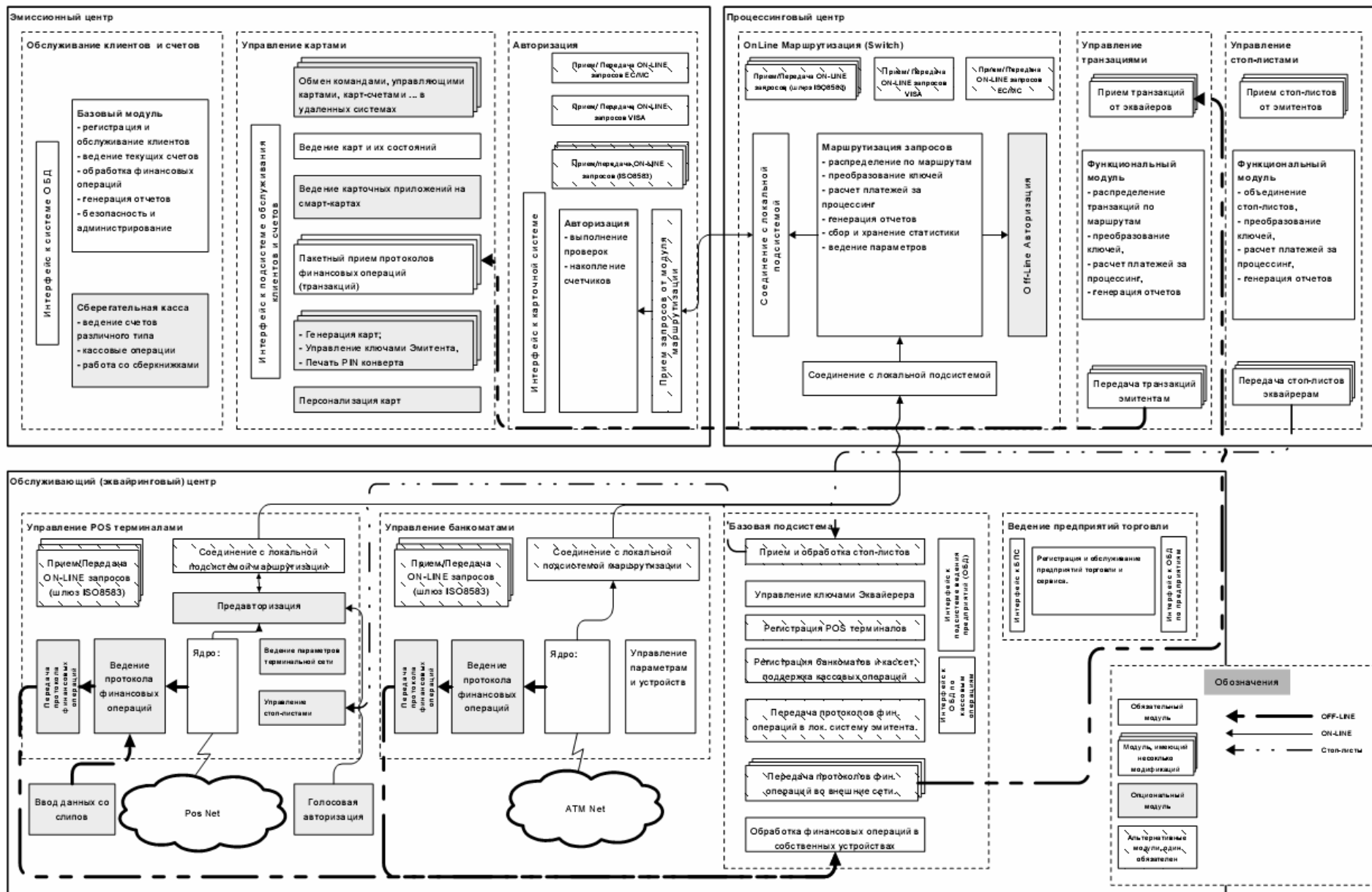


Рис 3.1 Общая функциональная схема программного обеспечения

Выбор тех или иных подсистем и модулей определяется требованиями к построению системы. Обсудим некоторые из них.

Подсистема "Обслуживания клиентов и счетов" необходима в том случае, если заказчик не обладает аналогичной по функциональному назначению системой для работы с физическими лицами или "карточное" программное обеспечение превосходит ранее приобретенное по критерию "цена - качество". Если используется такая подсистема, то интегрированные характеристики по закрытию банковского операционного дня должны передаваться в общую систему ОВД. Это реализуется либо передачей файлов согласованного формата, либо даже на бумажном носителе для последующего ручного ввода. В любом случае данный интерфейс настраивается в зависимости от используемого в банке ПО и в зависимости от сложившихся у конкретного заказчика традиций обработки информации.

Опциональный модуль "Сберегательная касса" позволяет в рамках предлагаемого решения одновременно с ведением карточных счетов вести и обслуживать счета некарточные, причем различного типа - валютные и рублевые, срочные и до востребования и т. д., проводить коммунальные платежи. При установке системы в Процессинговом центре этот модуль не нужен.

