Министерство образования Республики Беларусь
Учреждение образования
«Белорусский государственный университет
информатики и радиоэлектроники»

Факультет инфокоммуникаций

Кафедра защиты информации

Т. В. Борботько, О. В. Бойправ

ЗАЩИТА ИНФОРМАЦИИ В БАНКОВСКИХ ТЕХНОЛОГИЯХ

Рекомендовано УМО по образованию в области информатики и радиоэлектроники в качестве учебно-методического пособия для специальности 1-98 01 02 «Защита информации в телекоммуникациях

Минск БГУИР 2018

УДК 004.056:336.71(076)
ББК 32.973.26-018.2я73
Б82

Рецензенты:

кафедра автоматизированных систем управления войсками учреждения образования «Военная академия Республики Беларусь» (протокол №5 от 20.04.2017);

доцент кафедры управления информационными ресурсами Академии управления при Президенте Республики Беларусь, кандидат технических наук, доцент Н. И. Белодед

Борботько, Т. В.

Б82 Защита информации в банковских технологиях : учеб.-метод. пособие / Т. В. Борботько, О. В. Бойправ. – Минск : БГУИР, 2018. – 58 с. : ил.
ISBN 978-985-543-368-3.

Содержит сведения об особенностях организации и автоматизации банковской деятельности, принципах функционирования систем дистанционного банковского обслуживания и электронных платежных систем, а также методах и средствах обеспечения их безопасности.

УДК 004.056:336.71(076)
ББК 32.973.26-018.2я73

ISBN 978-985-543-368-3

СОДЕРЖАНИЕ

1. ОРГАНИЗАЦИЯ И АВТОМАТИЗАЦИЯ БАНКОВСКОЙ ДЕЯТЕЛЬНОСТИ В РЕСПУБЛИКЕ БЕЛАРУСЬ

1.1. Банковская система Республики Беларусь

Банковская система Республики Беларусь является составной частью кредитной системы и представляет из себя совокупность банковских институтов двух уровней. На первом уровне находится Национальный банк Республики Беларусь (центральный банк), а на втором – сеть коммерческих банков. Банковское законодательство устанавливает правовое положение субъектов банковских правоотношений; определяет порядок создания, деятельности, реорганизации и ликвидации банков. В банковском законодательстве заложены основные принципы банковской деятельности, используемые в международной практике:

- регулирование деятельности коммерческих банков и реализация пруденциального (prudence (франц.) – благоразумие, осторожность) надзора осуществляются Национальным банком;
- банковская деятельность и осуществление отдельных операций подлежат обязательному лицензированию;
- банки свободны от обязательств государства, равно как и государство не несет ответственность по обязательствам банков;
- органы государственной власти не вправе вмешиваться в оперативную деятельность банков;
- банки обязаны в период осуществления своей деятельности соблюдать установленные нормативы безопасного ведения дела;
- банки обеспечивают тайну по счетам, вкладам и операциям клиентов в установленных законом рамках.

Приведенные принципы могут быть скорректированы законодательным органом страны при наличии на то объективных экономических причин. Однако при игнорировании этих принципов невозможно построить полноценную банковскую систему, отвечающую международным стандартам. Несоответствие международным стандартам и принципам влечет за собой проблемы с интегрированием национальных банковских систем в мировое экономическое хозяйство.

Национальный банк Республики Беларусь (НБ РБ) представляет первый уровень банковской системы страны. Как центральный банк любой страны он занимается разработкой и проведением совместно с правительством денежно-кредитной политики государства и подотчетен в своей деятельности Президенту Республики Беларусь (в международной практике центральный банк подотчетен высшему законодательному органу страны – парламенту, а его руководитель не является членом правительства в целях сохранения независимости от правительства). Капитал НБ РБ полностью принадлежит государству.

Правовой основой деятельности НБ РБ является Конституция Республики Беларусь, Банковский кодекс Республики Беларусь, Законы Республики Беларусь и нормативные правовые акты Президента Республики Беларусь.

Главная цель политики НБ РБ – обеспечение внутренней и внешней устойчивости национальной денежной единицы и поддержание стабильных цен, обеспечение ликвидности, кредитоспособности и надежности функционирования банковской системы.

Для выполнения своих уставных целей НБ РБ законодательно наделен рядом функций (ст. 26 Банковского кодекса), основные из них:

- осуществление эмиссии денег;
- регулирование денежного обращения;
- регулирование кредитных отношений;
- осуществление валютного регулирования;
- осуществление государственной регистрации банков, кредитных и других учреждений, осуществляющих банковские операции;
- надзор за деятельностью банков по соблюдению ими безопасного и ликвидного функционирования;
- регулирование внешнеэкономической деятельности банков;
- обеспечение единого порядка бухгалтерского учета и отчетности в банковской системе;
- разработка платежного баланса Республики Беларусь;
- определение порядка проведения безналичных и наличных расчетов.

Круг операций, осуществляемых НБ РБ, определяется его функциями и целями как центрального банка страны. Операции НБ подразделяются на пассивные (операции по созданию ресурсов банка) и активные (операции по их размещению). К основным *пассивным операциям* НБ относятся: эмиссия банкнот, прием вкладов кредитных учреждений, представителей иностранных правительств и банков, капиталы и резервы.

К основным *активным операциям* относятся: учетно-ссудные операции, ломбардные кредиты (ссуды под залог векселей, казначейских обязательств и других ценных бумаг), инвестиции в государственные ценные бумаги (основная форма кредитования государства).

Отличительной особенностью операций, проводимых НБ, является то, что они осуществляются не с целью извлечения доходов, а с целью выполнения основных параметров денежно-кредитной политики, используя основные инструменты регулирования рынка.

Условно коммерческие банки можно классифицировать по нескольким группам и формам. Степень детализации критериев классификации банков определяется глубиной требуемого анализа. Критерии также определяются целями анализа. Приведем только несколько критериев, которые могут быть положены в основу классификации банков:

- по финансовому объему (объемы активов и другие показатели);
- по форме собственности (государственные, частные, банки-резиденты, банки с участием иностранного капитала);
- по набору предоставляемых услуг (кредитные, сберегательные);
- по обслуживаемой клиентуре (крупные предприятия, мелкий бизнес, частные лица);

- по отраслевому признаку (промышленность, агросектор, коммунальное хозяйство);

- по организационной структуре (филиальный банк, банковское объединение, единый банк).

Правовой основой создания и прекращения деятельности коммерческих банков в Республике Беларусь являются Банковский кодекс Республики Беларусь и нормативные документы НБ РБ.

Коммерческие банки создаются учредителями (участниками) – юридическими и физическими лицами, за исключением общественных объединений, преследующих политические цели.

Банки могут учреждаться на основе государственной и частной форм собственности в виде акционерных обществ (закрытого или открытого типа) или унитарного предприятия.

В Республике Беларусь могут создаваться универсальные банки, имеющие лицензию на осуществление всех видов банковских операций, а также специализированные банки, деятельность которых направлена на осуществление отдельных банковских операций.

Иностранные учредители могут создавать на территории Республики Беларусь банки со 100%-м собственным капиталом, совместные банки – на долевой основе с белорусскими соучредителями, филиалы – на правах юридического лица и представительства. Размер (квота) участия иностранного капитала в банковской системе Республики Беларусь устанавливается НБ РБ.

Уставный фонд банка состоит из вкладов его учредителей (участников). При создании банка минимальный размер его уставного фонда (устанавливается Национальным банком) должен быть сформирован из денежных средств.

Для формирования уставного фонда банка могут быть использованы только собственные средства учредителей (участников) банка.

К моменту подачи комплекта учредительных документов на регистрацию (перерегистрацию) уставный фонд банка должен быть оплачен полностью. Минимальный размер собственных средств (капитала) установлен для действующего банка в сумме, эквивалентной 5 млн евро; для действующего банка, имеющего лицензию на привлечение во вклады средств физических лиц, – в сумме, эквивалентной 10 млн евро.

Для банков, создаваемых и действующих на территории свободных экономических зон Республики Беларусь (СЭЗ), установлен минимальный размер уставного фонда в сумме 500 тыс. евро.

Денежные взносы в уставный фонд банка могут осуществляться как в национальной денежной единице Республики Беларусь, так и в свободно конвертируемой валюте. При этом минимальный размер иностранных инвестиций в уставный фонд банка определяется в размере, эквивалентном 20 тыс. евро.

При внесении учредителями неденежного вклада в уставный фонд минимальный размер уставного фонда должен быть полностью оплачен в денежной форме. Доля неденежного взноса в уставном фонде, сформированном в размере свыше минимального, не должна превышать 20 % в первые два года работы банка и 10 % в последующие годы.

Банкам могут быть выданы следующие виды лицензий: общая, внутренняя, генеральная, разовая.

Общая лицензия дает право банку осуществлять указанные в ней банковские операции в национальной денежной единице на территории Республики Беларусь. Лицензия выдается во время государственной регистрации.

Внутренняя лицензия дает право банку осуществлять указанные в ней операции в иностранной валюте на территории Республики Беларусь. Лицензия выдается по заявлению банка во время или после государственной регистрации.

Генеральная лицензия дает право банку осуществлять указанные в ней операции как на территории Республики Беларусь, так и за ее пределами. Лицензия выдается по прошествии, как минимум, одного года после государственной регистрации банка. Банку с иностранными инвестициями лицензия может быть выдана ранее указанного срока.

Разовая лицензия дает право банку на проведение конкретной банковской операции в иностранной валюте в разовом порядке.

Лицензия на привлечение во вклады средств физических лиц дает право банку на осуществление операций в национальной денежной единице и в иностранной валюте, а именно:

- привлекать во вклады средства физических лиц;
- открывать и вести счета физических лиц;
- осуществлять расчетное и (или) кассовое обслуживание физических лиц.

Лицензия на осуществление операций с драгоценными металлами и драгоценными камнями дает право банку осуществлять указанные в ней операции. Перечень документов, представляемых для регистрации и получения лицензий, определяется НБ РБ.

Деятельность банков может быть прекращена путем их реорганизации или ликвидации. Реорганизация банка осуществляется в форме слияния, присоединения, преобразования, разделения, выделения. Решение о реорганизации банка принимается собранием акционеров (участников) банка или в случаях, предусмотренных законодательством Республики Беларусь, судом и доводится до сведения всех акционеров (участников) банка и лиц, состоящих в договорных отношениях с ним.

1.2. Межбанковские переводы средств и расчеты

Банковская система Республики Беларусь представляет собой универсальные кредитные институты с полным набором классических банковских услуг, выполняющих следующие функции:

- посредничество в кредите между субъектами, экономно расходующими свои средства (имеющими временный избыток ресурсов) и осуществляющими свою деятельность с превышением расходов над поступлениями (дефицитно расходующих средства);
- посредничество в платежах;
- превращение в капитал денежных доходов и сбережений;

- создание кредитных орудий обращения.

Круг вышеперечисленных функций банковских институтов сформировался в результате эволюционного развития банковского дела.

Существующие в специальной литературе определения коммерческого банка как финансового посредника позволяют выделять в его деятельности пассивные и активные операции.

Пассивные операции обеспечивают банку формирование ресурсов. В структуре банковских пассивов присутствуют собственные средства, заемные и привлеченные. Собственные средства банка (собственный капитал), в отличие от заемных и привлеченных, не обременены обязательствами по возврату. Собственный капитал является финансовой базой развития банка, обеспечивающей покрытие возникающих в процессе работы рисков. Формирование собственного капитала банка осуществляется в первую очередь за счет внешних (привлечение средств в уставный фонд) и внутренних (перераспределение прибыли) источников. В международной практике доля собственного капитала в ресурсах-нетто в пределах 10 % считается нормой. Однако анализ деятельности коммерческих банков в неустойчивой экономической среде (развивающиеся страны и страны с переходной экономикой) дает основание констатировать, что обеспечить покрытие рисков без ущерба для дальнейшего функционирования банка возможно, имея собственный капитал на уровне 20 % и более в ресурсах-нетто.

Операции по открытию и ведению расчетных и депозитных счетов клиентов (юридических и физических лиц), выпуску собственных ценных бумаг (кроме акций), получению межбанковских и централизованных кредитных ресурсов обеспечивают банку формирование ресурсной базы. Иначе говоря, пассивные операции обеспечивают формирование кредитного потенциала банка.

Активные операции заключаются в размещении мобилизованных ресурсов в целях получения доходов без ущерба для ликвидности банка. Уровень доходности банковских активов находится в обратной зависимости от ликвидности. Таким образом, основными критериями активных операций банков должны выступать:

- ликвидность (высоколиквидные, ликвидные, неликвидные);
- доходность (доходные, бездоходные);
- риски (высокий, низкий).

При этом следует иметь в виду, что ни одна категория банковских активов не может быть одновременно ликвидной, приносить высокий уровень дохода и не быть подверженной рискам.

Среди активных операций коммерческих банков выделяют:

- кредитные операции;
- инвестиционную деятельность;
- финансовые услуги;
- кассовые операции;
- прочие операции.

Кредитные операции – предоставление денежных средств другим лицам, в том числе банкам, в размере и на условиях, предусмотренных кредитным до-

говором на принципах срочности, платности и возвратности. Кредитные операции составляют основу активной деятельности банка и обеспечивают основную часть доходов.

Инвестиционная деятельность заключается в приобретении банком ценных бумаг и других финансовых инструментов (акции, облигации, векселя и пр.) и прав по совместной хозяйственной деятельности. Основная цель инвестиционной деятельности заключается в извлечении доходов и обеспечении оптимальной структуры ликвидных активов.

Финансовые услуги относятся по экономической сути к ссудным операциям. К ним относятся факторинговые и лизинговые операции.

Кассовые операции заключаются в своевременном и качественном обслуживании клиентов по приему (инкассированию), хранению и выдаче денежных средств. Ведение кассовых операций регулируется Национальным банком Республики Беларусь.

Прочие операции обеспечивают доходность коммерческого банка за счет работы с иностранной валютой, по агентским трастовым, расчетным и другим договорам.

Межбанковские расчеты по крупным и срочным денежным переводам и по результатам проведенного клиринга (по прочим денежным переводам, по сделкам купли-продажи ценных бумаг, по операциям с банковскими пластиковыми карточками) производятся в системе BISS.

Межбанковские расчеты в системе BISS осуществляются на основании электронных платежных документов и не сопровождаются обменом копиями расчетных документов на бумажных носителях. Минимальная сумма крупного денежного перевода устанавливается НБ РБ.

Банк-отправитель на основании первичных расчетов документов, оформленных в соответствии с законодательством Республики Беларусь, составляет от своего имени электронные платежные документы, удостоверяет их электронно-цифровой подписью и передает в систему BISS. Электронный платежный документ должен содержать все реквизиты первичных расчетных документов, включая текстовые реквизиты и очередность платежа. Ответственность за сохранение в электронном платежном документе неизменным содержания реквизитов первичного расчетного документа несет банк-отправитель.

Электронные платежные документы с момента приема системой BISS обрабатываются по мере их поступления по принципу «первый пришел – первым ушел». После их обработки система BISS формирует и направляет банку-отправителю электронный служебный документ, подтверждающий списание средств с корреспондентского счета, банку-получателю – электронный документ, подтверждающий зачисление средств на корреспондентский счет и оригинал электронного платежного документа банка-отправителя.

Корреспондентский счет – счет, открываемый одним банком другому, на котором отражаются операции, производимые одним банком по поручению и за счет другого банка на основании межбанковского корреспондентского сообщения.

Если на момент поступления в систему BISS электронных платежных документов на корреспондентском счете банка-отправителя нет достаточных средств или средства зарезервированы банком, электронные платежные документы ставятся в очередь ожидания средств. Очередь ожидания формируется в соответствии с приоритетами, установленными банком-отправителем.

Электронные платежные документы, не выполненные к моменту закрытия операционного дня системы BISS, автоматически аннулируются. Системой BISS формируются и направляются в банки-отправители электронные служебные документы об аннулированных электронных платежных документах.

