**Безопасность электронных платежей**

***Электронные платежи в банке.***

В главе 4 были рассмотрены особенности подхода к защите электронных банковских систем. Специфической чертой этих систем является специальная форма обмена электронными данными - электронных платежей, без которых ни один современный банк не может существовать.

Обмен электронными данными (ОЭД) — это межкомпьютерный обмен деловыми, коммерческими, финансовыми электронными документами. Например, заказами, платежными инструкциями, контрактными предложениями, накладными, квитанциями и т.п.

ОЭД обеспечивает оперативное взаимодействие торговых партнеров (клиентов, поставщиков,торговых посредников и др.) на всех этапах подготовки торговой сделки, заключения контракта и реализации поставки. На этапе оплаты контракта и перевода денежных средств ОЭД может приводить к электронному обмену финансовыми документами. При этом создается эффективная среда для торгово-платежных операций: [3, с.71]

\* Возможно ознакомление торговых партнеров с предложениями товаров и услуг, выбор необходимого товара/услуги, уточнение коммерческих условий (стоимости и сроков поставки, торговых скидок, гарантийных и сервисных обязательств) в реальном масштабе времени;

\* Заказ товара/услуг или запрос контрактного предложения в реальном масштабе времени;

\* Оперативный контроль поставки товара, получение по электронной почте сопроводительных документов (накладных, фактур, комплектующих ведомостей и т.д.);

\* Подтверждение завершения поставки товара/услуги, выставление и оплата счетов;

\* Выполнение банковских кредитных и платежных операций. К достоинствам ОЭД следует отнести:

\* Уменьшение стоимости операций за счет перехода на безбумажную технологию. Эксперты оценивают стоимость обработки и ведения бумажной документации в 3-8% от общей стоимости коммерческих операций и доставки товаров. Выигрыш от применения ОЭД оценивается, например, в автомобильной промышленности США более чем в $200 на один изготовленный автомобиль [14];

\* Повышение скорости расчета и оборота денег;

\* Повышение удобства расчетов.

Существует две ключевые стратегии развития ОЭД:

1. ОЭД используется как преимущество в конкурентной борьбе, позволяющее осуществлять более тесное взаимодействие с партнерами. Такая стратегия принята в крупных организациях и получила название «Подхода Расширенного Предприятия» (Extended Enterprise) [2, с.230].

2. ОЭД используется в некоторых специфических индустриальных проектах или в инициативах объединений коммерческих и других организаций для повышения эффективности их взаимодействия.

Банки в США и Западной Европе уже осознали свою ключевую роль в распространении ОЭД и поняли те значительные преимущества, которые дает более тесное взаимодействие с деловыми и личными партнерами. ОЭД помогает банкам в предоставлении услуг клиентам, особенно мелким, тем, которые ранее не могли позволить себе ими воспользоваться из-за их высокой стоимости.

Основным препятствием широкому распространению ОЭД является многообразие представлений документов при обмене ими по каналам связи. Для преодоления этого препятствия различными организациями были разработаны стандарты представления документов в системах ОЭД для различных отраслей деятельности: [2, с.234]

QDTI - General Trade Interchange (Европа, международная торговля);

МДСНД - National Automated Clearing House Association (США, Национальная ассоциация автоматизированных расчетных палат);

TDCC - Transportation Data Coordinating Committee (Координационный комитет по данным перевозок);

VICS - Voluntary Interindustry Communication Standart (США, Добровольный межотраслевой коммуникационный стандарт);

WINS - Warehouse Information Network Standarts (Стандарты информационной сети товарных складов).

В октябре 1993 года международная группа UN/ECE опубликовала первую версию стандарта EDIFACT. Разработанный набор синтаксических правил и коммерческих элементов данных был оформлен в виде двух стандартов ISO [2, с.241]:

ISO 7372 - Trade Data Element Directory (Справочник коммерческих элементов данных);

ISO 9735 - EDIFACT - Application level syntax rules (Синтаксические правила прикладного уровня).

Частным случаем ОЭД являются электронные платежи - обмен финансовыми документами между клиентами и банками, между банками и другими финансовыми и коммерческими организациями.