Подсистема "Управление картами" является ядром системы "Эмиссионный центр". А далее возможны варианты.

При использовании в платежной системе карт с микросхемой используется модуль "Ведение карточных приложений на смарт-картах". Обычно речь здесь идет об электронном кошельке, однако в случае многофункциональных систем, а также при обслуживании микропроцессорных карт, соответствующих спецификациям EMV международных платежных систем, данный модуль получает соответствующие расширения.

Генерация и персонализация карт может производиться как непосредственно в банке-эмитенте, так и по поручению банка в какой-либо процессинговой компании или в банке-спонсоре. В первом случае используются соответствующие компоненты подсистемы, во втором - почтовые модули, обеспечивающие пересылку необходимой информации о картах, счетах и их владельцах процессору. У конкретного процессора карт конкретной платежной системы (например, VISA или СТБкарт) могут быть свои специфические требования к форматам этой информации, поэтому возникает определенное множество возможных реализаций данного модуля.

Аналогично обстоит дело и с модулем, обеспечивающим пакетный прием протоколов финансовых операций (транзакций). Ведь вид передаваемых файлов зависит от конкретного источника. Это может быть процессинговая компания или банк-спонсор. В рамках предлагаемого комплексного решения транзакции могут приходить как из внешнего мира,

так и передаваться по локальной сети от системы «Эквайринговый центр», установленной в том же банке.

Подсистема «Авторизация on-line» будет необходима в случае обслуживания, например, карт с магнитной полосой. Проверки осуществляются при взаимодействии данной подсистемы с базой данных, являющейся частью других компонент системы («Обслуживание карт и счетов» и «Ведение карт и состояний»). При этом авторизационные запросы могут приходить как из локально установленной системы «Эквайринговый центр», так и извне (Visa, Europay, других платежных систем).

11.4.3. Программное обеспечение эквайрингового центра

Основные функции системы "Эквайринговый центр" следующие:

- обеспечение информационного взаимодействия с устройствами приема карт (банкоматами и терминалами),
- поддержка кассовых операций при работе с банкоматами,
- обеспечение расчетов с торговлей.

Может устанавливаться в банках-эквайрерах и процессинговых компаниях.

Содержит четыре основные подсистемы:

- "Базовая подсистема";
- "Ведение предприятий торговли";
- "Управление POS-терминалами" - POS Manager;
- "Управление банкоматами" - ATM Controller.

Подсистемы и основные функциональные, интерфейсные и коммуникационные модули с перечнем выполняемых функций и реализованных функциональных автоматизированных рабочих мест представлены в табл. 3.2.

Таблица 3.2. Система "Эквайринговый центр"

NN	Подсистема/Модуль	Функции	Тип АРМ
1	Базовая подсистема		
1.1	Ядро подсистемы	безопасность и администрирование; генерация ключей	Администратор системы
1.2	Поддержка работы с терминалами	регистрация POS-терминалов; обработка финансовых операций и бухгалтерия; генерация	Работа с терминалами Бухгалтер по терминалам
1.3	Поддержка работы с банкоматами	регистрация банкоматов; обработка финансовых	Работа с банкоматами Бухгалтер по банкоматам

1.4	Интерфейсный модуль к системе ОБД по кассовым операциям	передача интегрированных данных в	Автомат
1.5	Интерфейсный модуль к системе ведения предприятий торговли	передача данных в систему ведения предприятий	Автомат
1.6	Модули приема стоп-листов	прием стоп-листов (заказная в рамках данного решения)	Оператор по точкам приема / Автомат
1.7	Модули пакетной передачи финансовых операций (протоколов)	пакетный прием протоколов транзакций (заказная или в рамках)	Оператор по обслуживанию точек приема / Автомат
2	Подсистема "Ведение предприятий"		
2.1	Регистрация и обслуживание предприятий торговли и сервиса	регистрация и обслуживание предприятий; обработка финансовых операций и бухгалтерия; генерация	Бухгалтер
2.2	Интерфейсный модуль к базовой подсистеме и модулю ведения терминалов	взаимодействие двух подсистем	Автомат
2.3	Интерфейсный модуль к системе ОБД по торговле (заказной)	передача интегрированных данных в ОБД	Автомат
3	Подсистема "Управление"		
3.1	Ядро подсистемы	поддержка коммуникаций с сетью банкоматов; настройка параметров, работа с протоколами, оперативное управление	Автомат Инженер по коммуникациям
3.2	Управление параметрами устройств	управление параметрами	Инженер по удаленному обслуживанию
3.3	Управление стоп-листами	стоп-листами	Инженер по удаленному обслуживанию
3.4	Модуль предавторизации	принятие решений об авторизации запросов без обращения к	Инженер по удаленному обслуживанию / Автомат
3.5	Модуль голосовой	голосовая авторизация (при использовании)	Оператор-телефонист
3.6	Модуль ввода данных со слипов	ввод данных со слипов	Оператор по вводу слипов
3.7	Ведение и передача протоколов финансовых операций	ведение и передача протоколов финансовых операций	Автомат
3.8	Передача авторизационных запросов в	передача авторизационных запросов - в локальную подсистему или	Автомат
4	Подсистема "Управление"		

4.1	Ядро подсистемы	поддержка коммуникаций с сетью банкоматов; настройка параметров, работа с протоколами, оперативное управление	Автомат Инженер по коммуникациям
4.2	Управление параметрами устройств	управление параметрами	Инженер по удаленному обслуживанию
4.3	Ведение и передача протоколов операций	ведение и передача протоколов финансовых	Автомат
4.4	Передача авторизационных запросов в	передача авторизационных запросов - в локальную подсистему или	Автомат

Выбор тех или иных подсистем и модулей определяется требованиями к построению системы. Приведем пример.