1.3. Архитектура автоматизированной банковской системы

Основные принципы построения современных АБС: модульность; единство информационного пространства; обеспечение безопасности.

АБС включает в себя следующие уровни:

1. Front office (верхний уровень), который образуют модули, обеспечивающие быстрый и удобный ввод информации, ее первичную обработку и любое внешнее взаимодействие банка с клиентами, другими банками, НБ, информационными и торговыми агентами (программными системами по обработке информации).

2. Back office (средний уровень), который составляют специальные приложения, которые соответствуют разным направлениям внутрибанковской деятельности и внутренним расчетам (работа с кредитами, депозитами, ценными бумагами, платежными карточками и т. д.).

3. Accounting (нижний уровень), который образуют модули, которые выполняют базовые функции бухгалтерского учета или составляют бухгалтерское ядро.

Структура АБС представлена на рис. 1.1.

Рис. 1.1. Структура АБС

Электронное сообщение – информация, подлежащая передаче и включающая данные об одной или нескольких финансовых операциях, а также сведения, связанные с этими операциями.

Концепции развития АБС следующие:

1. Единая программа для выполнения однотипных операций (расчетно-кассовое обслуживание, депозиты или кредиты).

2. Многокомпонентная (модульная) система для широкого спектра операций (рис. 1.2).

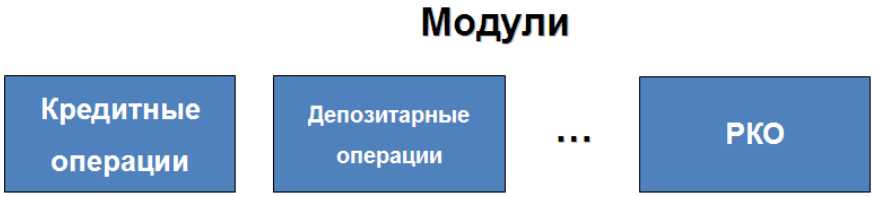

Рис. 1.2. Структурная схема модульной системы

Схема, соответствующая архитектуре АБС, базирующейся на общем финансовом ядре, представлена на рис. 1.3.

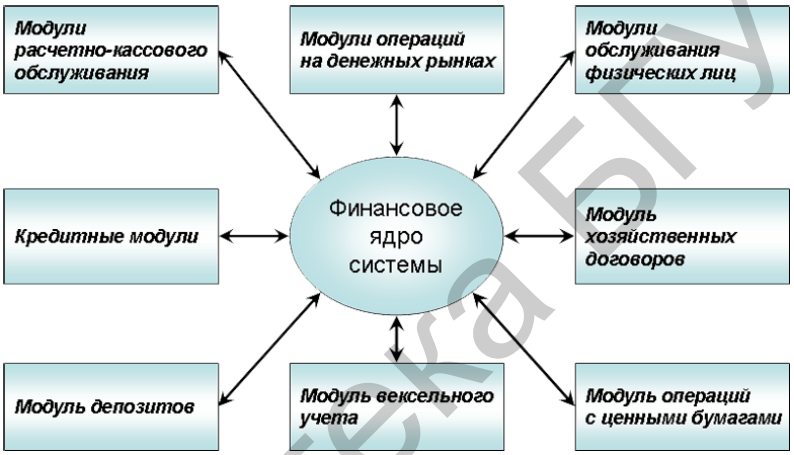

Рис 1.3. Архитектура АБС, базирующейся на общем финансовом ядре

Выделяются следующие разновидности схем построения АБС:

- централизованная;
- консолидационная;
- репликационная;
- распределенная.

Особенности *централизованной* схемы построения АБС:

1. Для ведения всех баз данных используется центральный вычислительный комплекс (ЦВК), находящийся в головном учреждении банка.

2. Доступ к данным из филиалов осуществляется в режиме «клиент-сервер».

3. Обработка всей информации производится ЦВК.

Достоинство централизованной схемы построения АБС – гарантия актуальности данных в любой момент, недостаток – большая нагрузка на ЦВК и высокие требования к надежности связи.

Особенности *консолидационной* схемы построения АБС:

1. Каждый филиал практически автономен.

2. Для ведения баз данных используется вычислительный комплекс филиала, там же производятся и все операции.

3. Расчеты между банковскими филиалами осуществляются по клиринговой схеме.

4. С определенной периодичностью филиалы подключаются к ЦВК головного учреждения для клиринга и (или) консолидации баланса.

Достоинство консолидационной схемы построения АБС – неограниченное число уровней иерархии в структуре банка. Недостатки схемы: банк не имеет оперативного представления ни о текущем состоянии своих активов, ни об их движении; клиенты не могут рассчитывать на получение во всех учреждениях банка одинакового набора услуг.

Особенности *репликационной* схемы построения АБС:

1. Каждое учреждение банка имеет полнофункциональный вычислительный комплекс, работающий в автономном режиме.

2. Периодически производятся сеансы связи между филиалами и головным отделением.

3. Во время сеанса связи производится не просто консолидация баланса, а полная актуализация баз данных.

Достоинство репликационной схемы построения АБС заключается в том, что каждый филиал имеет полную актуальную БД. Недостатки схемы: высокие требования к вычислительным мощностям и телекоммуникациям; необходимость частой репликации БД.

Особенности *распределенной* схемы построения АБС:

1. Предполагает использование монитора (менеджера) транзакций, который изолирует «клиентскую» часть от «серверной».

2. Со стороны клиента монитор транзакций выглядит как обычный сервер, со стороны сервера – как обычный клиент.

3. Принципиальная разница заключается в том, что монитор транзакций «знает», на каком (или на каких) из серверов размещены данные, к которым обращается клиент.

4. Отдельные части этой информации могут находиться на разных серверах, тем не менее благодаря монитору транзакций клиент обращается к ним так, как будто они располагаются на одном сервере.

Достоинство распределенной схемы построения АБС – наличие возможности обращаться к любым имеющимся данным в режиме реального времени. Недостатки схемы: сложность; необходимость высокой квалификации персонала; высокая стоимость; необходимость надежных телекоммуникаций.

1.4. Автоматизированная система межбанковских расчетов

Автоматизированная система (АС) межбанковских расчетов (МБР) – совокупность норм, правил, процедур и программно-технических средств, обеспечивающих осуществление межбанковских расчетов.

Участники АС МБР:

- НБ РБ;
- банки.

Состав АС МБР:

- АС «Центральный архив МБР» принимает на хранение электронные платежные документы и электронные сообщения по межбанковским расчетам и обеспечивает их сохранность и использование в интересах участников системы BISS в порядке, определенном иным банковским законодательством;
- система передачи финансовой информации (СПФИ) – совокупность программно-технических комплексов, обеспечивающих надежную и безопасную передачу электронных платежных документов и электронных сообщений по межбанковским расчетам);
- BISS (ядро АС МБР).

Схема, соответствующая архитектуре АС МБР, представлена на рис. 1.4.

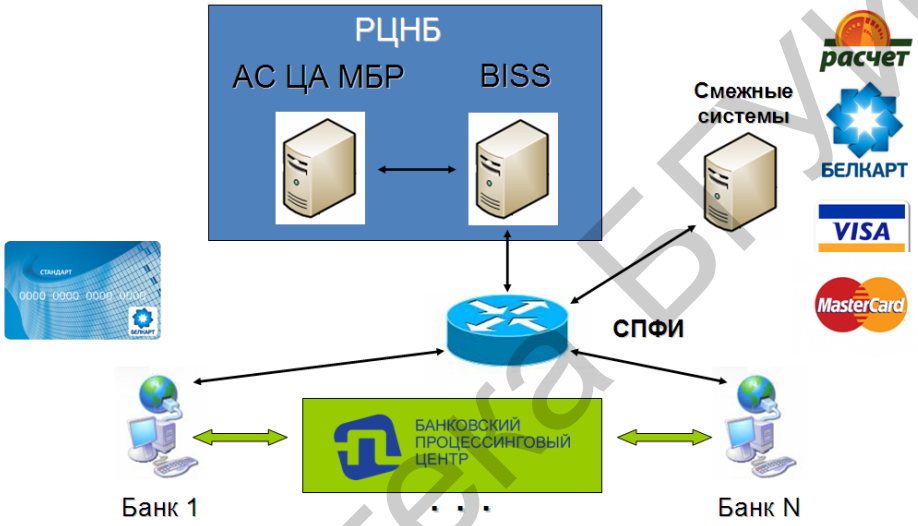

Рис. 1.4. Архитектура АС МБР

Банковский процессинговый центр – центр, осуществляющий на договорных условиях процессинг по операциям с использованием банковских платежных карточек и клиринг по денежным требованиям и обязательствам банков Республики Беларусь.

1.5. Автоматизированная информационная система единого расчетного и информационного пространства

Единое расчетное и информационное пространство – 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.

Основные участники автоматизированной информационной системы (АИС) ЕРИП:

- потребитель услуг (плательщик) – физическое или юридическое лицо, потребляющее услуги производителей услуг и производящее оплату за услуги через расчетных агентов;

- производитель услуг (поставщик) – юридическое лицо, оказывающее услуги юридическим и физическим лицам и получающее за эти услуги оплату на свои расчетные счета через расчетных агентов;

- расчетный агент – банк, небанковская кредитно-финансовая организация, организация почтовой и электрической связи, осуществляющая роль посредника при приеме платежей от потребителей услуг в пользу производителей услуг.

Основные задачи АИС ЕРИП:

- обеспечение расчетных агентов информацией, необходимой для приема платежей за услуги, оказанные исполнителями услуг;

- контроль прохождения платежей для обеспечения своевременности и полноты поступления на расчетные счета исполнителей услуг денежных средств потребителей услуг;

- предоставление исполнительным комитетам необходимой статистической и учетной информации.

Схема, соответствующая архитектуре АИС ЕРИП, представлена рис. 1.5.

Рис. 1.5. Архитектура АИС ЕРИП

Банк производителя услуг – банк, в котором открыт расчетный счет производителя услуг, на который поступают денежные средства за оказанные услуги и с которым заключен договор на расчетно-кассовое обслуживание.

Расчетный агент – банк, небанковская кредитно-финансовая организация, предоставляющие информацию, необходимую для осуществления платежей.

Биллинговая система – программный комплекс, осуществляющий учет объема потребляемых абонентами услуг, расчет и списание денежных средств в соответствии с тарифами компании.

Расчетная система ЕРИП обеспечивает прием и гарантию перечисления денежных средств за оказанные услуги от потребителя этих услуг производителю услуг.

Основные функции центрального узла (ЦУ):

- подготовка необходимой нормативно-справочной информации и распространение ее участникам системы;

- прием от региональных узлов требований к оплате производителей услуг;

- предоставление доступа расчетным агентам к консолидированной базе данных требований на оплату всех производителей услуг;

- контроль процесса выполнения платежей в пользу производителей услуг и проведение расчетов между участниками;

- осуществление мониторинга работы всей системы;

- предоставление аналитической и статистической информации заинтересованным участникам по системе в целом.

Основные функции регионального узла (РУ):

- регистрация условий договоров с производителями услуг;

- выполнение приема и обработки требований к оплате производителей услуг и передача полученных данных в центральный узел;

- информирование производителей услуг о совершенных платежах в их пользу, предоставление аналитической и статистической информации местным органам власти.

РУ – структурное подразделение НБ РБ (в составе Главных управлений НБ РБ по областям), осуществляющее взаимодействие с производителями услуг в регионе и ЦУ.

1.6. Обеспечение информационной безопасности автоматизированных банковских систем

Специфика защиты АБС обусловлена особенностями решаемых ими задач. Как правило, АБС обрабатывают большой поток постоянно поступающих запросов в реальном масштабе времени, каждый из которых не требует для обработки многочисленных ресурсов, но все вместе они могут быть обработаны только высокопроизводительной системой.

В АБС хранится и обрабатывается конфиденциальная информация, не предназначенная для широкой публики. Подделка ее или даже утечка могут привести к серьезным (для банка или его клиентов) последствиям. Поэтому АБС обречены оставаться относительно закрытыми, работать под управлением специфического программного обеспечения и уделять большое внимание обеспечению своей безопасности.

Другой особенностью АБС являются повышенные требования к надежности аппаратного и программного обеспечения. В силу этого многие современные АБС тяготеют к так называемой отказоустойчивой архитектуре («fault-tolerant») компьютеров, позволяющей осуществлять непрерывную обработку информации даже в условиях различных сбоев и отказов.

Можно выделить два типа задач, решаемых АБС:

1. Аналитические. К этому типу относятся задачи планирования, анализа счетов и т. д. Они не являются оперативными и могут требовать для решения длительного времени, а их результаты могут оказать влияние на политику банка в отношении конкретного клиента или проекта. Поэтому подсистема, с помощью которой решаются аналитические задачи, должна быть надежно изолирована от основной системы обработки информации.

Для решения такого рода задач обычно не требуется мощных вычислительных ресурсов, обычно достаточно 10–20 % мощности всей системы. Однако ввиду возможной ценности результатов их защита должна быть постоянной.

2. Повседневные. К этому типу относятся задачи, решаемые в повседневной деятельности, в первую очередь, – выполнение платежей и корректировка счетов. Именно они и определяют размер и мощность основной системы банка. Для их решения обычно требуется гораздо больше ресурсов, чем для аналитических задач.

В то же время ценность информации, обрабатываемой при решении таких задач, имеет временный характер. Постепенно ценность информации, например, о выполнении какого-либо платежа, становится неактуальной. Естественно, это зависит от многих факторов, а именно: суммы и времени платежа, номера счета, дополнительных характеристик и т. д. Поэтому обычно бывает достаточным обеспечить защиту платежа именно в момент его осуществления. При этом защита самого процесса обработки и конечных результатов должна быть постоянной.

Главное в защите финансовых организаций – оперативное и по возможности полное восстановление информации после аварий и катастроф. В основном защита информации от разрушения достигается созданием резервных копий и их внешним хранением, использованием средств бесперебойного электропитания и организацией горячего резерва аппаратных средств.

Следующая по важности для финансовых организаций проблема – это управление доступом пользователей к хранимой и обрабатываемой информации. Здесь широко используются различные программные системы управления доступом, которые иногда могут заменять и антивирусные программные средства. В основном используются приобретенные программные средства управления доступом. Причем в финансовых организациях особое внимание уделяют такому управлению пользователей именно в сети.

В государственных организациях гораздо шире применяются сертифицированные NCSC программные средства. Это объясняется существующими требованиями к обработке информации. Для защиты от компьютерных вирусов широко применяются специализированные антивирусные пакеты. Средства разграничения доступа используются намного реже.

К отличиям организации защиты информационных сетей в финансовых учреждениях можно отнести широкое использование коммерческого программного обеспечения для управления доступом к сети, защита точек подключения к системе через коммутируемые линии связи. Другие способы защиты, такие как применение антивирусных средств, оконечное и канальное шифрование передаваемых данных, аутентификация сообщений, в основном применяются примерно одинаково (за исключением антивирусных средств).

Большое внимание как в финансовых, так и в государственных организациях уделяется физической защите помещений, в которых расположены компьютеры. Это означает, что защита ПК от доступа посторонних лиц решается не только с помощью программных средств, но и организационно-технических (охрана, кодовые замки и т. д.).

Шифрование локальной информации применяют чуть более 20 % финансовых организаций. Причинами этого являются сложность распространения ключей, жесткие требования к быстродействию системы, а также необходимость оперативного восстановления информации при сбоях и отказах оборудования.

Значительно меньшее внимание в финансовых организациях уделяется защите телефонных линий связи (4 %) и использованию ПК, разработанных с учетом требования стандарта Tempest (защита от утечки информации по каналам электромагнитных излучений и наводок). В государственных организациях решению проблемы противодействия получению информации с использованием электромагнитных излучений и наводок уделяют гораздо большее внимание.