Суть концепции электронных платежей заключается в том, что пересылаемые по линиям связи сообщения, должным образом оформленные и переданные, являются основанием для выполнения одной или нескольких банковских операций. Никаких бумажных документов для выполнения этих операций в принципе не требуется (хотя они могут быть выданы). Другими словами, пересылаемое по линиям связи сообщение несет информацию о том, что отправитель выполнил некоторые операции над своим счетом, в частности над корреспондентским счетом банка-получателя (в роли которого может выступать клиринговый центр), и что получатель должен выполнить определенные в сообщении операции. На основании такого сообщения можно переслать или получить деньги, открыть кредит, оплатить покупку или услугу и выполнить любую другую банковскую операцию. Такие сообщения называются электронными деньгами, а выполнение банковских операций на основании посылки или получения таких сообщений - электронными платежами. Естественно, весь процесс осуществления электронных платежей нуждается в надежной защите. Иначе банк и его клиентов ожидают серьезные неприятности.

Электронные платежи применяются при межбанковских, торговых и персональных расчетах.

Межбанковские и торговые расчеты производятся между организациями (юридическими лицами), поэтому их иногда называют корпоративными. Расчеты с участием физических лиц-клиентов получили название персональных.

Большинство крупных хищений в банковских системах прямо или косвенно связано именно с системами электронных платежей.

На пути создания систем электронных платежей, особенно глобальных, охватывающих большое число финансовых институтов и их клиентов в различных странах, встречается множество препятствий. Основными из них являются:

1. Отсутствие единых стандартов на операции и услуги, что существенно затрудняет создание объединенных банковских систем. Каждый крупный банк стремится создать свою сеть ОЭД, что увеличивает расходы на ее эксплуатацию и содержание. Дублирующие друг друга системы затрудняют пользование ими, создавая взаимные помехи и ограничивая возможности клиентов.

2. Возрастание мобильности денежных масс, что ведет к увеличению возможности финансовых спекуляций, расширяет потоки «блуждающих капиталов». Эти деньги способны за короткое время менять ситуацию на рынке, дестабилизировать ее.

3. Сбои и отказы технических и ошибки программных средств при осуществлении финансовых расчетов, что может привести к серьезным осложнениям для дальнейших расчетов и потере доверия к банку со стороны клиентов, особенно в силу тесного переплетения банковских связей (своего рода «размножение ошибки»). При этом существенно возрастает роль и ответственность операторов и администрации системы, которые непосредственно управляют обработкой информации.

Любая организация, которая хочет стать клиентом какой-либо системы электронных платежей, либо организовать собственную систему, должна отдавать себе в этом отчет.

Для надежной работы система электронных платежей должна быть хорошо защищена.

Торговые расчеты производятся между различными торговыми организациями. Банки в этих расчетах участвуют как посредники при перечислении денег со счета организации-плательщика на счет организации-получателя.

Торговые расчеты чрезвычайно важны для общего успеха программы электронных платежей. Объем финансовых операций различных компаний обычно составляет значительную часть общего объема операций банка.

Виды торговых расчетов сильно различаются для разных организаций, но всегда при их осуществлении обрабатывается два типа информации: платежных сообщений и вспомогательная (статистика, сводки, уведомления). Для финансовых организаций наибольший интерес представляет, конечно, информация платежных сообщений - номера счетов, суммы, баланс и т.д. Для торговых организаций оба вида сведений одинаково важны - первый дает ключ к финансовому состоянию, второй - помогает при принятии решений и выработке политики.

Чаще всего распространены торговые расчеты следующих двух видов: [16]

\* Прямой депозит (direct deposit).

Смысл этого вида расчетов заключается в том, что организация поручает банку осуществлять некоторые виды платежей своих служащих или клиентов автоматически, с помощью заранее подготовленных магнитных носителей или специальных сообщений. Условия осуществления таких расчетов оговариваются заранее (источник финансирования, сумма и т.д.). Они используются в основном для регулярных платежей (выплаты различного рода страховок, погашение кредитов, зарплата и т.д.). В организационном плане прямой депозит более удобен, чем, например, платежи с помощью чеков.

С 1989 г. число служащих, использующих прямой депозит, удвоилось и составило 25% от общего количества. Более 7 млн. американцев получают сегодня заработную плату в виде прямого депозита. Банкам прямой депозит сулит следующие выгоды:

- уменьшение объема задач, связанных с обработкой бумажных документов и, как следствие, экономия значительных сумм;

- увеличение числа депозитов, так как 100% объема платежей должны быть внесены на депозит.

Кроме банков в выигрыше остаются и хозяева, и работники; повышаются удобства и уменьшаются затраты.

\* Расчеты при помощи ОЭД.

В качестве данных здесь выступают накладные, фактуры, комплектующие ведомости и т.д.