Базовая подсистема является необходимой в большинстве случаев. Обязательными модулями базовой подсистемы являются ядро и модуль обработки финансовых операций. В случае обслуживания терминалов и банкоматов могут опционально потребоваться модули регистрации этих устройств. Для взаимодействия системы "Эквайринговый центр" с другими "карточными" компонентами данной установки комплекса (здесь же локально установленными системами "Эмиссионный центр" и "Процессинговый центр"), с системой "Операционный день банка", с внешним миром (другие процессинговые и эмиссионные центры) используются различные коммуникационные и интерфейсные модули. Часть их является заказной или настраиваемой и ориентирована на те или иные используемые форматы и протоколы обмена данными.

Подсистема "Ведение предприятий торговли" предназначена для полного учета финансового взаимодействия эквайрера с сетью приема карт, формирования платежных поручений для перевода на счета этих предприятий при обслуживании владельцев карт и т.д.

Подсистемы "Управление POS терминалами" и "Управление банкоматами" позволяют вести управление параметрами устройств, осуществлять мониторинг их текущего состояния.

В случае автономного использования подсистем вне рамок комплексного решения опционально может вестись база данных о транзакциях. Если же решение комплексное, все транзакции хранятся в соответствующих таблицах общей СУБД.

При обслуживании эмбоосированных карт в торговой и сервисной сети, а также и в банковских отделениях при выдаче наличных до сих пор в некоторых случаях используются простейшие механические устройства - импринтеры. Авторизация карт при этом осуществляется по телефону (голосовая авторизация). Чеком является специальный многослойный бланк -

слип, на листах которого остается отпечаток номера карты, иногда -учетного номера импринтера и даты. Слипы затем отправляются в банк, где их данные вручную вводятся в компьютер для дальнейшей обработки. Для поддержания такой технологии используются соответствующие опциональные модули.

Также опциональным модулем в подсистеме "Управление POS-терминалами» является модуль «Предавторизация». Он позволяет без дальнейшего он-лайнного запроса по определенным рисковым процедурам на уровне подсистемы принять решение о разрешении транзакции или об отказе в обслуживании. Возможно использование самых разных критериев, например, разрешать все платежи на сумму не более определенной суммы, отклонять все запросы на большие суммы в случае, если запрос пришел с терминала, установленного в булочной и т.д.

Для передачи авторизационных запросов в данную локальную установку (в подсистему «Авторизация» системы «Эмиссионный центр» или в систему «Процессинговый центр») используется модуль соединения с локальной системой. В случае присоединения данного эквайрингового центра с внешним процессинговым работают модули приема-передачи в соответствии с протоколом ISO8583, который может иметь ряд конкретных реализаций.

11.4.4. Программное обеспечение процессингового центра

Основные функции системы "Процессинговый центр" следующие:

- обеспечение информационного взаимодействия между эмиссионными, эквайринговыми и процессинговыми центрами.

Система может устанавливаться в процессинговых компаниях и банках-эквайерах.

Она содержит три основные подсистемы:

- "Базовая подсистема";
- "Маршрутизатор on-line» - Switch;
- "Маршрутизатор off-line».

Подсистемы и основные функциональные, интерфейсные и коммуникационные модули с перечнем выполняемых функций и реализованных функциональных автоматизированных рабочих мест представлены в табл. 3.3.

Таблица 3.3. Система "Процессинговый центр"

NN	Подсистема/Модуль	Функции	Тип АРМ
1	Базовая подсистема		
1.1	Ядро подсистемы	безопасность и администрирование; генерация ключей; регистрация	Администратор системы