Защита финансовых организаций (в том числе и банков) строится несколько иначе, чем государственных (в том числе и военных) организаций. Следовательно, для защиты АБС нельзя применять те же самые технические и организационные решения, которые были разработаны для государственного сектора.

Защита АБС должна разрабатываться для каждой системы индивидуально в соответствии с общими правилами:

- анализ риска, заканчивающийся разработкой проекта системы и планов защиты, непрерывной работы и восстановления;
- реализация системы защиты на основе результатов анализа риска;
- постоянный контроль за работой системы защиты и АБС в целом (программный, системный и административный).

На каждом этапе реализуются определенные требования к защите. Их точное соблюдение приводит к созданию безопасной системы.

Каждую систему защиты информации АБС следует разрабатывать индивидуально, учитывая следующие особенности:

- организационную структуру банка;
- объем и характер информационных потоков (внутри банка в целом, внутри отделов, между отделами, внешних потоков);
- количество и характер выполняемых операций: аналитических и повседневных (один из ключевых показателей активности банка – число банковских операций в день – является основой для определения параметров системы);
- количество персонала и его функциональные обязанности;
- количество и характер клиентов;
- график суточной нагрузки и др.

Этапы построения защиты автоматизированных банковских систем следующие:

1. *Анализ возможных угроз*. Фиксирование конфигурации аппаратных и программных средств, технологии обработки информации и определения возможных воздействий на каждый компонент системы.

2. *Разработка системы защиты*. Документ, содержащий перечень защищаемых компонентов и возможных воздействий на них, цель, правила обработки информации, обеспечивающие ее защиту от различных воздействий, описание разработанной системы защиты.

3. *Реализация системы защиты*. Установка и настройка средств защиты, необходимых для реализации зафиксированных в плане защиты правил обработки информации.

Механизмы реализации системы защиты следующие:

1. *Добавленная защита (add-on)*. Используются дополнительные программно-аппаратные средства. Средства защиты поддерживаются внутренними механизмами АС.

2. *Встроенная защита (built-in)*. Механизмы защиты – часть АС. Механизмы защиты могут быть распределенными. Средства защиты – единый механизм обеспечения информационной безопасности (ИБ).

3. *Сопровождение системы защиты*. Аудит и корректировка действий на первых трех этапах.

Организация группы управления защитой информации, включающей специалистов в этой области, – одна из наиболее важных задач управления защитой АБС. Иногда эту группу называют также группой информационной безопасности.

В обязанности входящих в эту группу сотрудников должно быть включено не только исполнение директив вышестоящего руководства, но и участие в выработке решений по всем вопросам, связанным с процессом обработки информации с точки зрения обеспечения его защиты. Более того, все их распоряжения, касающиеся этой области, обязательны к исполнению сотрудниками всех уровней и организационных звеньев. Кроме того, организационно эта группа должна быть обособлена от всех отделов или групп, занимающихся управлением самой системой, программированием и другими относящимися к системе задачами во избежание возможного столкновения интересов.

Несмотря на то что обязанности и ответственность сотрудников группы информационной безопасности варьируются от организации к организации, можно составить перечень основных функциональных обязанностей сотрудников группы информационной безопасности во всех учреждениях:

1. Управление доступом пользователей системы к данным, включая установку (периодическую) и смену паролей, управление средствами защиты коммуникаций и криптозащиту предаваемых, хранимых и обрабатываемых данных.

2. Разработка планов защиты, обеспечение непрерывной работы и восстановления (ОНРВ) функционирования. Контроль за их соблюдением, а также контроль за хранением резервных копий.

3. Доведение до пользователей изменений в области защиты, которые имеют к ним отношение, обучение персонала и пользователей АБС.

4. Взаимодействие со службой менеджмента АБС по вопросам защиты информации в АБС.

5. Совместная работа с представителями других организаций по вопросам безопасности (непосредственный контакт или консультации с партнерами или клиентами).

6. Тесное сотрудничество и поддержание хороших отношений со службой менеджмента и администрацией АБС.

7. Расследование происшедших нарушений защиты.

8. Координация действий с аудиторской службой, совместное проведение аудиторских проверок.

9. Постоянная проверка соответствия принятых в организации правил безопасности обработки информации существующим правовым нормам, контроль за соблюдением этого соответствия.

10. Поддержание хороших отношений с теми отделами, чьи задачи могут (по каким-то особым причинам) выполняться в обход существующих правил.

Естественно, все эти задачи не под силу выполнить одному человеку, особенно если организация (банк) довольно велика. Более того, в группу управления защитой могут входить сотрудники с разными функциональными обязанностями. Обычно выделяют четыре группы сотрудников (по возрастанию иерархии):

1. Сотрудник группы безопасности. В его обязанности входит обеспечение должного контроля за защитой наборов данных и программ, помощь пользователям и организация общей поддержки групп управления защитой и менеджмента в своей зоне ответственности. При децентрализованном управлении каждая подсистема АБС имеет своего сотрудника группы безопасности.

2. Администратор безопасности системы. В его обязанности входит ежемесячная публикация нововведений в области защиты, новых стандартов, а также контроль за выполнением планов непрерывной работы и восстановления (если в этом возникает необходимость), а также за хранением резервных копий.

3. Администратор безопасности данных. В его обязанности входит реализация и изменение средств защиты данных, контроль за состоянием защиты наборов данных, ужесточение защиты в случае необходимости, а также координирование работы с другими администраторами.

4. Руководитель (начальник) группы по управлению обработкой информации и защитой. В его обязанности входит разработка и поддержка эффективных мер защиты при обработке информации для обеспечения сохранности данных, оборудования и программного обеспечения; контроль за выполнением плана восстановления и общее руководство административными группами в подсистемах АБС (при децентрализованном управлении).

Существует несколько вариантов детально разработанного штатного расписания такой группы, которые включают перечень функциональных обязанностей, необходимых знаний и навыков, распределение времени и усилий. При организации защиты существование такой группы и детально разработанные обязанности ее сотрудников совершенно необходимы.

1.7. Системы резервного копирования данных

Резервное копирование данных (backup) – комплекс мер, направленных на сохранение целостности информации и быстрое ее восстановление после программных или аппаратных сбоев.

Объекты резервного копирования:

- системные разделы и диски;
- базы данных;

- файлы;
- настройки;
- операционные системы.

Принципы резервного копирования данных:

- полное;
- инкрементное;
- дифференциальное.

При полном резервном копировании в архив включаются все архивируемые данные по состоянию на момент создания архива.

Инкрементный архив содержит только данные, изменившиеся с момента создания последнего архива.

При дифференциальном копировании создается независимый файл, содержащий все изменения данных по отношению к последнему полному архиву.

Режимы резервного копирования :

- автоматический (по определенному расписанию);
- ручной (по мере необходимости).

Для резервного копирования данных используются различные программные средства, наиболее распространенными среди которых являются программы компаний Acronis, Norton.

2. ЭЛЕКТРОННЫЕ ПЛАТЕЖНЫЕ СИСТЕМЫ

2.1. Технология электронного обмена данными

EDI – технология электронного обмена данными, которая применяется в той области электронной коммерции, где основными участниками являются юридические лица.

Цель EDI – создание процедур обмена информацией с предопределенным форматом, между различными информационными системами двух и более организаций в процессе заключения сделок, выполнения заказов и контрактов.

Преимущества системы EDI:

- сокращение бумажного документооборота;
- сокращение времени на приемку/поставку товаров;
- сокращение расходов.

Основные функции системы EDI:

- формирование структурированных данных;
- управление передачей данных;
- обеспечение безопасности;
- формирование электронных накладных.

Электронные накладные – информация по поставке товара и расчету налога на добавленную стоимость.

На рис. 2.1 представлена схема EDI системы TOPBY.

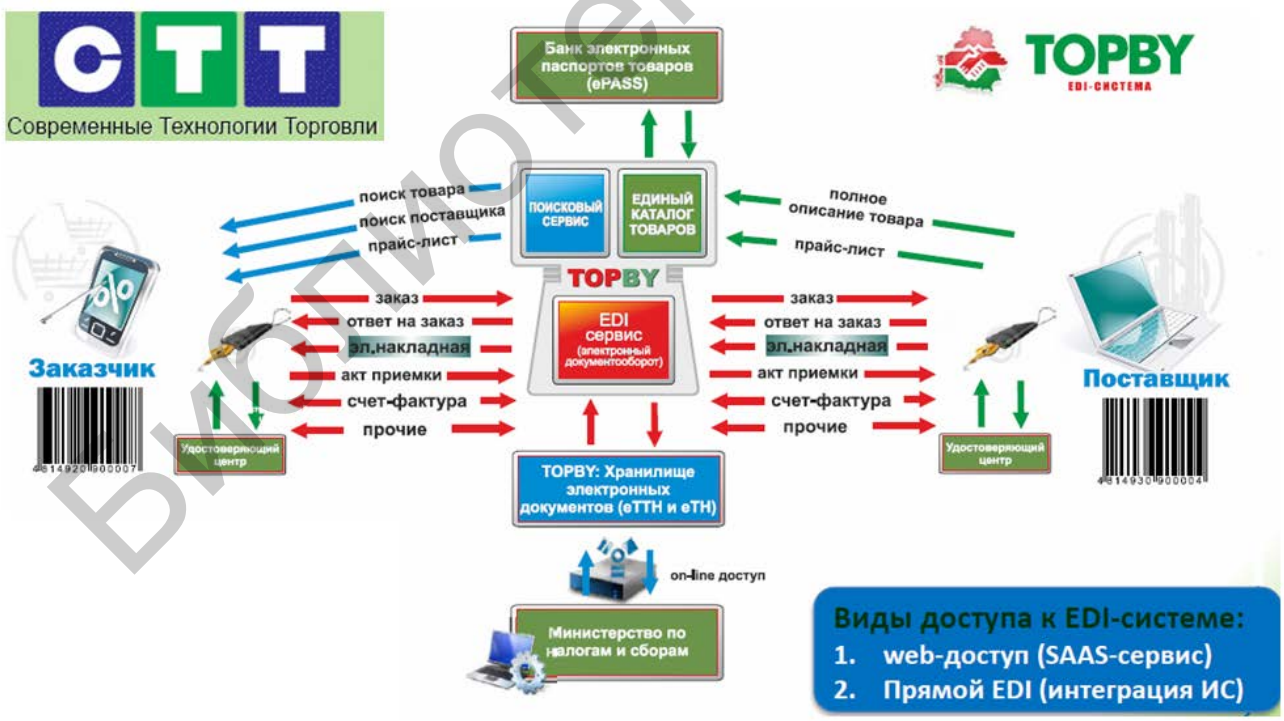

Рис. 2.1. Схема EDI системы TOPBY

Схема интеграции систем EDI и «клиент-банк» представлена на рис. 2.2.

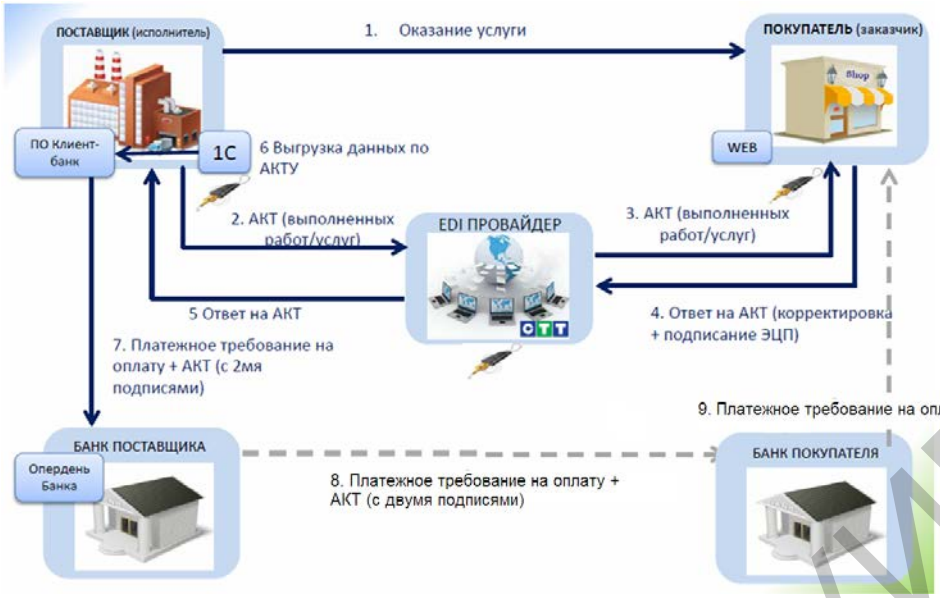

Рис. 2.2. Интеграция систем EDI и «клиент-банк»

Основные принципы управления передачей данных:

- управление должно выполняться как внутри организации, так и во внешней телекоммуникационной сети;
- полученные сообщения должны быть переданы приложению, ответственному за их обработку, в то время как сообщения для партнеров должны объединяться в единое сообщение перед отправкой получателю;
- телекоммуникационные функции должны реализовывать как внутренние протоколы обмена данными, так и протоколы, использующиеся партнерами.

Основные функции программного обеспечения системы EDI:

- управление внутренними сообщениями системы (проверка, сохранение, получение, доставка и т. д.);
- синхронизация данных различных подразделений предприятия;
- глобальный аудит транзакций для поддержания целостности данных системы и обеспечения защищенности системы.

2.2. Структура электронной платежной системы

Участники электронной платежной системы (ЭПС):

- платежные агрегаторы;
- производители услуг;
- провайдер платежных сервисов;
- покупатели.

Производитель услуг – юридическое лицо, индивидуальный предприниматель, реализующие товары (работы, услуги).

Провайдер платежных сервисов – юридическое лицо, оказывающее организациям торговли (сервиса) и банкам услуги по приему платежей в их адрес.

Схема взаимодействия участников ЭПС представлена на рис. 2.3.

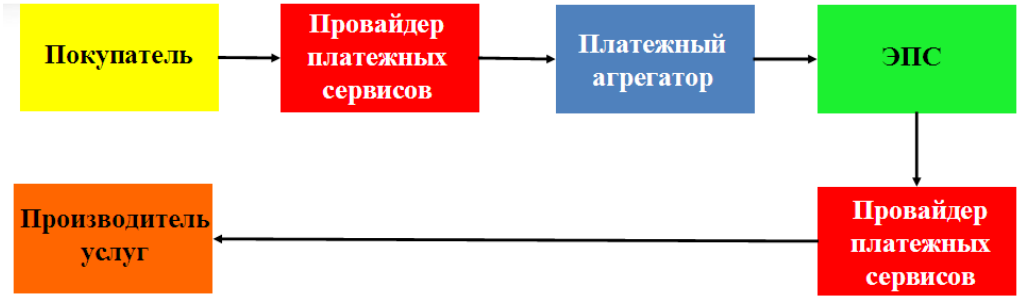

Рис. 2.3. Схема взаимодействия участников ЭПС

Платежный агрегатор – юридическое лицо, обеспечивающее на основании заключенного с производителем услуг договора информационное и (или) финансовое взаимодействие указанного производителя услуг и его клиентов.

Преимущества платежных агрегаторов:

- снижение временных и финансовых затрат продавцов;
- обеспечение широкого выбора способов оплаты для покупателей.

Схема, соответствующая типовой архитектуре платежной системы, представлена на рис. 2.4.

Рис. 2.4. Типовая архитектура платежной системы

Эквайер – организация, реализующая выполнение необходимых операций по обеспечению взаимодействия участников обслуживания средствами платежной системы.

Эмитент – организация, обеспечивающая выпуск платежных карт и гарантирующая выполнение финансовых обязательств, связанных с использованием выпущенного ею платежного средства.

Назначение платежной системы БЕЛКАРТ – обеспечение эмиссии, эквайринга, процессинга при проведении расчетов с использованием банковских платежных карт (БПК).

Участники платежной системы БЕЛКАРТ:

- банки - резиденты Республики Беларусь;
- ОАО «Банковский процессинговый центр»;
- расчетный банк – Национальный банк Республики Беларусь.