Для осуществления ОЭД необходима реализация следующего набора основных услуг :

- электронная почта по стандарту Х.400 ;

- передача файлов;

- связь «точка-точка»;

- доступ к базам данных в режиме on-line;

- почтовый ящик;

- преобразование стандартов представления информации.

Примерами существующих в настоящее время систем торговых расчетов с использованием ОЭД могут служить:

- National Bank и Royal Bank (Канада) связаны со своими клиентами и партнерами с помощью IBM Information Network;

- Bank of Scotland Transcontinental Automated Payment Service (TAPS), основанная в 1986 г., связывает Bank of Scotland с клиентами и партнерами в 15 странах с помощью корреспондентских банков и автоматизированных клиринговых палат.

Электронные межбанковские расчеты бывают в основном двух видов:

\* Клиринговые расчеты с использованием мощной вычислительной системы банка-посредника (клирингового банка) и корреспондентских счетов банков-участников расчетов в этом банке. Система основана на зачете взаимных денежных требований и обязательств юридических лиц с последующим переводом сальдо. Клиринг также широко используется на фондовых и товарных биржах, где зачет взаимных требований участников сделок проводится через клиринговую палату или особую электронную клиринговую систему.

Межбанковские клиринговые расчеты осуществляются через специальные клиринговые палаты, коммерческие банки, между отделениями и филиалами одного банка - через головную контору. В ряде стран функции клиринговых палат выполняют центральные банки. Автоматизированные клиринговые палаты (АКП) предоставляют услуги по обмену средствами между финансовыми учреждениями. Платежные операции в основном сводятся либо к дебетованию, либо к кредитованию. Членами системы АКП являются финансовые учреждения, которые состоят в ассоциации АКП. Ассоциация образуется для того, чтобы разрабатывать правила, процедуры и стандарты выполнения электронных платежей в пределах географического региона. Необходимо отметить, что АКП не что иное, как механизм для перемещения денежных средств и сопроводительной информации. Сами по себе они не выполняют платежных услуг. АКП были созданы в дополнение к системам обработки бумажных финансовых документов. Первая АКП появилась в Калифорнии в 1972 г., в настоящее время в США функционируют 48 АКП. В 1978 г. была создана Национальная Ассоциация АКП (National Automated Clearing House Association; NACHA), объединяющая все 48 сети АКП на кооперативных началах. [2, с.289]

Объем и характер операций постоянно расширяются. АКП начинают выполнять деловые расчеты и операции обмена электронными данными. После трехлетних усилий различных банков и компаний была создана система СТР (Corporate Trade Payment), предназначенная для автоматизированной обработки кредитов и дебетов. По мнению специалистов в ближайшее время тенденция расширения функций АКП будет сохраняться.

\* Прямые расчеты, при которых два банка осуществляют связь непосредственно между собой с помощью счетов "лоро-ностро", возможно, при участии третьего лица, играющего организационную или вспомогательную роль. Естественно, объем взаимных операций должен быть достаточно велик для оправдания затрат на организацию такой системы расчетов. Обычно такая система объединяет несколько банков, при этом каждая пара может связываться непосредственно между собой, минуя посредников. Однако в этом случае возникает необходимость управляющего центра, занимающегося защитой взаимодействующих банков (рассылкой ключей, управлением, контролем функционирования и регистрацией событий).

В мире существует достаточно много таких систем - от небольших, связывающих несколько банков или филиалов, до гигантских международных, связывающих тысячи участников. Наиболее известной системой этого класса является SWIFT.

В последнее время появился третий вид электронных платежей - обработка электронных чеков (electronic check truncation), суть которого состоит в прекращении пути пересылки бумажного чека в финансовой организации, в которой он был предъявлен. В случае необходимости дальше «путешествует» его электронный аналог в виде специального сообщения. Пересылка и погашение электронного чека осуществляются с помощью АКП. [2, с.291]

В 1990 г. NACHA анонсировала первый этап тестирования национальной экспериментальной программы «Electronic Check Truncation». Ее целью является сокращение расходов на обработку огромного количества бумажных чеков.

Пересылка денег с помощью системы электронных платежей включает следующие этапы (в зависимости от конкретных условий и самой системы порядок может меняться):

1. Определенный счет в системе первого банка уменьшается на требуемую сумму.

2. Корреспондентский счет второго банка в первом увеличивается на ту же сумму.