1.2	Модули приема данных для генерации карт от Эмитента	прием данных для генерации карт от Эмитента, если данная функция по его поручению	Оператор по работе с пластиковыми картами / Автомат
1.3	Модули приема данных от Эмитента для управления карт-счетами и состояниями карт	прием данных от Эмитента для управления карт-счетами, если данная функция поручена Процессору, или состояний карты для поддержки офф-	Оператор по работе с пластиковыми картами / Автомат
2	Подсистема "Маршрутизатор on-line"		
2.1	Маршрутизация запросов	распределение авторизационных запросов по маршрутам; преобразование ключей; сбор и хранение статистики; ведение параметров; расчет платежей за процессинг; генерация отчетов; настройка параметров, работа с протоколами, оперативное	Автомат Сопровождение сети Бухгалтер Инженер по коммуникациям
2.2	Off-line авторизация	проверка условий возможности авторизации карты без обращения к	Автомат
2.3	Модули передачи/приема авторизационных	передача авторизационных запросов к эмитентам и другим	Автомат
2.4	Интерфейсный модуль к локальным эквайринга и эмиссии	прием и передача данных внутри данной локальной	Автомат
3	Подсистема "Маршрутизатор off-line"		
3.1	Управление потоками стоп-листов	объединение стоп-листов, поступивших от эмитентов; преобразование ключей; расчет платежей за процессинг; генерация	Автомат
3.2	Модули передачи и приема стоп-листов	прием стоп-листов от эмитентов и передача	Автомат
3.3	Управление потоками транзакций	распределение транзакций, поступивших от эквайнеров, по маршрутам; преобразование ключей; расчет платежей за процессинг; генерация	Автомат
3.4	Модули приема и передачи журналов транзакций	прием журналов транзакций от эквайнеров и передача эмитентам	Автомат

Выбор тех или иных подсистем и модулей определяется требованиями к построению системы.

Базовая подсистема (точнее, ее ядро) является необходимой. Доступны две почтовые коммуникационные опции. Первая позволяет в заданных форматах получать от банков-эмитентов данные по картам, которые необходимо выпустить (персонализировать и напечатать ПИН-конверт). Требуется в том случае, если банк-эмитент поручил процессору выпустить карты для его клиентов. Вторая служит для приема от банков эмитентов файлов с состояниями эмитированных карт (лимиты, статусы и т. д.). Требуется в том случае, если банк-эмитент поручил процессору осуществлять авторизацию карт.

Подсистема "Маршрутизация on-line", или Switch, необходима, если в данной платежной системе требуется он-лайн авторизация. Подсистема позволяет обеспечить защищенную маршрутизацию данных запросов и ответов, сбор и хранение статистических данных, расчет взаимных платежей между участниками системы. Имеет необходимые коммуникационные модули различных форматов.

Подсистемы "Маршрутизация off-line" обеспечивает доставку стоп-листов от эмитентов к эквайерам и протоколов финансовых операций от эквайеров к эмитентам. Требуется как в случае обслуживания карт в он-лайн режиме, так и при обслуживании карт в режиме офф-лайн, например, при использовании микропроцессорных карт с приложением типа «электронный кошелек».

11.5. Примеры реализации

11.5.1. Локальная одноэмитентная система на микропроцессорных картах

Данная системная установка предполагает обслуживание карт с приложением типа "электронный кошелек", например, на АЗС. Приняты следующие предположения:

- обслуживание карточных счетов осуществляется в рамках данного решения (компоненты система "Эмиссионный центр");
- расчеты с АЗС также осуществляются внутри данного решения (компоненты системы "Эквайринговый центр").

Следует подчеркнуть, что общая схема не претерпевает каких-либо изменений и в случае обслуживания карт в произвольных торговых точках, а не только на АЗС.

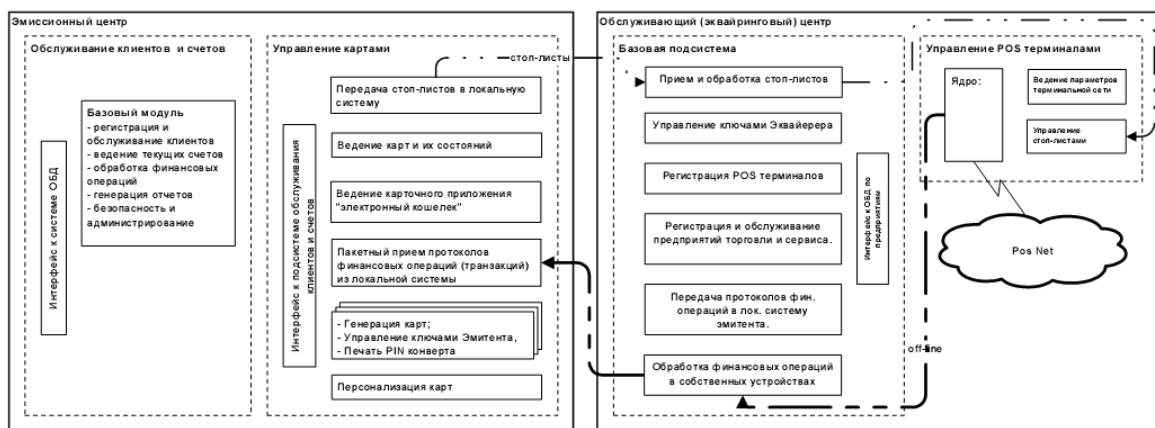


Рис. 3.2. Локальная одноэмитентная система

11.5.2. Расширение системы до уровня многоэмитентной

Локальная платежная система расширяется до уровня межрегиональной. Эмиссия и обслуживание ведется в нескольких городах (филиалах банка,) возможно, в других банках. Приняты следующие предположения:

карты обслуживаются только в терминальной сети, банкоматов нет;

генерация карт осуществляется в едином персонализационном центре, возможно, с окончательной персонализацией микросхемы на местах;

клиенты и торговля обслуживается в соответствии с п. 3.5.1.