Функция банка-резидента платежной системы БЕЛКАРТ – выпуск (эмиссия) платежных карт и обеспечение финансовых операций с их использованием.

Функции ОАО «Банковский процессинговый центр» – ведение авторизационной базы и маршрутизация авторизационных запросов; обработка операций, совершенных по карточкам банка и в эквайринговой сети банка.

Функция расчетного банка – выполнение расчетов по межбанковским операциям.

Схема проведения транзакций в системе БЕЛКАРТ представлена на рис. 2.5.

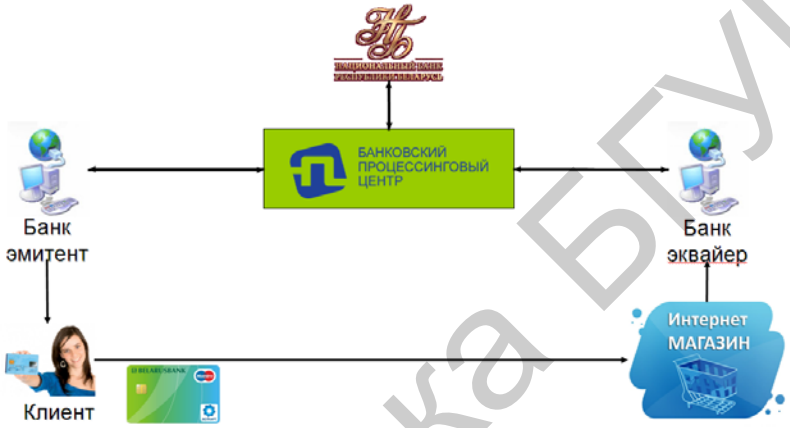

Рис. 2.5. Схема проведения транзакций в системе БЕЛКАРТ

2.3. Технология электронных денег

Электронные деньги (ЭД) – хранящиеся в электронном виде единицы стоимости, выпущенные в обращение в обмен на наличные или безналичные денежные средства и принимаемые в качестве средства платежа при осуществлении расчетов.

Покупательская способность ограничена кругом организаций, принимающих платежи.

Право выпуска в обращение ЭД предоставлено только банкам и небанковским кредитно-финансовым организациям Республики Беларусь.

Виртуальные деньги отличаются от электронных тем, что их поддержка, представление и способ использования нематериальны. Можно их рассматривать как ссылку на некоторый счет.

Скриптуальный характер электронных и виртуальных денег связан со статусом эмитента (т. к. они не выпускаются центральным банком), а также с возможностью оперативного контроля транзакций и движения денег.

Электронный кошелек – устройство с памятью, учитывающее средства, которыми обладает его владелец (рис. 2.6).

Рис. 2.6. Схема функционирования системы с электронными кошельками

Консолидированный счет отражает общий баланс всех электронных кошельков.

Способы реализации электронных кошельков:

- в виде аппаратных средств;
- в виде программных средств.

2.4. Международная платежная система SWIFT

Сообщество SWIFT (англ. Society for Worldwide Interbank Financial Telecommunications) было основано в 1973 г. Первые операции с применением платежной системы SWIFT I начали осуществляться в 1977 г.

Система SWIFT II была внедрена и пришла на смену SWIFT I в 1990 г. В настоящее время жители более 90 стран мира являются ее пользователями.

Основные преимущества системы заключаются в следующем:

- использование актуальных способов передачи информации, стандартизация и оптимизация этого процесса, что повышает эффективность функционирования банков;
- гарантированная надежность процесса обмена сообщениями;
- низкие затраты на оплату услуг передачи сообщений за счет высокой интенсивности трафика;
- возможность для пользователей получать доступ к их корреспондентам по всему миру (длительность процесса доставки сообщения – от 5 до 20 мин в зависимости от его приоритета);
- отсутствие проблем языкового барьера между участниками процесса обмена сообщениями за счет использования общего единого формата последних;
- повышение конкурентоспособности банков-членов SWIFT за счет того, что международный и кредитный оборот все более концентрируется на пользователях SWIFT;
- возможность использования системы в качестве форума для достижения договоренности о стандартах, касающихся способов представления и передачи сообщений.

Выделяют четыре уровня в архитектуре SWIFT (рис. 2.7):
1) банковский терминал;
2) региональный процессор;
3) слайс-процессор;
4) процессор управления системой.

Рис. 2.7. Архитектура системы SWIFT II

Банковский терминал располагается в банке. Он используется для предоставления персоналу банка доступа в сеть. В системе SWIFT в качестве банковских терминалов, как правило, используются ПК.

Назначение *регионального процессора* – обеспечение взаимодействия между пользователями системы SWIFT, которые находятся в пределах одного государства или группы государств.

Слайс-процессор обеспечивает обмен сообщениями между региональными процессорами, которые к нему подключены. Ежедневно слайс-процессор обрабатывает до полутора миллионов сообщений. Кроме того, его назначение заключается в архивировании сообщений (как кратко-, так и долгосрочном периоде), а также формировании системных отчетов. Длительность хранения сообщения в архиве слайс-процессора не превышает 14 дней. Актуальность архивирования сообщений обусловлена необходимостью решения проблем, связанных с некорректной интерпретацией сообщений. В настоящее время существует два слайс-процессора, каждый из которых построен с применением трех машин A12 (фирма производитель – Unisys). При этом одна из этих машин является резервной.

Процессор управления системой используется в следующих целях:
- мониторинг системы SWIFT;
- контроль процесса передачи сообщений в системе SWIFT;
- контроль состояния слайс-процессоров и региональных процессоров;
- управление работой слайс-процессоров и региональных процессоров;

- управление работой сетевых программ и банковских терминалов;

- контроль прикладных задач, которые выбираются пользователем.

В настоящее время существует два процессора управления системой. Один из них расположен в Нидерландах, а второй – в Соединенных Штатах Америки.

Процессор управления системой не задействован в реализации механизмов обработки сообщений.

На рис. 2.8 показаны пути передачи сообщений и платежей в системе SWIFT.

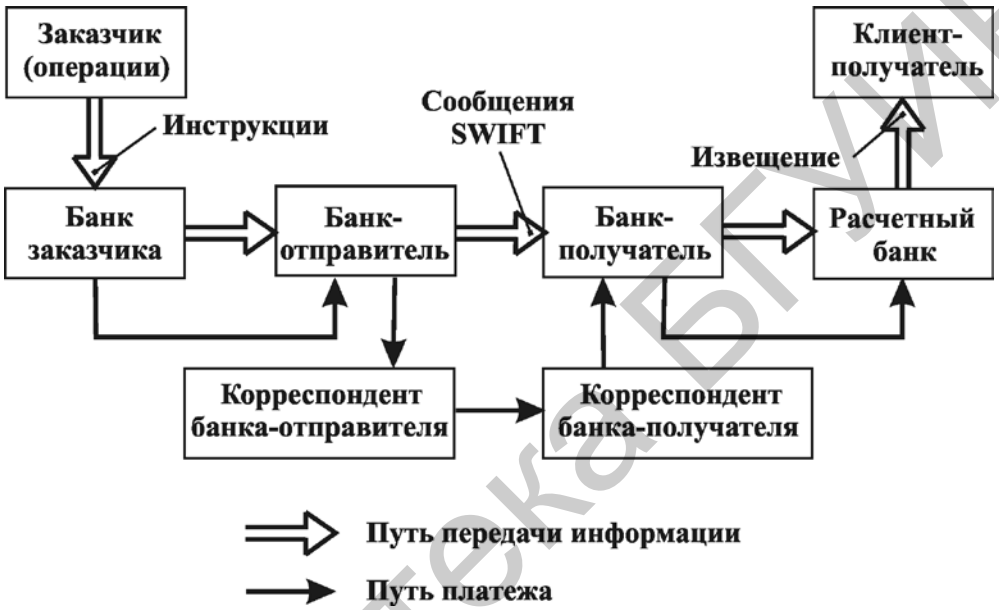

Рис. 2.8. Процесс передачи сообщений и осуществления платежей

Структурными элементами сообщений, передаваемых посредством системы SWIFT, являются поля, с использованием которых выполняется процедура идентификации всех участников передачи этого сообщения, а также платежей.

Алгоритм выполнения расчетов с использованием системы SWIFT следующий:

1. Банк субъекта, который является заказчиком операции, информирует банк-отправитель о необходимости отправить сообщение. После этого первый банк переводит второму необходимую сумму денежных средств.

2. После приема сообщения банк получателя переводит полученную сумму на счет банка, который осуществляет платежи.

3. Уведомление о платежах банков-корреспондентов, которое реализуется путем отправки им специальных сообщений. Если в процессе участвуют четыре банка, являющихся посредниками, то в полях отправляемого сообщения должны содержаться сведения, необходимые для идентификации банка-заказчика, расчетного банка и банков-корреспондентов отправителя и получателя. В тексте сообщения при этом не указываются данные, необходимые для идентификации отправителя и получателя, т. к. эти данные находятся в заголовке сообщения.

3. СИСТЕМЫ ДИСТАНЦИОННОГО БАНКОВСКОГО ОБСЛУЖИВАНИЯ

3.1. Основы построения систем дистанционного банковского обслуживания

Системы дистанционного банковского обслуживания (ДБО) предназначены для управления банковским счетом без физического контакта со специалистом банка. Для использования этой системы необходимо применять оборудование банка и пользователя.

Направления обеспечения информационной безопасности систем ДБО:

- аутентификация участников информационного взаимодействия;
- конфиденциальность и целостность сообщений;
- невозможность отказа от транзакции;
- юридическая значимость электронных документов.

Способы аутентификации в системах ДБО:

- SIM (subscriber identification module);
- уникальный пароль (4–5 символов).

Персональный идентификационный номер (PIN) – последовательность цифр (обычно 4, но может быть до 12), используемая для идентификации клиента банка.

По способу назначения PIN подразделяются на следующие типы:

- назначаемые выведенные;
- назначаемые случайные;
- выбираемые пользователем.

Выделяют следующие способы проверки PIN:

- алгоритмический (рис. 3.1);
- неалгоритмический.

Рис. 3.1. Схема генерации PIN

Если при использовании схемы, представленной на рис. 3.1, в результате обработки не удалось получить требуемое количество десятичных цифр, то из отброшенных комбинаций вычитается 10.

В соответствии с алгоритмическим способом у пользователя запрашивается PIN, который преобразуется по специальному алгоритму, после чего сравнивается со значением PIN, которое хранится на карточке.

Достоинства способа:

- отсутствие копии PIN в базах данных банка, что исключает его похищение сотрудниками банка;
- PIN не передается между терминалом и банком, что исключает возможность его перехвата;
- исключение необходимости передачи PIN между терминалом и банком в режиме реального времени.

В соответствии с неалгоритмическим способом проверка PIN осуществляется путем прямого сравнения полученного PIN со значениями, хранимыми в базе данных банка.

Гарантированность идентификации с использованием PIN возможна при соблюдении следующих условий:

- банковская карта выдается только клиенту;
- клиент не теряет банковскую карту;
- отсутствует возможность подделать или похитить банковскую карту;
- в работе АБС банка отсутствуют сбои;
- в банке нет сотрудников, являющихся мошенниками.

3.2. Архитектура типовых систем дистанционного банковского обслуживания

К типовым системам ДБО относятся:

- интернет-банкинг;
- мобильный банкинг;
- SMS-банкинг.

Схема, соответствующая архитектуре интернет-банкинга, представлена на рис. 3.2.

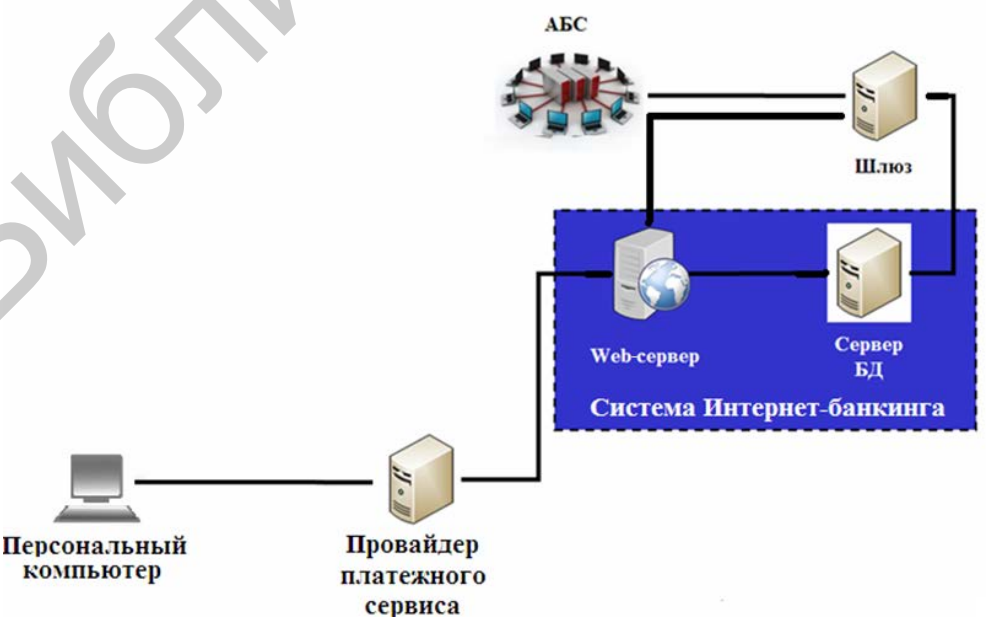

Рис. 3.2. Архитектура системы интернет-банкинга

Преимущества интернет-банкинга для клиента:

- возможность проведения транзакций в удобное для него время;
- не требуется физического присутствия в офисе банка.

Преимущества интернет-банкинга для банка:

- привлечение клиентов без учета территориального фактора;
- снижение затрат за счет сокращения штата сотрудников, экономии на поддержку сети филиалов.

Модели интернет-банкинга:

- традиционные банки, дополняющие свои услуги, онлайновым бизнесом;
- виртуальные банки, работающие только через Интернет.

В мобильном банкинге предполагается использование портативных устройств для получения и передачи информации при совершении транзакций через Интернет. Идентификация клиента проводится с использованием реквизитов его SIM (Subscriber Identification Module – модуль идентификации абонента).

Преимущества мобильного банкинга для клиента:

- возможность проведения транзакций в удобном для него месте и удобное время;
- перечень доступных операций идентичен тем, которые доступны при расчетно-кассовом обслуживании.

Достоинства мобильного банкинга:

- повсеместный доступ (в зоне действия сети);
- не требуется нахождения рядом со стационарным компьютером для выполнения платежей;
- локализация: доступ к информации, относящейся именно к данному региону;
- персонализация: SIM позволяет аутентифицировать владельца.

Недостатки мобильного банкинга:

- ограничения, связанные с пропускной способностью сетей передачи данных;
- небольшие размеры экрана некоторых устройств.

Классы платежей в мобильном банкинге:

- карточные (совместное использование устройства передачи данных вместе с платежной картой);
- бескарточные (выполнение платежей путем дебетирования счета покупателя как клиента компании, предоставляющей услуги сотовой связи, или за счет применения электронных денег).

Особенности реализации интерфейса пользователя мобильного банкинга:

- web-браузер, который позволяет обеспечить работу в системе интернет-банкинга при доступе к ней с портативного устройства (смартфон, планшетный компьютер, сотовый телефон;
- специализированное ПО (прикладное ПО, предназначенное для работы в системе мобильного банкинга).

SMS-банкинг – удаленное управление банковским счетом посредством SMS-сообщений (рис. 3.3).

Рис. 3.3. Схема функционирования SMS-банкинга

3.3. Системы дистанционного банковского обслуживания на основе ATM- и POS-терминалов

Рассмотрим схему прохождения платежа между автоматическим кассовым аппаратом (АКА), банком, которому принадлежит АКА (получатель), и банком, который выпустил карточки (эмитент) (рис. 3.4).