3. От первого банка второму посылается сообщение, содержащее информацию о выполняемых действиях (идентификаторы счетов, сумма, дата, условия и т.д.); при этом пересылаемое сообщение должно быть соответствующим образом защищено от подделки: зашифровано, снабжено цифровой подписью и контрольными полями и т.д.

4. С корреспондентского счета первого банка во втором списывается требуемая сумма.

5. Определенный счет во втором банке увеличивается на требуемую сумму.

6. Второй банк посылает первому уведомление о произведенных корректировках счета; это сообщение также должно быть защищено от подделки способом, аналогичным защите платежного сообщения.

7. Протокол обмена фиксируется у обоих абонентов и, возможно, у третьего лица (в центре управления сетью) для предотвращения конфликтов.

На пути передачи сообщений могут быть посредники - клиринговые центры, банки-посредники в передаче информации и т.п. Основная сложность таких расчетов - уверенность в своем партнере, то есть каждый из абонентов должен быть уверен, что его корреспондент выполнит все необходимые действия.

Для расширения применения электронных платежей проводится стандартизация электронного представления финансовых документов. Она была начата в 70-х годах в рамках двух организаций [2, с. 298]:

1) ANSI (American National Standart Institute) опубликовал документ ANSI X9.2-1080, (Interchange Message Specification for Debit and Credit Card Message Exchange Among Financial Institute, Спецификация обменных сообщений для дебетных и кредитных карточек обмена между финансовыми организациями). В 1988 аналогичный стандарт был принят ISO и получил название ISO 8583 (Bank Card Originated Messages Interchange Message Specifications - Content for Financial Transactions);

2) SWIFT (Society for Worldwide Interbank Financial Telecommunications) разработало серию стандартов межбанковских сообщений.

В соответствии со стандартом ISO 8583 финансовый документ содержит ряд элементов данных (реквизитов), расположенных в определенных полях сообщения или электронного документа (электронной кредитной карточки, сообщения в формате Х.400 или документа в синтаксисе EDIFACT). Каждому элементу данных (ЭД) назначается свой уникальный номер. Элемент данных может быть как обязательным (то есть входить в каждое сообщение данного вида), так и необязательным (в некоторых сообщениях может отсутствовать).

Битовая шкала определяет состав сообщения (те ЭД, которые в нем присутствуют). Если некоторый разряд битовой шкалы установлен в единицу, это означает, что соответствующий ЭД присутствует в сообщении. Благодаря такому методу кодирования сообщений уменьшается общая длина сообщения, достигается гибкость в представлении сообщений со многими ЭД, обеспечивается возможность включения новых ЭД и типов сообщений в электронный документ стандартной структуры. [2, с. 299]

Существует несколько способов электронных межбанковских платежей. Рассмотрим два из них: оплата чеком (оплата после услуги) и оплата аккредитивом (оплата ожидаемой услуги). Другие способы, как например оплата с помощью платежных требований или платежных поручений, имеют сходную организацию.

Оплата чеком основана на бумажном или другом документе, содержащим идентификацию подателя. Этот документ является основанием для перевода определенной в чеке суммы со счета владельца на счет подателя. Платеж чеком включает следующие этапы :

- получение чека;

- представление чека в банк;

- запрос о переводе со счета владельца чека на счет подателя;

- перевод денег;

- уведомление о платеже.

Основными недостатками таких платежей являются необходимость существования вспомогательного документа (чека), который легко подделать, а также значительные затраты времени на выполнение платежа (до нескольких дней).

Поэтому в последнее время более распространен такой вид платежей как оплата аккредитивом. Он включает следующие этапы:

- уведомление банка клиентом о предоставлении кредита;

- уведомление банка получателя о предоставлении кредита и перевод денег;

- уведомление получателя о получении кредита.

Такая система позволяет осуществлять платежи в очень короткие сроки. Уведомление о предоставлении кредита можно направлять по (электронной) почте, на дискетах, магнитных лентах.

Каждый из рассмотренных выше видов платежей имеет свои преимущества и свои недостатки. Чеки наиболее удобны при оплате незначительных сумм, а также при нерегулярных платежах. В этих случаях задержка платежа не очень существенна, а использование кредита нецелесообразно. Расчеты с помощью аккредитива обычно используются при регулярной оплате и для значительных сумм. В этих случаях отсутствие клиринговой задержки позволяет экономить много времени и средств за счет уменьшения периода оборота денег. Общим недостатком этих двух способов является необходимость затрат на организацию надежной системы электронных платежей. [2, с. 300]

***Вопросы безопасности электронных платежей.***

Для определения общих проблем защиты систем ОЭД рассмотрим в прохождение документа при ОЭД. Можно выделить три основных этапа:

- подготовка документа к отправке;

- передача документа по каналу связи;

- прием документа и его обратное преобразование.