При этом во всех эмиссионно-эквайринговых центрах устанавливается ПОВ соответствии со схемой рис. 3.2. Кроме того, для функционирования системы в целом как единого платежного пространства и для поддержки технологии персонализации карт в едином - главном - центре необходимо для каждого центра провести установку дополнительного ПО (система "Процессинговый центр" и модули приема/передачи данных для персонализации карт). Структурная схема необходимого расширения приведена на рис.

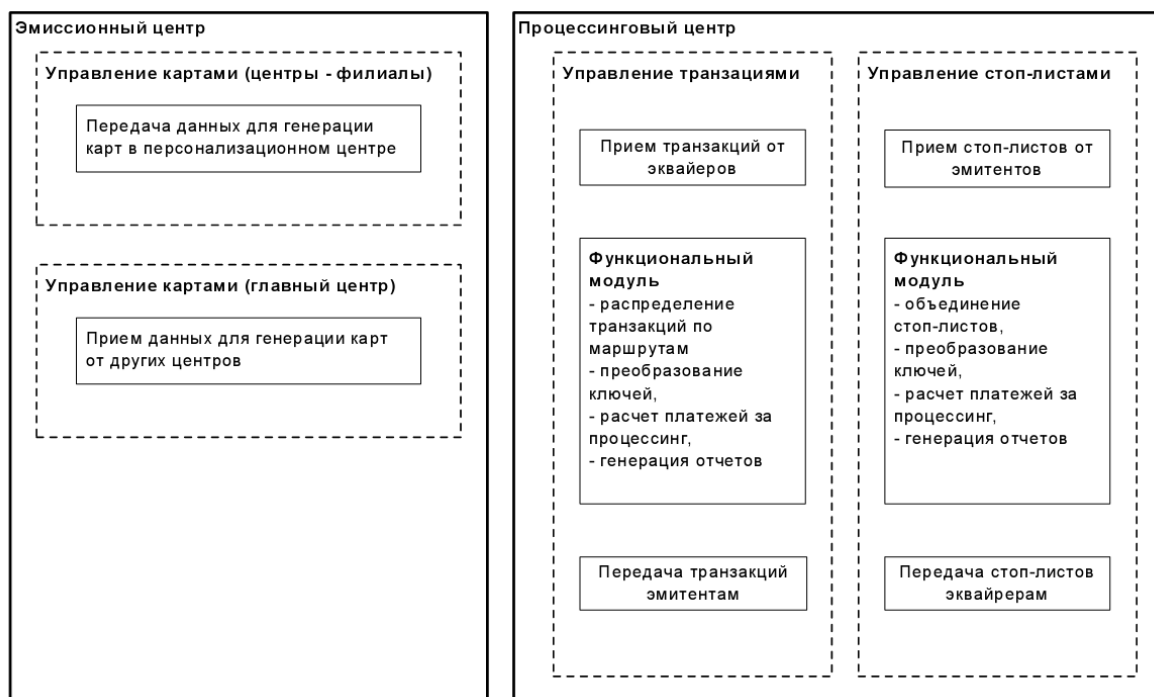


Рис. 3.3. Расширение до многоэмитентности

11.5.3. Эмиссия карт международных платежных систем

Подсистемы "Обслуживание клиентов и счетов" и "Управление картами" (рис. 3.2) позволяют в том числе и сопровождать карточные счета и сами карты международных платежных систем. Но необходимо установить и дополнительные компоненты, номенклатура которых зависит от принятых организационных решений.

В случае, если банк-эмитент поручает третьей стороне (банку-спонсору) или процессинговой компании осуществлять генерацию карт и их авторизацию, то дополнительными будут почтовые модули передачи и приема необходимой информации.

Если эмитент сам осуществляет генерацию карт, то необходимо установить соответствующее оборудование, например, эмбоссер, а также программное обеспечение, зависящее от типа эмитируемых карт. Так, эмиссия комбинированных карт типа VisaSmartDebit/Credit требует использования дополнительных по отношению к эмиссии только карт с магнитной полосой устройств и программных модулей.

Для самостоятельной авторизации карт устанавливается также подсистема "Авторизация". Структурная схема такого варианта изображена на рис. 3.4 (заштрихованы ранее описанные компоненты).

11.5.4. Обслуживание карт международных платежных систем

Наиболее полный вариант системы, установленной в банке, позволяет не только эмитировать карты, но и вести их полное обслуживание в собственной терминальной и банкоматной сети. Требуется практически полная номенклатура подсистем и модулей в соответствии со структурой, изображенной на рис. 3.1.