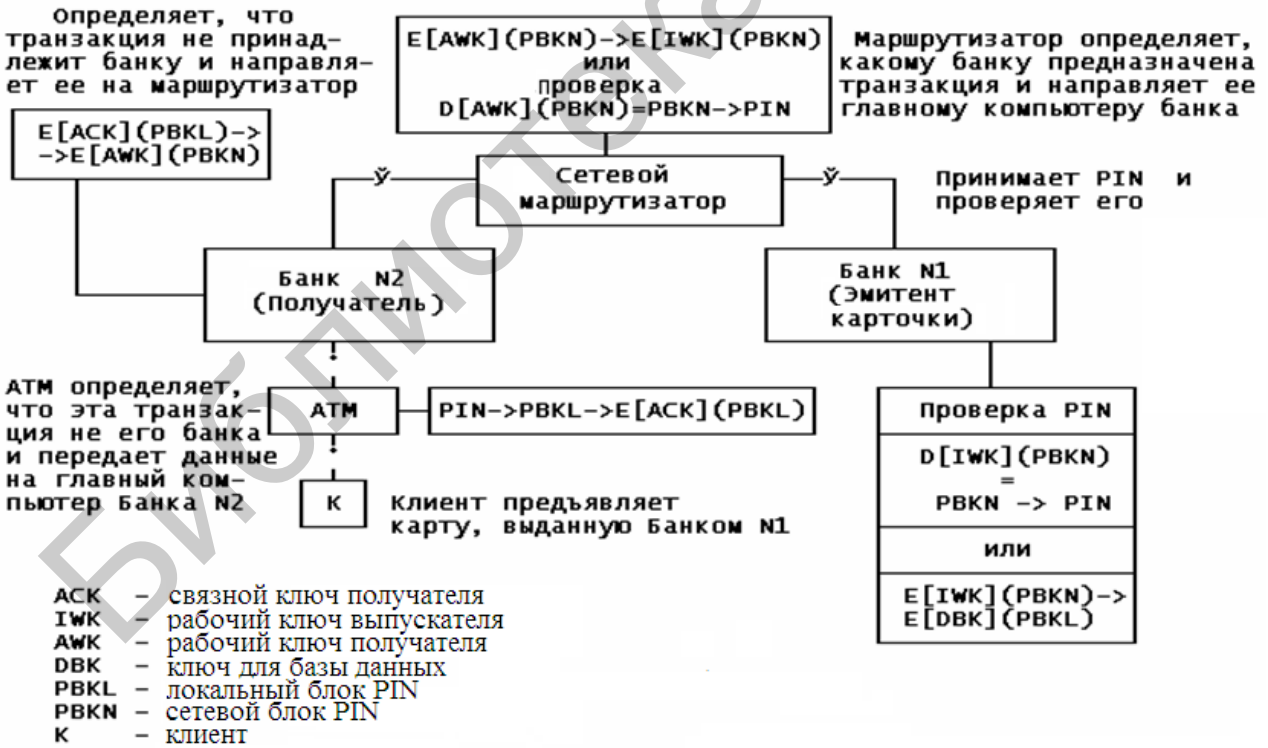

Рис. 3.4. Схема прохождения платежа между АКА, банком – владельцем АКА, банком-эмитентом

На рис. 3.4 показан вариант расчета между банками (банк №1 и банк №2) в некоторой гипотетической сети АКА. Предположим, что в ней клиент бан-

ка №1 обратился к АКА банка №2. При этом в сети происходят следующие действия:

1. Считывающее устройство АКА считывает информацию, записанную на банковской карточке, предъявленной клиентом, и затем АКА определяет, имеет ли клиент счет в банке №2.

2. В том случае, когда клиент не имеет счета в банке №2, транзакция направляется на сетевой маршрутизатор, который, используя номер идентификации банка (Bank Identification Number, BIN), направляет ее на главный компьютер банка №1 или производит проверку PIN для банка №1.

3. Если проверка PIN производится в самом компьютере банка №1, то компьютер получает полную информацию о транзакции и проверяет достоверность PIN некоторым образом.

4. Вне зависимости от того, с каким результатом завершилась проверка, компьютер банка №1 пересылает сообщение с результатом проверки через сетевой маршрутизатор компьютеру банка №2.

Этот пример показывает, что к эмитенту предъявляются следующие требования:

- выпускаемые им карточки должны восприниматься всеми АКА сети;
- он должен обладать технологией проверки собственных обменных PIN (если в АКА используется встроенная проверка принадлежности транзакции, то главный компьютер должен эмулировать результаты проверки в таком же формате).

К получателю, в свою очередь, предъявляются другие требования:

- в АКА или главном компьютере банка должна быть реализована проверка принадлежности транзакции;
- если нет возможности проверить правильность чужого PIN, получатель должен передать данные о транзакции на сетевой маршрутизатор.

Системы POS предназначены для сокращения расходов по обработке бумажных денег и для уменьшения риска покупателя и продавца, связанного с этой обработкой. Схема системы POS представлена на рис. 3.5.

Рис. 3.5. Схема системы POS

Покупатель для оплаты покупки предъявляет свою дебетовую или кредитную карточку и для подтверждения личности вводит PIN. Продавец со своей стороны вводит сумму, которую необходимо уплатить за покупку или за услуги.

Запрос на перевод денег направляется в банк продавца. Тот для проверки подлинности карточки, предъявленной покупателем, переадресует запрос в банк покупателя. Если карточка подлинная и покупатель имеет право применять ее для оплаты продуктов и услуг, банк покупателя переводит деньги в банк продавца на его счет. После перевода денег банк продавца посылает извещение на терминал POS, в котором сообщает о завершении транзакции. После этого продавец выдает покупателю извещение.

4. ЗАЩИТА АВТОМАТИЗИРОВАННЫХ СИСТЕМ ОТ АТАК

4.1. Общие сведения об атаках

Атака на АС – действие или последовательность действий нарушителя, которые приводят к реализации угроз путем использования уязвимостей этой АС.

Уязвимости АС:

- недостатки аппаратно-программных средств по вине разработчика;
- уязвимости, добавленные администратором при настройке АС;
- уязвимости, внесенные пользователем.

Цель атаки – нарушение одной из функций системы:

- конфиденциальности;
- целостности;
- доступности.

Атака может быть активной (результат – изменение данных) или пассивной (результат – раскрытие данных). При этом факт атаки необязательно означает, что она достигла цели. Степень успешности атаки зависит от уязвимости системы и эффективности контрмер.

Этапы атаки следующие:

1. Сбор информации:

- изучение окружения: провайдер целевой системы, адреса доверенных узлов, трафик, режим работы организации, телефонные номера и т. д.;
- идентификация топологии сети: количество компьютеров, способ их соединения, организация выхода в глобальную сеть;
- идентификация узлов сети: разведка IP-адреса узла, его доступности;
- идентификация сервисов и портов: наличие установленных сервисов (Telnet, FTP, web-сервера и т. д.) и доступа к ним, открытость портов;
- идентификация операционной системы: тип операционной системы;
- определение уязвимостей узла на основе ранее собранной информации.

2. Реализация атаки:

- проникновение в систему;
- контроль над системой.

3. Завершение атаки:

- устранение следов атаки с целью невозможности идентификации атакующего;
- маскирование внедренной программы;
- изменение контрольных сумм файлов;
- очистка журнала регистрации событий.

Общая классификация атак:

- регулярные (проводятся на любую систему вне зависимости от состава ее аппаратно-программных средств);
- использующие ошибки политики безопасности или администрирования;
- использующие ошибки программно-технических средств системы («баги»).

4.2. Классификация атак

Сетевая разведка. Цель – поиск работающих сервисов одного узла или целого диапазона, а также возможных уязвимостей, которым подвержены данные узлы.

Методика – отправка определенного типа TCP-пакетов (TCP SYN, ACK, FIN, RST) и анализ ответов сканируемого узла.

Выделяют следующие типы сканирования:

1. Проверка онлайна. Определение работающей системы на целевом IP-адресе, формирование echo-сообщений протокола ICMP с помощью утилиты ping путем перебора всех адресов или посылка широковещательного запроса.

2. SYN-сканирование. Наиболее популярный метод. Сканер портов генерирует пакет SYN. Если порт на целевом хосте открыт, с него придет пакет SYN-ACK. Хост сканера отвечает пакетом RST, закрывая тем самым соединение.

3. TCP-сканирование. Более простой метод. Операционная система, в случае если порт открыт, завершает трехэтапную процедуру установления соединения и затем сразу закрывает соединение. В противном случае, возвращается код ошибки. Не требует от атакующего специальных прав доступа. Большая загрузка сканируемой системы.

4. UDP-сканирование. UDP-пакет посылается на закрытый порт, на который система ответит сообщением ICMP «порт недоступен». Отсутствие такого сообщения объясняется тем, что порт открыт. Однако, если порт блокируется брандмауэром, то метод неверно покажет, что порт открыт.

5. ACK-сканирование. Применяется для определения, фильтрации портов и определения наличия брандмауэров и выяснения их правил функционирования. Простая фильтрация пакетов разрешит прохождение пакетов с установленным битом ACK, тогда как более сложные брандмауэры – нет.

6. FIN-сканирование. Позволяет обойти некоторые средства защиты от SYN-сканирования. На прибывший FIN-пакет на закрытый порт сервер должен ответить пакетом RST. FIN-пакеты на открытые порты должны игнорироваться сервером. Таким образом, можно отличить закрытый порт от открытого.

Этапы сетевой разведки:

1. DNS-запрос (Domain Name System). Имя владельца домена, диапазон IP-адресов.

2. Эхо-тестирование (ping sweep) адресов. Определение хостов (hosts).

3. Сканирование портов. Список сервисов, поддерживаемый хостами.

4. Анализ характеристик приложений. Получение информации для несанкционированного доступа (НСД).

Противодействие сетевой разведке:

1) ACL-фильтрация;

2) применение IDS (Intrusion Detection System) и IPS (Intrusion Prevention System);

3) использование NAT.

Анализ сетевого трафика. Цель – перехват и последующий анализ либо только анализ сетевого трафика, предназначенного для других узлов.

Методы сниффинга:

1) «прослушивание» сетевого трафика (эффективно при использовании в сети концентраторов) (рис. 4.1);

2) подключение сниффера в разрыв канала связи;

3) анализ побочного электромагнитного излучения (ПЭМИ) и восстановление трафика;

4) спуффинг – перенаправление трафика жертвы на сниффер с возвратом его адресату.

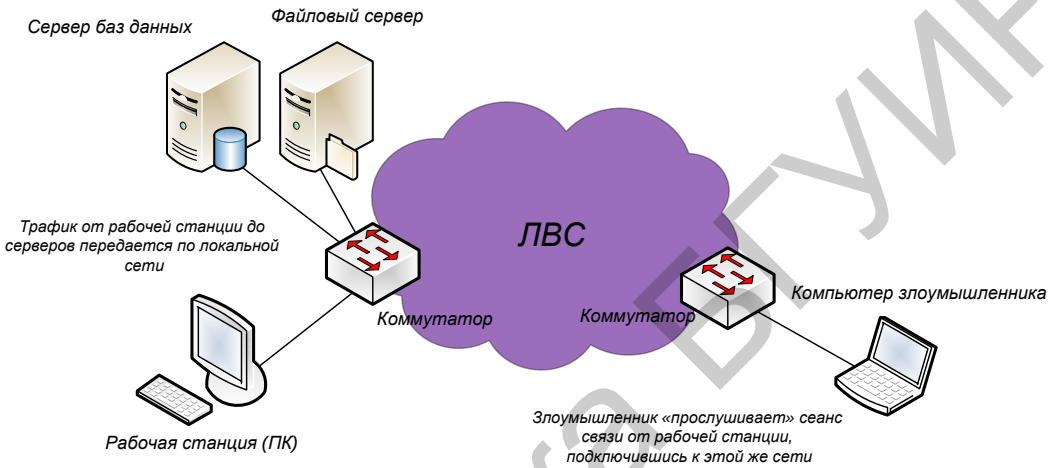

Рис. 4.1. Схема реализации прослушивания сетевого трафика

Метод ARP основан на некорректной обработке широковещательных запросов сетевой картой, находящейся в беспорядочном режиме. Осуществляется отправка пакета по адресу FF:FF:FF:FF:FF:FE (ложный широковещательный адрес с вычетом одного бита). Данный пакет зачастую воспринимается как широковещательный сетевой картой, находящейся в беспорядочном режиме. Соответственно хост, на котором запущен сниффер, ответит на него ARP-Reply.

Оба данных метода неидеальны и не работают в случае, когда ARP и ICMP фильтруются брандмауэром на хосте, использующем сниффер.

Спуффинг. Цель – заставить целевую систему отправлять трафик не легитимному получателю напрямую, а атакующему, который затем уже ретранслирует трафик его адресату.

Методы спуффинга:

1. MAC-спуффинг. На сетевой карте изменяется MAC-адрес, что заставляет коммутатор отправлять на порт, к которому подключен злоумышленник, пакеты, которые до этого он получать не мог.

2. ARP-спуффинг. Используется уязвимость протокола ARP, позволяющая разместить в ARP-кэше жертвы ложную запись о соответствии IP-адреса другой жертвы MAC-адресу атакующего.

До выполнения данной атаки в ARP-таблице узлов A и B существуют записи с IP- и MAC-адресами друг друга (рис. 4.2). Обмен информацией производится непосредственно между узлами A и B.

В ходе выполнения компьютер С, выполняющий атаку, отправляет ARP-ответы (без получения запросов):

- узлу А: с IP-адресом узла В и MAC-адресом узла С;
- узлу В: с IP-адресом узла А и MAC-адресом узла С.

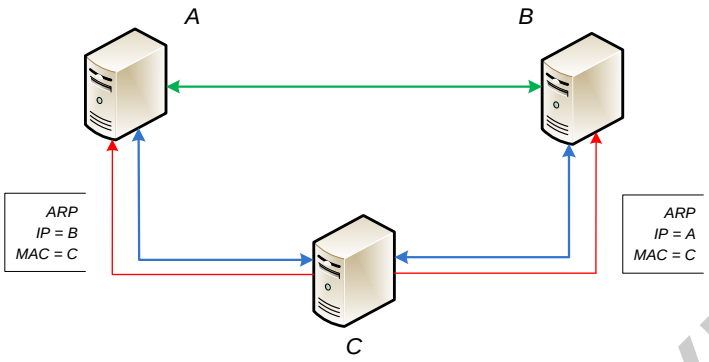

Рис. 4.2. Схема реализации ARP-спуффинга

В силу того что узлы поддерживают самопроизвольный ARP (gratuitous ARP), они модифицируют собственные ARP-таблицы и помещают туда записи, где вместо настоящих MAC-адресов узлов А и В стоит MAC-адрес узла С.

После того как атака выполнена, когда узел А хочет передать пакет узлу В, он находит в ARP-таблице запись (она соответствует компьютеру С) и определяет из нее MAC-адрес получателя. Отправленный по этому MAC-адресу пакет приходит узлу С вместо получателя. Компьютер С затем ретранслирует пакет тому, кому он действительно адресован, т. е. узлу В.

3. DNS-спуффинг (рис. 4.3). Ложная запись в кэш DNS-сервера целевой системы о соответствии DNS-имени хоста, которому целевая система доверяет IP-адреса атакующего.