С точки зрения защиты в системах ОЭД существуют следующие уязвимые места:

1. Пересылка платежных и других сообщений между банками или между банком и клиентом;

2. Обработка информации внутри организаций отправителя и получателя;

3. Доступ клиента к средствам, аккумулированным на счете.

Одно из наиболее уязвимых мест в системе ОЭД - пересылка платежных и других сообщений между банками, или между банком и банкоматом, или между банком и клиентом. При пересылке платежных и других сообщений возникают следующие проблемы:

- внутренние системы организаций Получателя и Отправителя должны быть приспособлены к получению/отправке электронных документов и обеспечивать необходимую защиту при их обработке внутри организации (защита оконечных систем);

- взаимодействие Получателя и Отправителя документа осуществляется опосредованно - через канал связи. Это порождает три типа проблем: 1) взаимного опознавания абонентов (проблема установления аутентификации при установлении соединения); 2) защиты документов, передаваемых по каналам связи (обеспечение целостности и конфиденциальности документов); 3) защиты самого процесса обмена документами (проблема доказательства отправления/доставки документа);

- в общем случае Отправитель и Получатель документа принадлежат к различным организациям и друг от друга независимы. Этот факт порождает проблему недоверия - будут ли предприняты необходимые меры по данному документу (обеспечение исполнения документа).

С технической точки зрения эти проблемы решаются с помощью нескольких механизмов, отвечающих за обеспечение адекватной безопасности электронных банковских систем. Работа большинства этих механизмов обеспечивается службами сети с расширенным набором услуг (Value-Added Network, VAN). Службы, реализующие ОЭД, должны выполнять следующие функции:

- обеспечить защиту от случайных и умышленных ошибок;

- обеспечить адаптацию к частым изменениям количества пользователей, типов оборудования, способов доступа, объемов трафика, топологии;

- поддерживать различные типы аппаратного и программного обеспечения, поставляемого различными производителями;

- осуществлять управление и поддержку сети для обеспечения непрерывности работы и быстрой диагностики нарушений;

- реализовывать полный спектр прикладных задач ОЭД, включая электронную почту;

- реализовывать максимально возможное число требований партнеров;

- включать службы резервного копирования и восстановления после аварий.

В системах ОЭД должны быть реализованы следующие механизмы, обеспечивающие реализацию функций защиты на отдельных узлах системы ОЭД и на уровне протоколов высокого уровня:

- равноправная аутентификацию абонентов;

- невозможность отказа от авторства сообщения/приема сообщения;

- контроль целостности сообщения;

- обеспечение конфиденциальности сообщения;

- управление доступом на оконечных системах;

- гарантии доставки сообщения;

- невозможность отказа or принятия мер по сообщению;

- регистрация последовательности сообщений;

- контроль целостности последовательности сообщений;

- обеспечение конфиденциальности потока сообщений.

Полнота решения рассмотренных выше проблем сильно зависит от правильного выбора системы шифрования. Система шифрования (или криптосистема) представляет собой совокупность алгоритмов шифрования и методов распространения ключей. Правильный выбор системы шифрования помогает:

- скрыть содержание документа от посторонних лиц (обеспечение конфиденциальности документа) путем шифрования его содержимого;

- обеспечить совместное использование документа группой пользователей системы ОЭД путем криптографического разделения информации и соответствующего протокола распределения ключей. При этом для лиц, не входящих в группу, документ недоступен;

- своевременно обнаружить искажение, подделку документа (обеспечение целостности документа) путем введения криптографического контрольного признака (имитовставки);

- удостовериться в том, что абонент, с которым происходит взаимодействие в сети является именно тем, за кого он себя выдает (аутентификация абонента/источника данных).

Следует отметить, что при защите систем ОЭД большую роль играет не столько шифрование документа, сколько обеспечение его целостности и аутентификация абонентов (источника данных) при проведении сеанса связи. Поэтому механизмы шифрования в таких системах играют обычно вспомогательную роль.