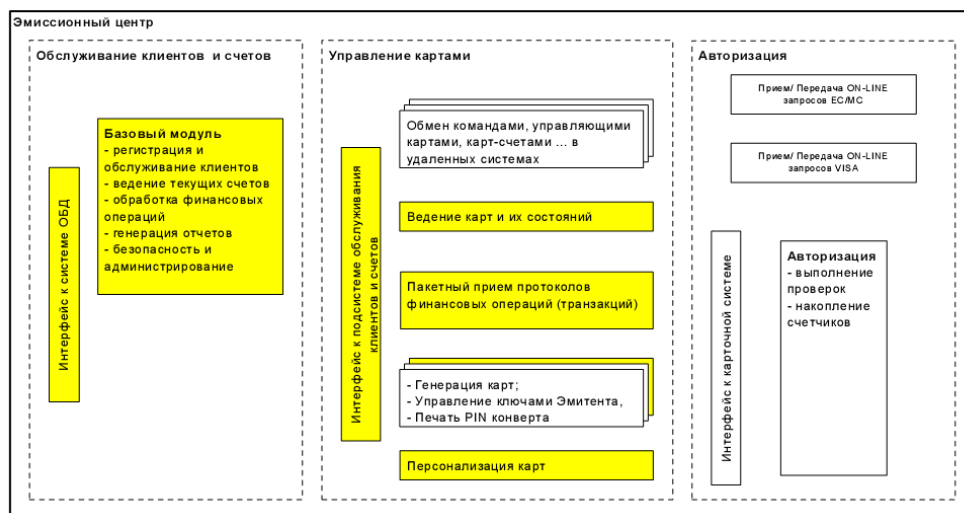


Рис. 3.4. Эмиссия международных карт

11.6. Вычислительная техника и оборудование центра

11.6.1. Типовая структура вычислительного центра

Типовая структура средств вычислительной техники, которая, вообще говоря, практически не зависит от функционального назначения данного центра приведена на рис. 6.1.

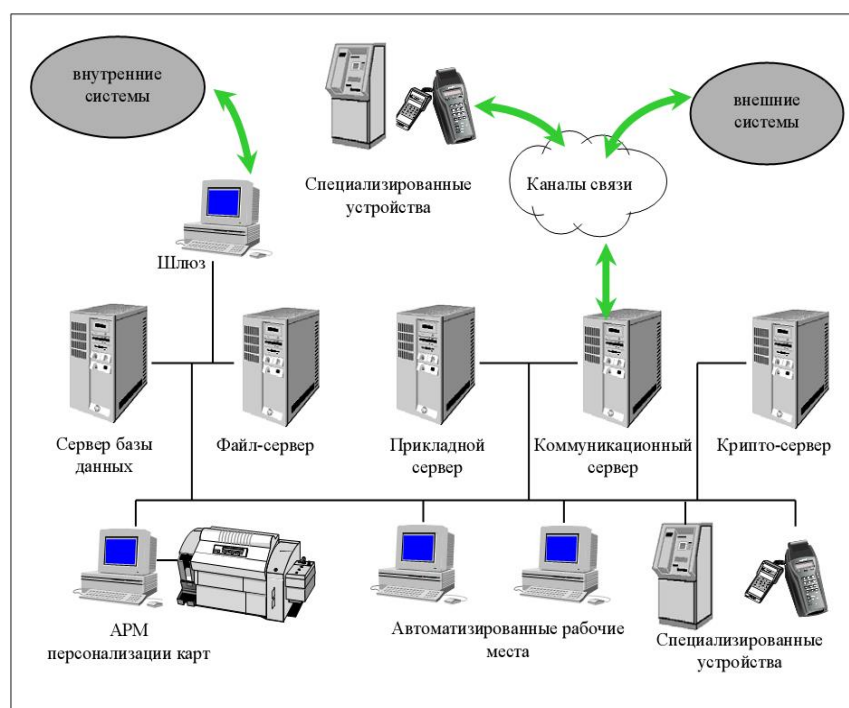


Рис. 4.1. Общая структура вычислительной техники

11.6.2. Серверы

Функционально выделяется 5 серверов:

Наименование	Функциональное назначение	Рекомендуемые характеристики
Сервер базы данных	Хранение базы данных	512 МВ ОЗУ, 60 GBHDD, 4 носителя, зеркалирование
Файловый сервер	Хранение рабочих файлов	256 МВ ОЗУ, 60 GBHDD, 4 носителя, зеркалирование
Прикладной сервер	Выполнение автоматических процедур	128 МВ ОЗУ, 20 GB HDD
Коммуникационный сервер	Поддержка коммуникаций	128 МВ ОЗУ, 10 GB HDD
Крипто-сервер	Выполнение криптографических функций	64 МВ ОЗУ, 10 GB HDD

Рекомендуемые характеристики приняты для системы со следующими количественными параметрами:

- эмиссия 10-20 тысяч карт;
- обслуживание 50-200 устройств приема карт.

В случае реализации системы меньшей размерности допустимо совмещение ряда серверов на единых машинах:

- сервер СУБД и файловый сервер;
- прикладной и коммуникационный, возможно, крипто-сервер.

Более того, иногда можно начинать и с одного общего сервера.

С другой стороны, при достаточно развитой системе необходимо предусмотреть средства повышения надежности и резервирования, такие, как:

- несколько процессоров на одном сервере;
- зеркалирование носителей на твердых дисках;
- кластеры;
- создание архивов на ленте или магнито-оптических дисках и т. д.