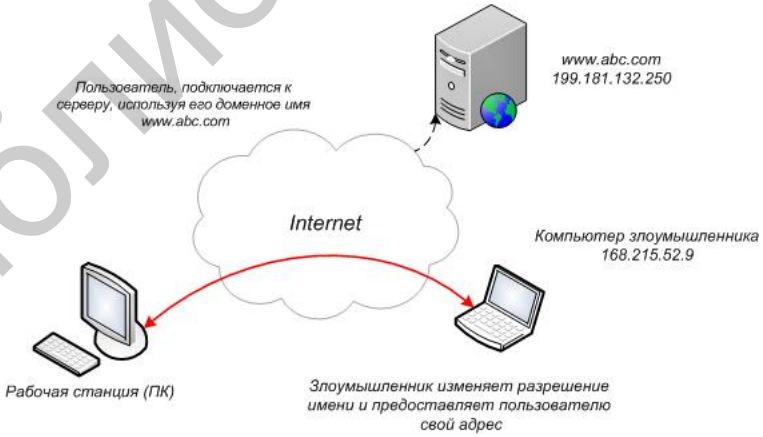

Рис. 4.3. Схема реализации DNS-спуффинга

4. IP-спуффинг. Использование в IP-пакетах, отправляемых целевой системой, IP-адресов хоста, которому она доверяет. Осуществима в UDP и в некоторых случаях возможна в TCP-соединениях.

Атака man-in-the-middle. Цель – анализ трафика, перехват текущей сессии между отправителем и получателем информации, получение доступа к

частным сетевым ресурсам, проведение атак типа DoS, нарушение целостности передаваемых данных в сетевой сессии (рис. 4.4).

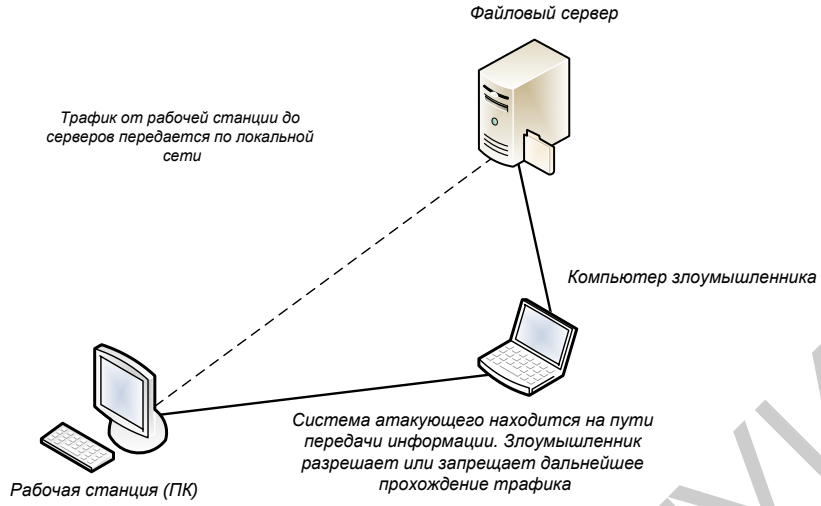

Рис. 4.4. Схема реализации атаки man-in-the-middle

Атака-отказ в обслуживании (DoS). Цель – сделать сеть организации недоступной для обычного использования за счет превышения допустимых пределов функционирования сети, операционной системы или приложения.

Причины DoS:

1. Ошибки в программном коде. Обращение к неиспользуемому фрагменту адресного пространства приводит к недопустимой инструкции или другой необрабатываемой исключительной ситуации, что вызывает аварийное завершение серверного приложения.

2. Недостаточная проверка данных пользователя приводит к бесконечному либо длительному циклу или повышенному длительному потреблению процессорных ресурсов.

3. Использование ошибок:

- эксплойт (exploit). Программа, фрагмент программного кода или последовательность команд, использующие уязвимости в программном обеспечении и применяемые для проведения атаки на вычислительную систему;

- удаленный (remote). Работает через сеть и использует уязвимость в защите без какого-либо предварительного доступа к уязвимой системе;

- локальный (local). Запускается непосредственно в уязвимой системе, требуя предварительного доступа к ней. Обычно используется для получения взломщиком прав администратора.

4. Флуд (flood). Большое количество обычно бессмысленных или сформированных в неправильном формате запросов к компьютерной системе или сетевому оборудованию:

- SYN-flood. На атакуемый узел направляется большое количество SYN-пакетов по протоколу TCP (запросов на открытие соединения). При этом на атакуемом сервере через короткое время исчерпывается количество открытых сокетов и сервер перестает отвечать;

- UDP-flood. Большим количеством UDP-пакетов разного размера вызывается перегрузка канала связи, и сервер, работающий по протоколу TCP, перестает отвечать;

- ICMP-flood. Аналогичен SYN-флуду. Отличие – использование ICMP-пакетов.

5. Атаки второго рода. Вызов ложного срабатывания системы защиты и блокирования ресурса.

Выделяют следующие виды DoS-атак:

1. Простая. Система злоумышленника создает трафик для вывода из строя целевой системы.

2. Распределенная. Проводится одновременно через множество подчиненных узлов, которые выполняют команды управляющего узла для атаки на целевую систему.

3. Отраженная. Отправка пакетов на промежуточный сервер, при котором в качестве адреса отправителя указывается адрес целевой системы, заставляет удаленный сервер отвечать целевой системе, тем самым создавая условия для DoS.

4. Межсайтовая. Используются сервисы сети, имеющие обширную инфраструктуру для обращения к сторонним web-узлам (онлайн-переводчики image-хостинги и т. д.) в качестве удаленного сервера.

Примеры DoS атак:

1. Ping of Death. Атакующий формирует echo-request размером более 65 535 байт, что приводит к переполнению буфера целевой системы.

2. SYN-flood. Атакующий формирует запрос на установление соединения (пакет с флагом SYN). Целевая система отвечает SYN+ACK. Узел атакующего игнорирует ответ.

3. Tribe Flood Network (TFN), Tribe Flood Network 2000 (TFN2K). Атакующий формирует запрос, в котором свой IP-адрес заменяет на IP-адрес целевой системы и передает пакет в BOT-сеть. Рабочие станции такой сети отвечают на данный пакет.

4. Smurf. Атакующий формирует широковещательный запрос (ICMP Echo), в котором свой IP-адрес заменяет на IP-адрес целевой системы и передает пакет в сеть передачи данных. Рабочие станции такой сети отвечают на данный пакет (ICMP-reply).

5. Fraggle. Атакующий формирует широковещательный запрос (UDP Echo), в котором свой IP-адрес заменяет на IP-адрес целевой системы и передает пакет в сеть передачи данных. Рабочие станции такой сети отвечают на данный пакет (UDP-replay или ICMP-replay).

Атаки на уровне приложений. Цель – получение доступа к рабочей станции от имени пользователя, работающего с приложением, используя уязвимости серверного программного обеспечения (sendmail, HTTP, FTP).

Причина – используются порты, которые пропускаются ACL на маршрутизаторах или межсетевых экранах (исключение – наличие модуля IDS).

Парольные атаки (brute force). Цель – получение конфиденциальной информации (паролей) путем перехвата аутентификационных факторов, передаваемых в виде MD5-хэша.

Зачастую, когда невозможно перехватить сеанс связи между целевыми узлами или когда в перехваченном сеансе информация для аутентификации передается не в текстовом виде, а, например, в виде MD5-хэша, злоумышленники пользуются атакой, которая основана на простом переборе пароля или имени учетной записи.

Реализация метода простого перебора (BruteForce) часто выполнена в виде скрипта или программы, которая пытается получить доступ к ресурсу.

Еще одна проблема возникает, когда пользователи применяют один и тот же (пусть даже очень хороший) пароль для доступа ко многим системам: корпоративной, персональной и системам Интернет. Поскольку устойчивость пароля равна устойчивости самого слабого хоста. Хакер, узнавший пароль через этот хост, получает доступ ко всем остальным системам, где используется тот же пароль.

Ботнет. Ботнет (roBOT NETwork) – сеть компьютеров, зараженных вредоносной программой типа Backdoor, дающей возможность дистанционного управления компьютером без ведома пользователя.

Управление компьютером с помощью Backdoor:

- прямое – при непосредственном подключении злоумышленника к компьютеру;
- опосредованное – при автоматическом подключении компьютера к центру управления злоумышленника.

Свойства:

1. Централизованное управление посредством C&C – Command and control centre (рис. 4.5).
2. Используемые каналы передачи данных:
- IRC (Internet Relay Chat);
- IM (Instant Messaging);
- www;
- TCP/IP.
3. Использование:
- рассылка спама;
- кибершантаж (DDoS);
- анонимный доступ в сеть;
- продажа и аренда;
- фишинг;
- получение конфиденциальной информации.

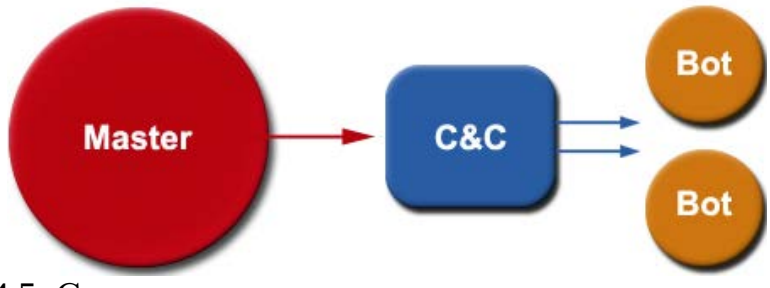

Рис. 4.5. Схема реализации централизованного управления

4.3. Основы построения систем противодействия атакам

Противодействие атакам – комплекс организационно-технических мероприятий, направленных на обнаружение, анализ и реагирование на попытки инцидентов безопасности, атак или несанкционированного доступа.

Организационно-правовая составляющая:

- документированная политика безопасности;
- положения о распознавании и противодействии атакам;
- наличие компетентных специалистов.

Содержание политики безопасности:

- зона ответственности;
- правила использования информационных ресурсов;
- план мероприятий, проводимых в случае распознавания атаки;
- ответственность персонала.

Техническая составляющая:

- штатные средства – сетевые журналы сетевых устройств, операционных систем и приложений;
- специализированные средства – средства распознавания и противодействия атакам.

Для обнаружение фактов прослушивания сетевого трафика применяется следующее:

- метод пинга (Ping method);
- метод ARP.

Метод пинга (Ping method) заключается в отсылке «ICMP Echo request» (Ping-запроса) не на MAC-адрес рабочей станции, а на ее IP-адрес. К примеру:

- хост, подозреваемый в использовании сниффера, имеет IP-адрес 10.1.1.1 и MAC-адрес 00-40-05-A4-79-32;
- отправка «ICMP Echo request», указав в запросе IP-адрес подозреваемого хоста и его измененный MAC-адрес, например, 00-40-05-A4-79-33;
- каждый хост, получив данный запрос, сравнивает указанный в запросе MAC-адрес со своим MAC-адресом. В случае совпадения MAC-адресов хост отвечает источнику запроса с помощью «ICMP Echo Reply», иначе пакет игнорируется. В данном случае ни один из хостов в сети не должен увидеть данный пакет;
- если получен ответ от какого-либо хоста, это значит, что у него не используется фильтр MAC-адресов, т. е. его сетевой адаптер находится в «беспорядочном режиме». Следовательно, на данном хосте используется сниффер.

Метод пинга может быть перенесен на другие протоколы, которые генерируют ответы на запросы, например, запрос на установление TCP-соединения или запрос по протоколу UDP на порт 7 (эхо).

Противодействие сниффингу:

1) аутентификация;
2) криптозащита;
3) антиснифферы.

Противодействие спуффингу:

1) отслеживание ARP-активности средствами IDS;
2) использование ACL;
3) шифрование и аутентификация (IP v6);
4) сравнение DNS-узла с данными третьей стороны.

Способы противодействия DoS-атакам:

1. Фильтрация – блокирование атаки на входе в сеть ISP.

2. Устранение уязвимостей – обновление ПО (неэффективно против атак типа flood).

3. Наращивание ресурсов – обновление аппаратных средств АС.

4. Рассредоточение – построение распределенных и продублированных систем.

5. Уклонение – отнесение непосредственной цели атаки подальше от других ресурсов, которые часто также подвергаются воздействию вместе с непосредственной целью.

6. Предотвращение – профилактика причин, побуждающих тех или иных лиц организовывать DoS-атаки.

7. Активные ответные меры – воздействие на источники, организатора или центр управления атакой как технического, так и организационно-правового характера.

8. Блэкхоллинг (BGP Blackhole) – «черная дыра» для трафика на стороне ISP, удаленно управляемая клиентом. Метод основан на использовании полной фильтрации (null routing) и протокола маршрутизации BGP.

Противодействие атакам на уровне приложений – ограничение списка разрешенных узлов для установления сеанса связи и своевременное обновление серверного программного обеспечения.

Методы защиты от парольных атак:

1) установление минимальной длины и сложности пароля;
2) использование одноразовых паролей;
3) задержка на авторизацию;
4) блокировка после неудачных N-попыток аутентификации ACL, IDS, IPS.

Методы противодействия Ботнет:

- воздействие на C&C;
- децентрализованное P2P (рис. 4.6).

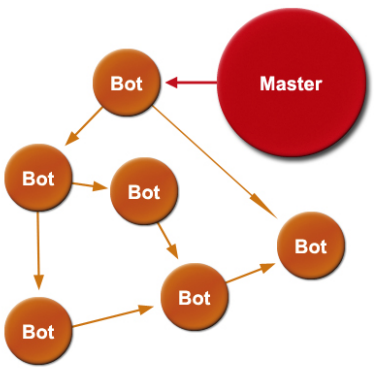

Рис. 4.6. Схема реализации децентрализованного управления

4.4. Системы противодействия утечки данных

Системы противодействия утечки данных (DLP-системы, англ. Data Leakage Prevention) представляют собой совокупность технологий и технических устройств (программных или программно-аппаратных), направленных на предотвращение утечек конфиденциальной информации за пределы информационной системы организации.

Функции DLP-систем:

- контроль за перемещением информации как на уровне коммуникаций с внешней сетью, так и на уровне оконечных устройств пользователей (рис. 4.7);
- сканирование хранящихся файлов и баз данных для обнаружения мест расположения конфиденциальной информации.

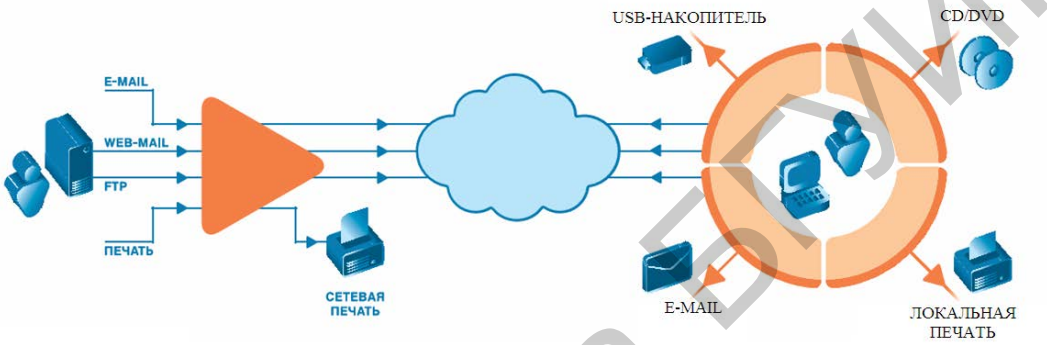

Рис. 4.7. Информационные потоки, контролируемые при помощи DLP-систем

Основными модулями DLP-систем являются:

- перехватчики/контроллеры на разные каналы передачи информации;
- агентские программы, устанавливаемые на оконечные устройства;
- центральный управляющий сервер.

На рис. 4.8 приведен пример размещения модулей DLP-системы на устройствах информационной системы организации.