Надежность всей криптосистемы в целом во многом зависит от механизмов рассылки (распределения) ключей между участниками взаимодействия. Проблема рассылки ключей в настоящее время не имеет общих решений. В каждом конкретном случае она должна решаться с учетом особенностей функционирования всей защищаемой АСОИБ. Существует много различных подходов к решению этой проблемы. Не вдаваясь в тонкости каждого из них, поскольку это выходит далеко за рамки обсуждаемого предмета, кратко опишем основные: [2, с.305]

\* Метод базовых/сеансовых ключей.

Суть метода состоит в том, что вводится иерархия ключей (главный ключ (ГК)/ключ шифрования ключей (КК)/ключ шифрования данных (КД).

Иерархия может быть двухуровневой (КК/КД) или трехуровневой (ГК/КК/КД). При этом старший ключ в иерархии распространяется между участниками взаимодействия неэлектронным образом, исключающем его перехват и/или компрометацию. Стандарт определяет три способа распространения ключей: непосредственная передача, передача с использованием центра распространения и передача с использованием центра трансляции ключей. Стандарт не применяется для распространения ключей между специализированными банковскими устройствами, такими как банкоматы и устройства расчета в точке продажи;

\* Метод открытых ключей. Основан на односторонних преобразованиях, при которых часть ключа остается открытой и может быть передана по линиям связи в открытом виде. Это избавляет от дорогостоящей процедуры распространения ключей шифрования неэлектронным способом;

\* Метод выведенного ключа, применяется для защиты информации, передаваемой между терминалом системы расчета в точке продажи и компьютером банка. При этом методе ключ для шифрования каждой следующей транзакции вычисляется путем одностороннего преобразования предыдущего ключа и параметров транзакции;

\* Метод ключа транзакции. Также применяется для защиты информации, передаваемой между терминалом системы расчета в точке продажи и компьютером банка. Он отличается от метода выведенного ключа тем, что при вычислении ключа для следующей транзакции не используются ее параметры.

Жестким ограничением на реализацию мер по защите информации накладываются требования уже существующих стандартов ОЭД. Поскольку абсолютно неуязвимых систем не бывает, каждая организация должна самостоятельно решать вопрос об уровне защищенности собственной системы ОЭД: что лучше - затратить дополнительные средства на организацию и поддержание защиты или сэкономить и работать в условиях постоянного риска.

Необходимость поддержки электронных банковских услуг с помощью специальных банковских и других сетей, а также с помощью национальных клиринговых систем, радикально изменила отношения между банками и их клиентами. Только за последнее десятилетие стали доступны, а сейчас используются повсеместно, различные клиринговые системы, осуществляющие весь спектр банковских операций. Данные и инструкции вводятся, распределяются и обрабатываются в них в режиме реального времени.

Безопасность операций с наличностью и расчетных услуг требует принятия тех же общих мер, которые необходимы для защиты любой электронной финансовой услуги. Особое внимание необходимо обратить на защиту терминалов, подключенных к системам электронных платежей.

Если банк выполняет операции повышенного риска, то реализуемые процедуры обеспечения безопасности должны включать парольную защиту, многоуровневую авторизацию пользователей, контроль операций, ведение системного журнала. Также следует осуществлять разграничение доступа пользователей к терминалам и другим внешним устройствам, которые должны быть защищены физически. Для обеспечения безопасности данных, передаваемых по линиям связи, необходимо использовать криптографические методы.

Система безопасности центральной АСОИБ должна включать многоуровневый контроль доступа к периферийным устройствам и центральной базе данных.

Если операции повышенного риска не выполняются, некоторые требования к безопасности могут быть ослаблены или ликвидированы совсем. Задачи по обеспечению безопасности определяются для каждого конкретного случая индивидуально в процессе анализа риска.

В настоящее время в мире существует большое количество систем электронных платежей. Наиболее известные из них: [2, с.312]

- S.W.I.F.T. (The Society for Worldwide Inter-bank Financial Telecommunication) - бесприбыльное кооперативное международное сообщество, целью которого является организация межбанковских расчетов по всему миру.

- FedWire - самая крупная система американских межбанковских коммуникаций, соединяющая головные конторы округа Federal Reserve, ветви банков Federal Reserve и более 500 других банков с помощью центра коммутации в Вирджинии.

- CHAPS (Clearing Houses Automated Payment System) - система поддержки электронных платежей между сравнительно небольшой (около 300) группой банков Лондона, большинство из которых отделения иностранных банков, использующих Лондон в качестве расчетного центра.

- CHIPS (Clearing Houses Interbank Payment System) - клиринговая система США, организованная Нью-йоркской ассоциацией клиринговых палат (New York Clearing House Association - NYCHA) (см. [1]).