При увеличении числа карт до многих десятков и сотен тысяч и числа обслуживаемых терминальных устройств до сотен и тысяч, особенно в случае поддержки он-лайнной авторизации, целесообразно в качестве серверов использовать и более мощные компьютеры, например, с RISC-архитектурой.

Дополнительно к перечисленным серверам на рис. 4.1 выделен сервер-шлюз. Этот сервер необходим в случае подключения программного обеспечения платежной системы к другим программно-техническим комплексам, установленным в банке. Это может, например, быть система "Операционный банковский день". Через шлюз производится обмен информацией между двумя системами.

11.6.3. Автоматизированные рабочие места

В системе используется широкая номенклатура автоматизированных рабочих мест (АРМ). К ним относятся:

- АРМ администратора системы;
- бухгалтерские АРМ различного назначения (работа с вкладчиками - физическими лицами, поддержка кассовых операций, расчеты с предприятиями торговли, взаиморасчеты между эмитентами и эквайрерами и т. д.);
- АРМ оператора «сберегательной кассы» по обслуживанию карточных счетов;
- персонализация карт;
- АРМ инженера по обслуживанию терминальных устройств и банкоматов;
- АРМ инженера-программиста по сопровождению системы и ее доработкам;
- АРМ ввода информации (например, со слипов или ведомостей);
- и т. д.

В качестве данных АРМ используются обычные персональные компьютеры. Специальных требований нет.

11.6.4. Дополнительное оборудование

При обслуживании клиентов в офисе эмитента необходимо в зависимости от типа решаемых задач предусмотреть дополнительное, в том числе «карточное» оборудование.

Во-первых, для печати документов (отчетов, справок, приходных и расходных ордеров, платежных поручений, движений средств по счету и т. д.) необходимы принтеры. Это могут быть обычные, а также специальные кассовые принтеры. Номенклатура определяется совместно с Заказчиком с учетом требований, регламентирующих виды и формы отчетных документов, со стороны государственных организаций (Банк России, Налоговая Инспекция) и традиций, сложившихся непосредственно у Заказчика.

Во-вторых, для обслуживания клиента в кассовом зале целесообразно автоматизировать поиск информации в базе данных, тем более что имеется такой удобный идентификатор как сама пластиковая карта. Поэтому целесообразно оснастить рабочее место либо терминалом, либо просто устройством чтения карты, подключенным к компьютеру. В зависимости от типа карт это может быть устройство чтения магнитной полосы либо устройство чтения/записи микросхемы в случае использования карт с микропроцессором. В последнем случае это же устройство позволяет пополнить «электронный кошелек» карты. Для подтверждения полномочий лица, предъявившего карту, используется специальная клавиатура для ввода персонального идентификационного номера (ПИН-клавиатура).

В третьих, потребуется коммуникационное оборудование - платы, модемы и т. д.

Наконец, имеются специфические требования к криптосерверу. Секретная информация (ключи различного назначения) обычно хранится в специальных защищенных от постороннего проникновения устройствах. Международные платежные системы используют для этих целей так называемые HSM (hardware security module). В локальных системах мы предлагаем значительно более дешевое решение - устройство чтения/записи микросхемы и специальную микропроцессорную карту.

Для печати ПИН-конвертов используется матричный принтер, как правило, подключенный непосредственно к криптосерверу. ПИН-конверт - специальный многослойный конверт-бланк с конструкцией, обеспечивающей секретную печать ПИН-кода и другой (несекретной) информации без применения красящей ленты.

ГЛОССАРИЙ

Банковский лизинг - лизинговая сделка, в которой в качестве лизинговой компании выступает банк, приобретающий по заказу лизингополучателя оборудование и сдающий ему это оборудование в аренду.

Дебиторская задолженность по лизингу - сумма арендной платы за оборудование, сданное банком в аренду деловым единицам в качестве альтернативы получению ссуды на приобретение этого оборудования.

Карточный счет - банковский счет, распоряжение которым может осуществляться с помощью банковской платежной карточки. На картсчет зачисляются средства, которые предназначены для дальнейшего расходования с помощью банковской платежной карточки.

Клиринг - КЛИРИНГ [англ. clearing] - система безналичных расчетов за товары, ценные бумаги и услуги, основанная на зачете взаимных требований и обязательств. Различают межбанковский КЛИРИНГ (расчеты между банками путем зачета взаимных денежных требований юридических лиц данной страны) и международный валютный КЛИРИНГ (расчеты во внешней торговле и других формах экономических отношений между странами, осуществляемые на основе международных платежных соглашений).

Овердрафт - форма краткосрочного кредита, предоставление которого осуществляется списанием средств по счету клиента (сверх остатка на счете), в результате чего образуется дебетовое сальдо.

Дилер — биржевой посредник, покупающий товар от своего имени и на свои деньги с целью последующей продажи на бирже.

Брокер — биржевой посредник, покупающий товар от имени клиента и на его деньги

Треjder — работник брокерской фирмы, непосредственно исполняющий заказы на куплю-продажу ценных бумаг в торговом зале биржи.