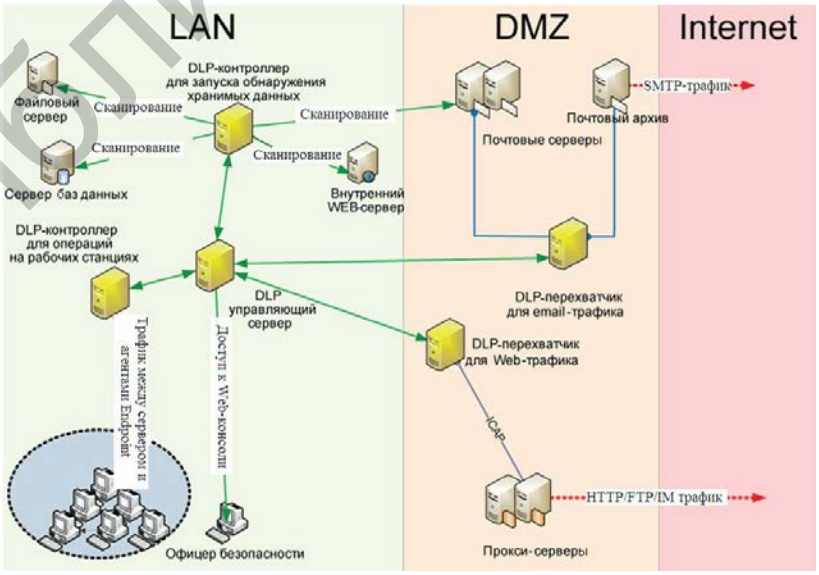

Рис. 4.8. Пример размещения модулей DLP-системы на устройствах информационной системы организации

Перехватчики анализируют потоки информации, которая может быть выведена за пределы информационной системы организации, обнаруживают конфиденциальные данные, классифицируют информацию и передают для обработки возможного инцидента на управляющий сервер. Перехватчики могут как копировать исходящий трафик, так и препятствовать его передаче за пределы информационной системы организации. В последнем случае потенциальная утечка может быть остановлена системой DLP.

Контроллеры для обнаружения хранимых данных запускают процессы обнаружениях в сетевых ресурсах конфиденциальной информации. Способы запуска обнаружения могут быть различными: от собственно сканирования от сервера контроллера до запуска отдельных программных агентов на существующие серверы или рабочие станции.

Контроллеры для операций на рабочих станциях распределяют политику безопасности на оконечные устройства, анализируют результаты деятельности сотрудников с конфиденциальной информацией и передают данные возможного инцидента на управляющий сервер.

Агентские программы на оконечных рабочих местах замечают конфиденциальные данные в обработке и следят за соблюдением таких правил, как сохранение на сменный носитель информации, отправки, распечатывания, копирования через буфер обмена.

Управляющий сервер сопоставляет поступающие от перехватчиков и контроллеров сведения и предоставляет интерфейс проработки инцидентов и построения отчетности.

4.5. Программно-аппаратные средства защиты информации от несанкционированного доступа

Цель использования программно-аппаратных средств защиты информации от несанкционированного доступа (НСД) – защита персонального компьютера (ПК) и информационных ресурсов от НСД и обеспечение конфиденциальности информации, обрабатываемой и хранимой в ПК при многопользовательском режиме его эксплуатации.

Рассмотрим программно-аппаратный комплекс (ПАК) «Аккорд». Его особенности заключаются в следующем:

- обеспечивает физическую охрану ПК и его средств, в том числе проведение мероприятий по недопущению изъятия контроллера комплекса;
- характеризуется наличием администратора службы безопасности – привилегированного пользователя, имеющего особый статус и абсолютные полномочия.

Функции ПАК «Аккорд»:

- идентификация пользователя по уникальному ТМ-идентификатору, аутентификация, ограничение времени доступа субъекта к ПК;
- блокирование экрана и клавиатуры в случаях, в которых могут реализовываться угрозы информационной безопасности;

- разграничение доступа к ресурсам ПК, определяемое атрибутами доступа, которые устанавливаются администратором в соответствие каждой паре «субъект доступа – объект доступа» при регистрации субъекта;

- управление стандартными процедурами печати, процедурами ввода/вывода на отчуждаемые носители информации;

- контроль целостности критичных программ и данных, защита от внедрения вредоносных программ;

- функциональное замыкание информационных систем (контроль подключаемого к ПК оборудования).

Дополнительные функциональные возможности ПАК «Аккорд»:

- установка требуемого времени жизни пароля и его минимальной длины;

- временные ограничения на использование ПК пользователем за счет установки интервала времени по дням недели;

- ограничение объема сведений выводимых на внешние устройства.

Схема, соответствующая архитектуре ПАК «Аккорд», представлена на рис. 4.9.

Выделяют следующие подсистемы ПАК «Аккорд»:

1. Подсистема управления доступом. Обеспечивает защиту от посторонних пользователей, управление доступом к объектам и организации совместного их использования зарегистрированными пользователями в соответствии с установленными правилами.

2. Подсистема регистрации и учета. Обеспечивает регистрацию в системном журнале различных событий, возникающих в ПК (пользователь, его действия и дата-время).

3. Подсистема обеспечения целостности. Обеспечивает исключение несанкционированных модификаций ПО, в том числе ПО комплекса, обрабатываемой информации, обеспечение защиты ПК от внедрения вредоносных программ.

Рис. 4.9. Архитектура ПАК «Аккорд»

Схема, соответствующая архитектуре средства защиты информации на основе ПАК «Аккорд», представлена на рис. 4.10.

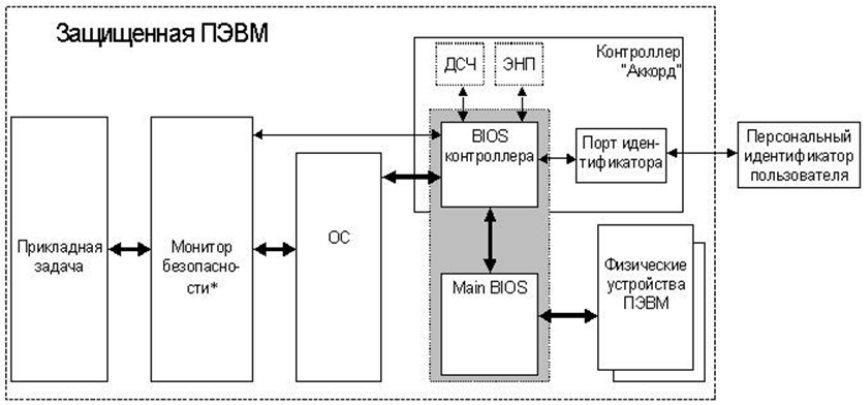

Рис. 4.10. Архитектура средства защиты информации на основе ПАК «Аккорд»: ДСЧ – датчик случайных чисел; ЭНП – энергонезависимая память

5. ПРИМЕНЕНИЕ МЕЖСЕТЕВЫХ ЭКРАНОВ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ

5.1. Основные компоненты архитектуры межсетевых экранов

Межсетевые экраны (МЭ) могут быть реализованы следующим образом:
- в виде приложения;
- в виде драйвера операционной системы;
- в виде драйвера под управлением отдельной операционной системы;
- в виде программного модуля программно-технического комплекса.

Схема, соответствующая архитектуре МЭ, представлена на рис. 5.1.

Рис. 5.1. Архитектура МЭ

Архитектура МЭ включает в себя следующие элементы:

1. Модуль аутентификации и авторизации. Обеспечивает поддержку внутренних и внешних схем и протоколов аутентификации (RADIUS, TACACS, RSA SecurlD, NT Domain и т. д.)

2. Журнал событий. Обеспечивает регистрацию всех происходящих событий и действий, выполняемых МЭ.

3. Консоль управления. Представляет собой прикладные средства, обеспечивающие выполнение всех административных действий над МЭ.

Выделяют следующие режимы работы МЭ:

1) фильтрация трафика;

2) посредничество.

МЭ, используемый для защиты одного компьютера, называется брандмауэром.

Эквивалент представления МЭ, работающего в первом режиме, – последовательность фильтров, обрабатывающих информационный поток. Каждый из фильтров предназначен для интерпретации отдельных правил фильтрации. Такой МЭ обеспечивает анализ трафика на основе правил.

Использование МЭ, работающего во втором режиме, обеспечивает следующие особенности:

- аутентификация пользователя выполняется при установлении сеанса связи за счет использования одноразовых паролей, цифровых сертификатов и т. д.;
- прозрачное шифрование данных;
- организация VPN;
- преобразование IP-адресов хостов-отправителей в один IP-адрес, ассоциируемый с МЭ.

5.2. Основные схемы подключения межсетевых экранов

Выделяют следующие схемы подключения МЭ.

1. Dual-homed (multihomed).
2. Демилитаризованная зона (DMZ – demilitarized zone).

Общий вид схемы dual-homed представлен на рис. 5.2.

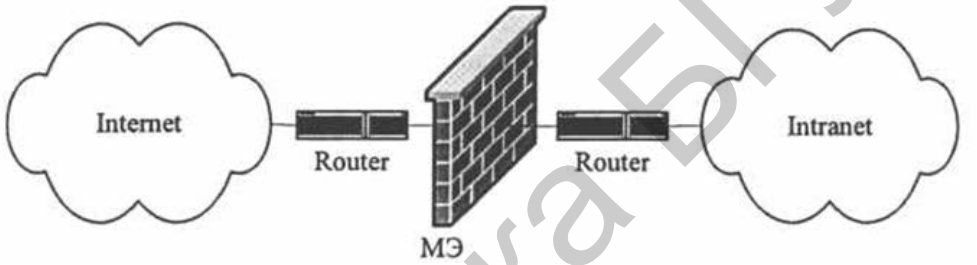

Рис. 5.2. Общий вид схемы dual-homed

Схема dual-homed включает в себя два Network Interface Controller. При использовании данной схемы реализуется физическое и логическое разделение сетей.

Общий вид схем подключения МЭ с DMZ представлен на рис. 5.3.

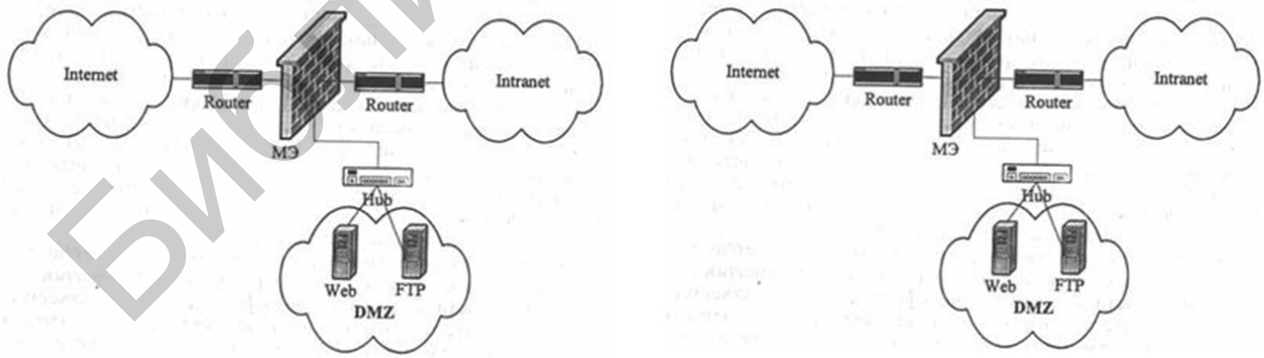

Рис. 5.3. Общий вид схем подключения МЭ с DMZ

DMZ обеспечивает:

- разграничение доступа по правилам;
- разделение доступа к внешним и внутренним ресурсам корпоративной сети;
- централизованное управление в защите ресурсов корпоративной сети.

Особенности реализации DMZ следующие (рис. 5.4):

1) выполнение запроса пользователя сети Интернет;
2) выполнение запроса от web-сервера к серверу баз данных;
3) запрос пользователя корпоративной сети.

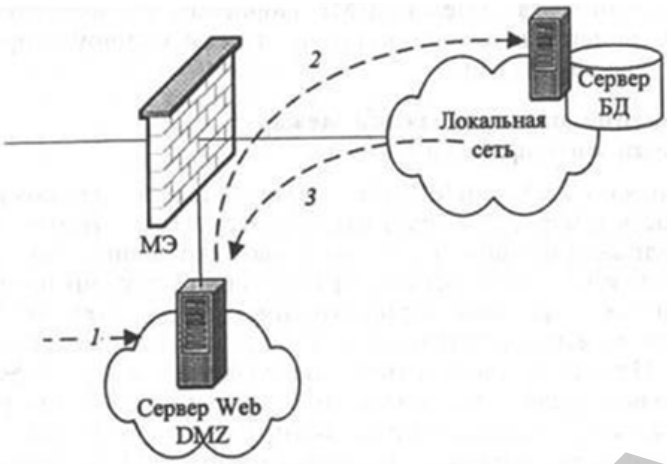

Рис. 5.4. Особенности реализации DMZ

5.3. Трансляция сетевых адресов

Трансляция внутренних сетевых адресов реализуется по отношению ко всем пакетам, следующим из внутренней сети во внешнюю. Для этих пакетов посредник выполняет автоматическое преобразование IP-адресов компьютеров-отправителей в один «надежный» IP-адрес, ассоциируемый с брандмауэром, из которого передаются все исходящие пакеты. В результате все исходящие из внутренней сети пакеты оказываются отправленными межсетевым экраном, что исключает прямой контакт между авторизованной внутренней сетью и являющейся потенциально опасной внешней сетью. IP-адрес брандмауэра становится единственным активным IP-адресом, который попадает во внешнюю сеть.

При таком подходе топология внутренней сети скрыта от внешних пользователей, что усложняет задачу несанкционированного доступа. Кроме повышения безопасности трансляция адресов позволяет иметь внутри сети собственную систему адресации, не согласованную с адресацией во внешней сети, например в сети Интернет. Это эффективно решает проблему расширения адресного пространства внутренней сети и дефицита адресов внешней сети.

Выделяют следующие разновидности NAT:

1) статический NAT отображает незарегистрированный IP-адрес на зарегистрированный IP-адрес на основании принципа «один к одному» (необходимо, когда устройство должно быть доступным снаружи сети);

2) динамический NAT отображает незарегистрированный IP-адрес на зарегистрированный адрес от группы зарегистрированных IP-адресов (может изменяться в зависимости от зарегистрированного адреса, доступного в пуле адресов, во время коммутации);

3) перегруженный NAT отображает несколько незарегистрированных адресов в единственный зарегистрированный IP-адрес, используя различные порты.

Достоинства:
- экономия адресного пространства;
- ограничение доступа из внешней сети;
- скрытие некоторых сервисов внутренней сети.
Недостатки:
- ограничения при работе по некоторым протоколам функционирования;
- необходимость хранения журнала трансляций.

5.4. Аутентификация в автоматизированных системах

Для обеспечения аутентификации в автоматизированных системах используются следующие протоколы:

1. PAP (Password Authentication Protocol). Обеспечивает распознавание пользователя по паролю. Пароли и идентификаторы передаются в незашифрованном виде. Аутентификация выполняется только сервером.

2. MSCHAP (Microsoft Challenge-Handshaking Authentication Protocol) и EAP-TLS (Extensible Authentication Protocol–Transport Layer Security). Обеспечивают распознавание пользователя путем использования системы «рукопожатия», а также защиту от повторного использования злоумышленником перехваченных пакетов с зашифрованным паролем и взаимную аутентификацию клиента и VPN-сервера.

5.5. Виртуальные частные сети

Виртуальная частная сеть (Virtual Private Network, VPN) – объединение локальных сетей и отдельных компьютеров через открытую внешнюю среду передачи информации в единую виртуальную корпоративную сеть, обеспечивающую безопасность циркулирующих данных (рис. 5.5).

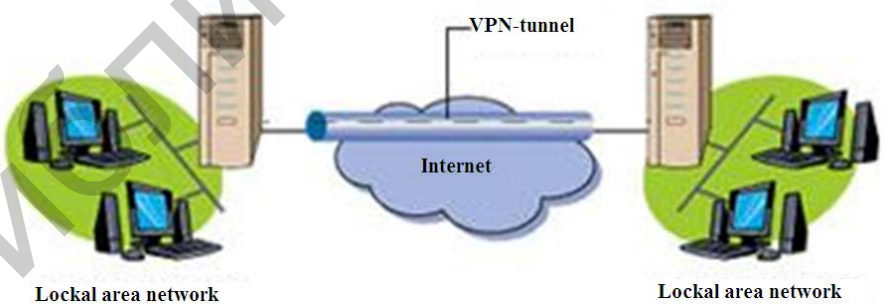

Рис. 5.5. Схема реализации виртуальной частной сети

Мероприятия по обеспечению информационной безопасности:
1) аутентификация взаимодействующих сторон;
2) криптографическая защита передаваемых данных;
3) проверка подлинности и целостности передаваемой информации.
Устройства VPN:
1) VPN-клиент – программный или программно-аппаратный комплекс на базе ПК;

2) VPN-сервер – программный или программно-аппаратный комплекс на базе серверного оборудования;

3) шлюз безопасности – сетевое устройство, подключаемое к двум сетям.