Рассмотрим подробнее организацию некоторых из этих систем, уделив особое внимание рассмотрению вопросов обеспечению их безопасности.

Система SWIFT.

Сообщество SWIFT было организовано в 1973 году и в 1977 г. начали осуществляться первые операции с использованием сетей связи. Члены сообщества находятся в Южной, Центральной и Северной Америке, Европе, Африке, Австралии и на Дальнем Востоке.

Система SWIFT позволяет пользователям получить следующие преимущества :

- повышение эффективности работы банков за счет стандартизации и современных способов передачи информации, способствующих развитию автоматизации и рационализации банковских процессов;

- надежный обмен платежными сообщениями;

- сокращение операционных расходов по сравнению с телексной связью;

- удобный прямой доступ пользователей SWIFT к своим корреспондентам по всему миру (доставка сообщения с обычным приоритетом в любую точку мира - 20 минут, доставка срочного сообщения - 30 секунд);

- использование стандартизованных сообщений SWIFT, позволяющее преодолеть языковые барьеры и свести к минимуму различия в практике осуществления банковских операций;

- повышение конкурентоспособности банков-членов SWIFT за счет того, что международный и кредитный оборот все более концентрируется на пользователях SWIFT.

Стоимость передачи сообщений членами сообщества определяется по единому тарифу и зависит от количества соединений, адреса, объема сообщения. За счет высокой интенсивности графика (более 5 млн. сообщений в день) стоимость передачи одного сообщения оказывается ниже, чем в других средствах связи (телекс, телеграф). Дополнительно к основной функции (обмену сообщениями) система SWIFT также выполняет роль форума для выработки соглашения о стандартах представления и передачи данных.

Существует две системы SWIFT: SWIFT I (введена в строй в 1977 году) и SWIFT II (внедрена с 1990 года). Хотя по архитектуре эти системы различны, пользователь не отличает сообщений, полученных по SWIFT I или SWIFT II. Ниже мы рассмотрим архитектуру и защиту системы SWIFT II.

В архитектуре SWIFT II можно выделить четыре основные уровне иерархии: [7, с.141]

- банковский терминал, который устанавливается в банке и предназначен для доступа персонала банка в сеть. Терминалами системы SWIFT обычно являются персональные компьютеры. Смонтированное оборудование может сдаваться «под ключ» (на базе миниЭВМ компаний Unisys и NCR) или интегрироваться в существующую банковскую систему (например на базе семейство миниЭВМ VAX компании DEC);

- региональный процессор (РП), основным назначением которого является организация взаимодействия пользователей некоторой ограниченной области (республики, страны, группы стран). Места расположения РП заранее не определяются. Как правило, РП оснащаются сдублированными ЭВМ фирмы Unisys;

- слайс-процессор (СП), необходимый для обмена сообщениями между подключенными к нему РП, краткосрочного или длительного архивирования сообщений и генерации системных отчетов. Система SWIFT может сохранять передаваемые сообщения на срок до 14 дней. Это помогает избегать проблем, связанных с трактовкой текстов сообщений. На сегодняшний день существует три СП, каждый из них которых оснащен тремя машинами А12 фирмы Unisys, одна из которой является резервной. Один СП может обработать до 3.5 миллионов сообщений в день. Допускается включение в сеть дополнительных СП;

- процессор управления системой (ПУС), выполняющий функции монитора системы, управления системой и сетью. Существует два ПУС, один из которых находится в Голландии, а второй в США. Каждый ПУС может контролировать состояние и управлять работой СП и РП, работой сетевых программ и оборудования, подключением пользователей и их рабочими сеансами, включая выбираемые пользователем прикладные задачи. ПУС единственный уровень системы, который не занят обработкой сообщений, а предназначен исключительно для управления системой SWIFT в целом.

Сообщения системы SWIFT содержат поля, идентифицирующие всех участников передачи информации и платежей.

Банк заказчика операции информирует банк-отправитель о необходимости послать сообщение и переводит ему соответствующую сумму. Банк получателя при приеме сообщения переводит эту сумму на счет расчетного банка, который осуществляет платежи.

Расчеты между банком-отправителем и банком-получателем осуществляются с помощью счета, который открывается в одном из них для другого. Кто для кого открывает счет, зависит от типа валюты, в которой производятся расчеты. Если платежи осуществляются в валюте государства, в котором находится банк-получатель, то он вносит соответствующую сумму в дебет счета банка-отправителя в своем банке. Наоборот, если платежи осуществляются в валюте государства, в котором находится банк-отправитель, то он открывает у себя счет банка получателя и предоставляет ему кредит на соответствующую сумму.