Банк международных расчётов (BMP; Bank for International Settlements — BIS), международный финансовый институт, созданный в 1930 в Базеле (Швейцария) центральными банками Англии, Франции, Германии, Бельгии, Италии, тремя частными банками США во главе с банкирским домом Морганов и японскими частными банками. Учреждение BMP было предусмотрено Гаагской конвенцией (планом Юнга, 1930). Банку было поручено принимать и выплачивать германские репарационные платежи, включая расчёты за поставки натурой, и оплачивать межсоюзнические долги, осуществлять операции, связанные с займом Юнга, главным образом США, и обслуживать платежи по займам Дауэса и Юнга. В связи с прекращением платежей по репарациям и военным долгам с 1931 характер деятельности банка меняется. BMP покупает и продаёт золото и иностранную валюту, принимает от центральных банков на хранение золото, предоставляет и получает от них ссуды под залог золота или легко реализуемых краткосрочных обязательств, включая казначейские векселя, покупает и продаёт котирующиеся на бирже облигации. Банк не имеет права выпускать банкноты, оплачиваемые по предъявлению, акцептовать тратты (переводные векселя), предоставлять ссуды правительствам, приобретать контроль над предпринимательскими компаниями. В годы 2-й мировой войны 1939—45 в BMP хранилось золото, награбленное фашистами. В банке продолжалось сотрудничество между директорами стран антигитлеровской коалиции (Франции, Англии и США) и фашистских стран. Валютно-финансовая конференция в Бреттон-Вудсе (1944) приняла решение о ликвидации BMP, но, пользуясь поддержкой реакционных элементов стран — членов банка, он уцелел и стал расширять свои операции. Банк участвовал в проведении операций по «плану Маршалла»,

осуществлял многосторонние клиринги для Европейского платёжного союза, после роспуска последнего — в рамках Европейского валютного соглашения. БМР является финансовым агентом Европейского объединения угля и стали, Международного Красного Креста, Всемирного почтового союза и др. БМР выступает в качестве европейского вспомогательного органа Международного валютного фонда и Международного банка реконструкции и развития, которому он содействует в размещении облигаций банка в Швейцарии. С начала 60-х гг. БМР стал центром международных соглашений империалистических держав по поддержке мировой валютной системы капитализма (см. Валютный кризис). Он участвовал в кредитовании Англии и Федеральной резервной системы США на основе соглашений типа «своп» (операций по взаимному обмену валютой на срок по твёрдому курсу) (см. Валютный рынок). В 1968—69 принимал участие в кредитах Франции. Являлся агентом «Золотого пула». В 1951 Япония выбыла из состава БМР. В 1968 в БМР входили центральные банки всех европейских капиталистических и социалистических стран, кроме СССР и ГДР; представителем США на общих собраниях акционеров является «фёрстнэшонал сити банк оф Нью-Йорк». В 1970 акционерами БМР стали Япония и Канада.

75% акций БМР принадлежит центральным банкам и 25% — частным банкам и лицам, банки-учредители располагают более 50% акций. Текущими делами банка руководит Совет директоров, в состав которого входят 8 управляющих центральными банками европейских стран: Англии, ФРГ, Франции, Бельгии, Италии, Швейцарии, Швеции и Нидерландов и 5 представителей финансовых, промышленных и торговых кругов, назначаемых этой восьмёркой. БМР имеет валютно-экономический отдел, осуществляющий исследования в области международных валютно-кредитных отношений. Выпускает ежегодный обзор, в котором даёт информацию и исследования международных валютно-кредитных отношений за год, и текущий бюллетень. Акционерный капитал в 1930 был установлен в 500 млн. золотых фр., в декабре 1969 увеличен до 1,5 млрд. фр. На 31 марта 1969 оплаченный капитал составлял 125 млн. золотых фр. (1 фр. = 0,29 г чистого золота); баланс составил 14,6 млрд. золотых фр., в том числе вклады центральных банков в золоте — 4,8 млрд. фр., в иностранной валюте — 6,6 млрд. фр., в активе — золото в слитках — 4,0 млрд. фр., ссуды (в большинстве краткосрочные) — 9,0 млрд. фр.

Риск ликвидности – это риск потери платежеспособности организации в силу тех или иных причин. Также под данным термином иногда понимается риск ликвидности актива – риск, связанный с неопределенностью срока реализации актива или курсовых потерь, связанный с реализацией.

Дата валютирования – 1) при списании средств со счета (дебетовании) – дата, начиная с которой дебетованная сумма не находится в распоряжении владельца счета; при зачислении средств на счет (кредитовании) – дата, начиная с которой владелец счета вправе распоряжаться зачисленными на этот счет средствами.

2) дата (а при наличии договоренности Сторон - и время) зачисления средств на корреспондентский счет Стороны, получающей данную валюту по условиям сделки.

Клиринг – осуществляемый до расчета процесс передачи, сверки и в некоторых случаях подтверждения платежей с последующим зачетом взаимных денежных требований и обязательств (неттинг) и формированием окончательных чистых позиций участников клиринга для расчета на нетто-основе.

Неттинг – взаимное погашение обязательств или активов между филиалами банка или несколькими банками.