Особенности передачи данных в VPN:

1) криптозащита всего пакета;

2) инкапсулирование;

3) туннелирование.

Схема реализации VPN с удаленным доступом представлена на рис. 5.6.

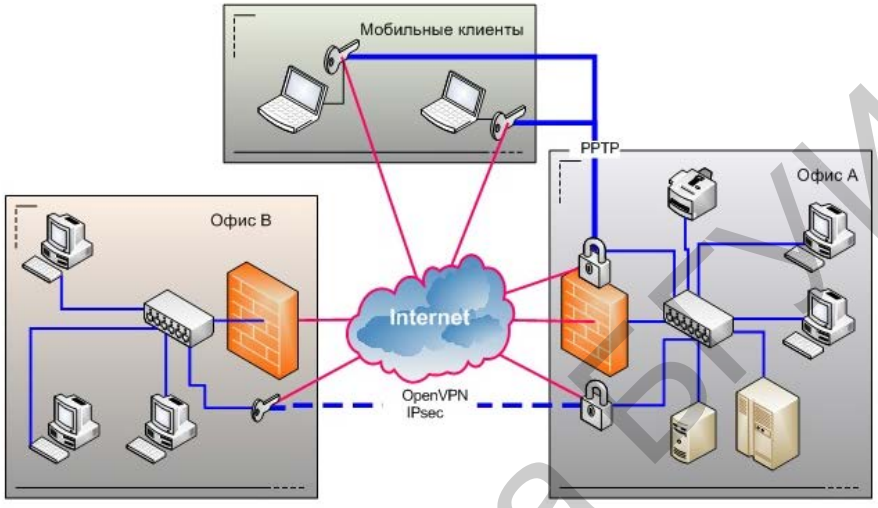

Рис. 5.6. Схема реализации VPN с удаленным доступом

Достоинства использования схемы, представленной на рис. 5.6:

1) снижение затрат на междугородных коммуникациях;

2) высокая масштабируемость сети.

Схема реализации внутрикорпоративной сети VPN представлена на рис. 5.7.

Рис. 5.7. Схема реализации внутрикорпоративной сети VPN

Схема реализации межкорпоративной сети VPN представлена на рис. 5.8.

Достоинства использования схем, представленых на рис. 5.7 и 5.8:

1) применение «мощных» криптографических протоколов;

2) высокая надежность;

3) гибкость управления.

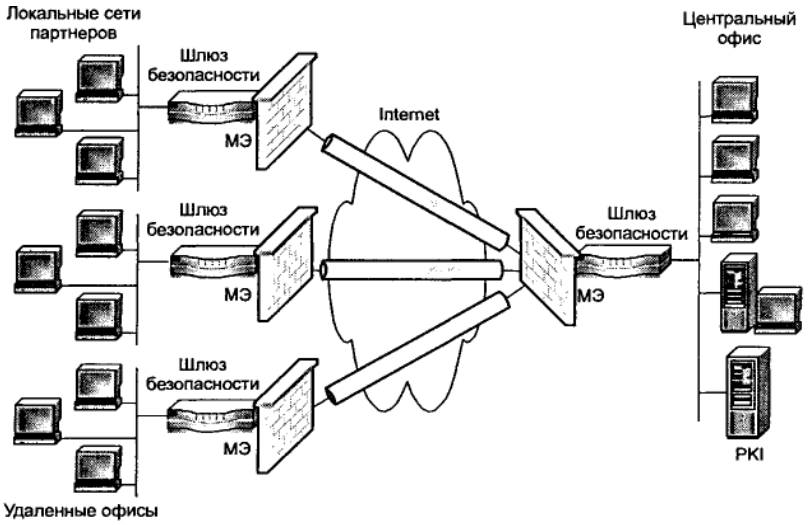

Рис. 5.8. Схема реализации межкорпоративной сети VPN

5.6. Противодействие спаму

Спам (Spam) – анонимная массовая незапрашиваемая рассылка электронных почтовых сообщений.

Основные виды:

- реклама;
- реклама незаконной продукции;
- «нигерийские письма»;
- фишинг.

Способы организации массовых рассылок:

1. Почтовый червь:
- распространение с помощью e-mail;
- поиск e-mail-адресов на зараженном хосте;
- рассылка по найденным адресам.

2. Почтовый сервер:
- основан на сервисе отправки пользователю сообщения о недоставке письма;
- подразумевает изменение адреса получателя таких сообщений.

Способы рассылки спама:

1. Электронная почта.

2. Usenet – использование неконтролируемых групп новостей для размещения рекламы.

3. Мгновенные сообщения – ICQ, QIP, MSN и т. д.

4. Социальные сети и сайты знакомств – получение доступа к учетным записям пользователям и рассылка сообщений от их имени.

5. Блоги, форумы, вики.

6. Сетевые сообщения – появляются в виде всплывающих окон, например, использование Microsoft Windows Messenger.

Способы поиска адресов электронной почты:

1. Общедоступные сайты – сканирование с применением индексирующего робота (харвестер).

2. Usenet – сканирование с применением индексирующего робота (харвестер).

3. Подбор по словарю – адрес почтового ящика – простое слово.

4. Использование троянских программ – получение содержания адресной книги.

5. Корпоративные базы данных – похищение или покупка у сотрудника компании.

Подходы в автоматической фильтрации спама:

1) по контексту – анализ содержания сообщения;

2) по адресу – опознание спамера.

Методы фильтрации спама:

1) статистический анализ – требуется обучение фильтра в ручном режиме;

2) «черный» список;

3) авторизация почтовых серверов;

4) использование DNS-имен;

5) «серые» списки – при получении письма с неизвестного адреса отправляется код временной ошибки (SMTP).

Технические аспекты фильтрации:

- провайдер;
- корпоративный сервер;
- клиент.

5.7. Противодействие вредоносным программам

Вредоносная программа (malware) – любая программа, предназначенная для получения НСД к вычислительным ресурсам хоста или к информации, хранимой на нем. В целях противодействия вредоносным программам используется антивирусное ПО.

Классификационные признаки антивирусного ПО:

- тип нейтрализуемого вредоносного ПО;
- вид анализируемых объектов или процессов;
- режим функционирования;
- реализуемый принцип защиты.

В зависимости от типа нейтрализуемого вредоносного ПО антивирусное ПО может реализовывать:

- реактивную защиту (от известного вредоносного ПО с использованием данных о нем, хранящихся в базах сигнатур об участках кода);
- проактивную защиту (от новых версий вредоносного ПО с использованием сведений о неуникальных особенностях программных кодов).

Вид объектов или процессов, анализируемых антивирусным ПО:

- код подозрительного ПО;
- алгоритм функционирования подозрительного ПО;

- изменения в файлах информационных систем и значениях их контрольных сумм.

Режимы функционирования антивирусного ПО:

- постоянный мониторинг;
- сканирование по расписанию, событию или запросу пользователя.

Принципы защиты, реализуемые антивирусным ПО:

- блокирование или ограничение активности объектов, содержащихся в «черных» списках баз сигнатур, и разрешение запуска всех остальных;
- разрешение активности только безопасных объектов из «белых» списков и запрет активности всех остальных;
- комбинированный принцип (использование «черных» списков для обнаружения угроз и «белых» списков для коррекции результатов детектирования и минимизации ложных срабатываний).

5.8. Применение методов и средств защиты информации в автоматизированных системах

Выбор методов и средств защиты информации в АС определяется перечнем угроз, которые могут быть реализованы по отношению к таким системам. Выделяют следующие типы этих угроз:

1) перехват данных покупателя;
2) мошенничество продавца;
3) мошенничество агента доставки.

Для предотвращение реализации угроз первого типа необходимо обеспечивать шифрование данных и аутентификацию покупателя, второго типа – аутентификацию продавца и аудит продаж, третьего типа – аутентификацию и аудит доставки.

Схемы защиты системы интернет-банкинга подсистемы «интернет-клиент» представлены на рис. 5.9 и 5.10 соответственно.

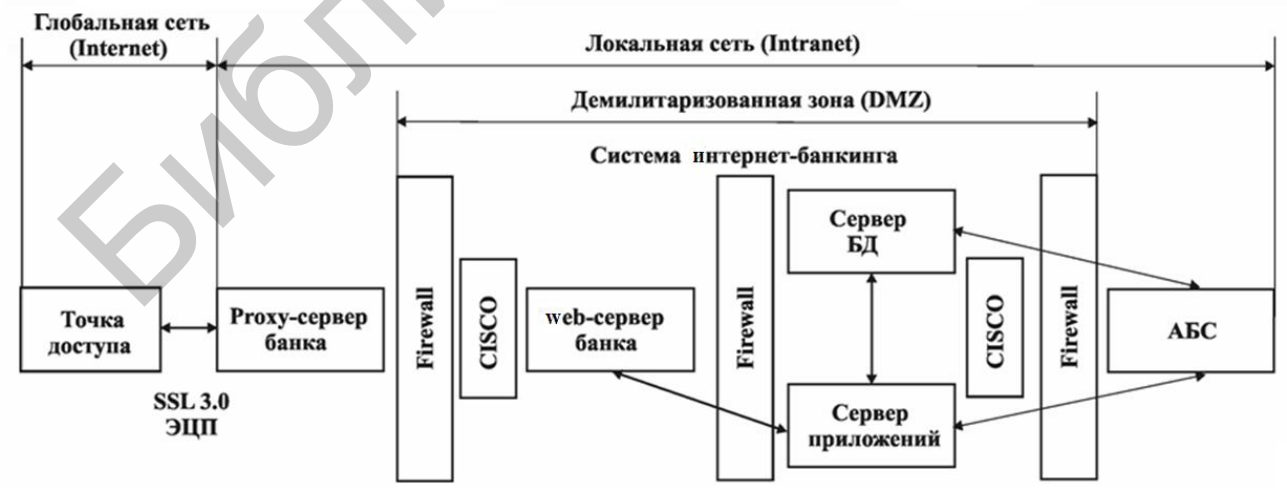

Рис. 5.9. Схема защиты системы интернет-банкинга

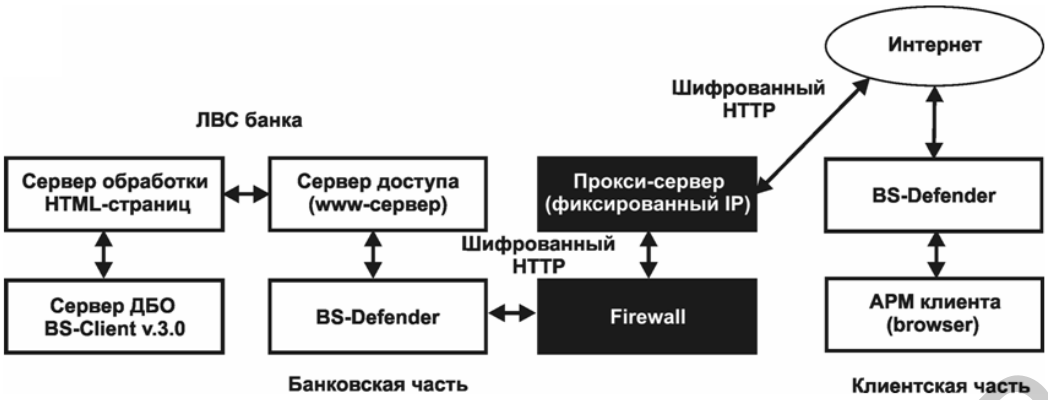

Рис. 5.10. Схема защиты подсистемы «интернет-клиент»

Для защиты системы интернет-банкинга необходимо применять следующие механизмы (см. рис. 5.9):

- аутентификацию (login, password, др. информация);
- криптографическую защиту информации (путем использования протоколов SSL/TLS, ЭЦП, сертификат X 509);
- сегментацию сети (путем создания DMZ);
- фильтрацию трафика (путем использования Firewall).

Для защиты подсистемы «интернет-клиент» необходимо применять следующие механизмы (см. рис. 5.10):

- использование proxy-сервера;
- шифрование данных;
- сегментацию сети (путем создания DMZ);
- реализацию механизма сессий.

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ

BISS	– Belarus Interbank Settlement System
EDI	– Electronic Data Interchange
PIN	– Personal Identification Number
POS	– Point of Sales
АБС	– автоматизированная банковская система
АКА	– автоматический кассовый аппарат
АС	– автоматизированная система
ДБО	– дистанционное банковское обслуживание
ЕРИП	– единое расчетное и информационное пространство
МБР	– межбанковский расчет
МЭ	– межсетевой экран
НБ РБ	– Национальный банк Республики Беларусь
ПК	– персональный компьютер
ПО	– программное обеспечение
ЭД	– электронные деньги
ЭПС	– электронная платежная система

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Защита информации в банковских технологиях : учеб.-метод. пособие / Л. М. Лыньков [и др.]. – Минск : БГУИР, 2008. – 194 с.

2. Шаньгин, В. Информационная безопасность компьютерных систем и сетей / В. Шаньгин. – М. : Форум, 2011. – 416 с.

3. Голдовский, И. Безопасность платежей в Интернете / И. Голдовский. – СПб. : Питер, 2001. – 240 с.

4. Обеспечение информационной безопасности бизнеса / под ред. А. П. Курило. – М. : Издательская группа БДЦ-Пресс, 2005. – 512 с.

5. Петренко, С. А. Управление информационными рисками. Экономически оправданная безопасность / С. А. Петренко, С. В. Симонов. – М. : Компания АйТи; ДМК Пресс, 2004. – 384 с.

6. Банковские операции : учеб. пособие / под ред. С. И. Пупликова. – Минск : Выш. шк., 2003. – 351 с.

7. Деднев, М. А. Защита информации в банковском деле и электронном бизнесе / М. А. Деднев, Д. В. Дыльнов, М. А. Иванов. – М. : Кудиц-образ, 2004. – 512 с.

8. Платонов, В. В. Программно-аппаратные средства обеспечения информационной безопасности вычислительных сетей / В. В. Платонов. – М. : Издательский центр «Академия», 2006. – 240 с.

9. Бил, Дж. Snort 2.1. Обнаружение вторжений / Дж. Бил ; пер. с англ. ; под. ред. А. П. Караваева. – М. : Бином, 2011. – 656 с.

Св. план 2017, поз. 40

Учебное издание

Бойправ Ольга Владимировна
Борботько Тимофей Валентинович

ЗАЩИТА ИНФОРМАЦИИ В БАНКОВСКИХ ТЕХНОЛОГИЯХ

УЧЕБНО-МЕТОДИЧЕСКОЕ ПОСОБИЕ

Редактор *Е. С. Юрец*
Корректор *Е. Н. Батурчик*
Компьютерная правка, оригинал-макет *М. В. Касабуцкий*

Подписано в печать 15.01.2018. Формат 60×84 1/16. Бумага офсетная. Гарнитура «Таймс».
Отпечатано на ризографе. Усл. печ. л. 3,6. Уч.-изд. л. 4,0. Тираж 50 экз. Заказ 250.

Издатель и полиграфическое исполнение: учреждение образования
«Белорусский государственный университет информатики и радиоэлектроники».
Свидетельство о государственной регистрации издателя, изготовителя,
распространителя печатных изданий №1/238 от 24.03.2014,
№2/113 от 07.04.2014, №3/615 от 07.04.2014.
ЛП №02330/264 от 14.04.2014.
220013, г. Минск, П. Бровки, 6