Безопасность в системе SWIFT обеспечивается применением организационных, программных и технических мер.

В системе SWIFT существует строгое разделение ответственности за поддержание безопасности системы. Так банк, подключенный к системе, отвечает за правильную эксплуатацию и физическую защиту терминалов, модемов и линий связи до регионального процессора, за правильное оформление сообщения при передаче его в сеть и наличие работоспособных терминалов. Всю остальную ответственность за передачу сообщений несет администрация системы. Управление защитой осуществляется управлением Главного инспектора. Контроль защищенности системы осуществляется через случайные промежутки времени, чтобы убедиться, что все требования к: безопасности выполняются должным образом.

Защита банковских терминалов предусматривает разграничение доступа пользователей к нему по паролю и специальной пластиковой карточке. При входе пользователя в систему производится взаимное опознавание терминала и системы. Автоматическое отключение от SWIFT происходит в следующих случаях:

- при обнаружении помехи или обрыве соединения;

- при неоднократном обнаружении ошибки при передаче данных или в принятом сообщении;

- при сбое РП, к которому подсоединены терминалы.

Сведения о подключении и отключении терминала регистрируются в специальном журнале.

Для обеспечения конфиденциальности передаваемых сообщений используется шифрование при помощи специальных устройств, устанавливаемых в тракте передачи «банковский терминал - региональный процессор». Для шифрования информации используются три типа ключей: главный (64 бита), вторичный (128 бит) и шифрования данных (64 бита). Главный и вторичный ключи устанавливаются представителями SWIFT. Ключ шифрования данных генерируется специальным шумовым источником в процессе работы. Смена модулей, содержащих первичный и вторичный ключи, осуществляется периодически по указанию Главного инспектора системы. Банкам предоставляется возможность устанавливать собственные устройства шифрования для защиты линии связи (естественно после консультаций с представителями SWIFT). Обеспечение конфиденциальности сообщений не является самой главной задачей системы, хотя этому также уделяется серьезное внимание.

Для аутентификации пользователей и обеспечения целостности сообщений в системе SWIFT существует оригинальный алгоритм аутентификации, детали которого держатся в секрете. Как и для любого такого алгоритма, базовыми требованиями являются надежное распределение ключей между двумя абонентами и защита их от остальных. Надежная аутентификация достигается за счет четкого распределения ответственности. Ключи рассылаются банкам попарно, другие банки и персонал сети доступа к ним не имеют; рассылается также руководство по управлению ключами: процедура и время замены ключей и т.д. Кроме того, SWIFT может использоваться для обмена конфиденциальной информацией между кооперацией банков, однако, в этом случае ответственность за обеспечение безопасности ложится на участников обмена.

В то же время аутентификации взаимодействующих организаций недостаточно для надежной работы сети, так как она не предполагает защиты от подмены, уничтожения или задержки сообщений.

Для обеспечения целостности потока передаваемых сообщений применяется механизм номеров сообщений. Соединения между SWIFT и пользователями поддерживаются двумя (входной и выходной) последовательностями номеров. Входная последовательность обрабатывается слайс-процессорами системы, выходная - получателями сообщений. Такой механизм обеспечивает полный контроль за последовательностью переданных и полученных сообщений для любой пары оконечных пользователей. Он удостоверяет, что ни одно сообщение не уничтожено и не продублировано.

Еще одна задача защиты - предотвращение передачи ложных сообщений, не искажающих последовательности номеров и имеющих истинную аутентификацию. Эта задача решается банками - оконечными пользователями системы. Именно они ответственны за корректность переданных от их имени сообщений. Кроме того, на пунктах обработки и передачи сообщений также существуют механизмы защиты от подделки сообщений.

Для центральной части SWIFT, состоящей из слайс-процессоров, региональных процессоров и линий связи, защита сообщений является задачей администрации системы. Доступ к системе, программное обеспечение и сообщения пользователей строго контролируются, как и доступ на территорию машинных залов. Международные линии связи, соединяющие слайс-процессоры между собой, слайс-процессоры и региональные процессоры, имеют надежную криптозащиту. Персонал системы SWIFT не имеет доступа к содержимому пересылаемых сообщений. [2, с.356]

В реализации защиты SWIFT отражены основные подходы, которые применяются при организации системы электронных платежей в целом.