УДК 336.717:004.78

Кузнецов А.А., Король О.Г.
Ткачов А.М.

Анализ механизмов обеспечения безопасности банковской информации во внутриплатежных системах коммерческого банка

Развитие экономики любого государства сегодня невозможно без высокоэффективной системы денежного обращения и использования современных платежных механизмов. Процесс развития рыночной экономики требует наличия соответствующей платежной системы, позволяющей осуществлять расчеты в народном хозяйстве в соответствии с общепринятыми мировыми стандартами. В этой связи на первый план выходят надежность, безопасность, а также срочность осуществления платежей.

Национальная платежная система – сложная многоуровневая система централизованного управления, обеспечивающая качественный стратегически важный канал проведения финансовых транзакций [1].

Такая система относится к сложным многоуровневым системам управления критического применения (СУКП), в которых передача информации требует контроля безопасности на каждом уровне [1]. Основными элементами системы являются система электронных платежей (СЭП) и внутриплатежная система коммерческого банка (ВПС КБ), структурная схема СУКП национальной платежной системы представлена на рис. 1.

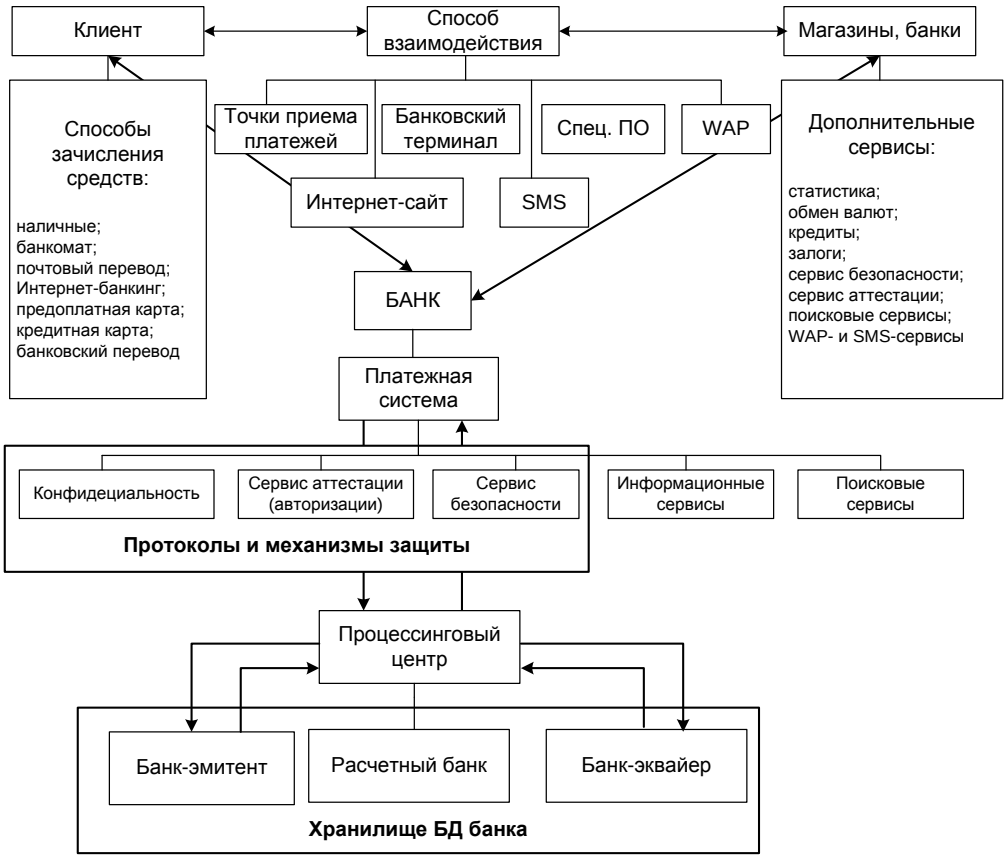

Рис. 1. **Структурная схема национальной платежной системы**

Эффективность функционирования каждого из элементов зависит от быстродействия и надежности используемых механизмов аутентификации. Практически любая современная банковская система не обходится без использования механизмов шифрования и обеспечения аутентичности информации.

Тем не менее, на сегодняшний день не существует научно-обоснованной концепции и механизмов обеспечения финансовой безопасности банковской деятельности национальной платежной системы в целом [2]. Новизна и актуальность проблем обеспечения безопасности банковской деятельности привлекают внимание ученых, среди которых: В.Ю. Гайкович В.Ю., А.Ю. Першин, М. И. Анохин, Н. П. Варновский, В. М. Сидельников, В. В. Ященко [3, 4]. и др. Среди зарубежных авторов — S. D. Galbraith, N. P. A. Smart, M. O. Rabin, В. Столлингс [5 — 7]. Современные подходы к обеспечению экономической и финансовой безопасности банковской деятельности, обеспечению их надежности и устойчивости представили в своих работах Ю. В. Романец, П. А. Тимофеев, В. Ф. Шаньгин [8]. Проведенный обзор работ в данном направлении показал, что проблемными вопросами в открытых системах, в том числе и ВПС КБ являются вопросы обеспечения аутентичности и целостности открытых ключей. Однако результаты этих работ позволяют выбрать механизмы обеспечения безопасности информации, отвечающие требованиям к стойкости и вычислительной сложности криптопреобразований лишь на определенное время.

Известным приемом в построении современных механизмов аутентификации является использование стойких криптопримитивов, примером являются схемы UMAC, TTMAC, HMAC и др. Подход, используемый в данных схемах, позволил свести стойкость схем аутентификации к стойкости используемого алгоритма (DES, TDES, AES), что также не решило возникшей проблемы. Следовательно, современной и востребованной задачей, позволяющей решить существующие противоречия при выборе механизмов аутентификации и оценки их стойкости, является проведение анализа криптографической стойкости существующих криптопримитивов и разработка рекомендаций по обоснованию стойкости современных систем аутентификации.

Целью статьи является рассмотрение основных механизмов обеспечения безопасности во внутриплатежных системах коммерческого банка (ВПС КБ), проведение анализа угроз и механизмов обеспечения аутентичности, целостности банковской информации в ВПС КБ.

В развитии рыночных отношений и формировании коммерческих структур главенствующую роль играют коммерческие банки, аккумулирующие огромные финансовые потоки. Это привлекает огромный интерес криминальных структур, спецслужб и конкурентов. Основная угроза при этом ложится именно на ВПС КБ [9]. В связи с этим, проблема безопасности национальной платежной системы (обеспечение аутентичности, целостности и конфиденциальности всех проводимых электронных операций) остается нерешенной.

Рассмотрим основные составляющие национальной платежной системы.

Система электронных платежей (СЭП) – комплекс аппаратных и программных средств, производящих оплату товаров посредством компьютерных или магнит-

ных карточек, предназначенных для создания основы электронных денег, перспективной альтернативы методам оплаты наличными деньгами и чеками [10]. На рис. 2 представлена обобщенная структурная схема электронной платежной системы.

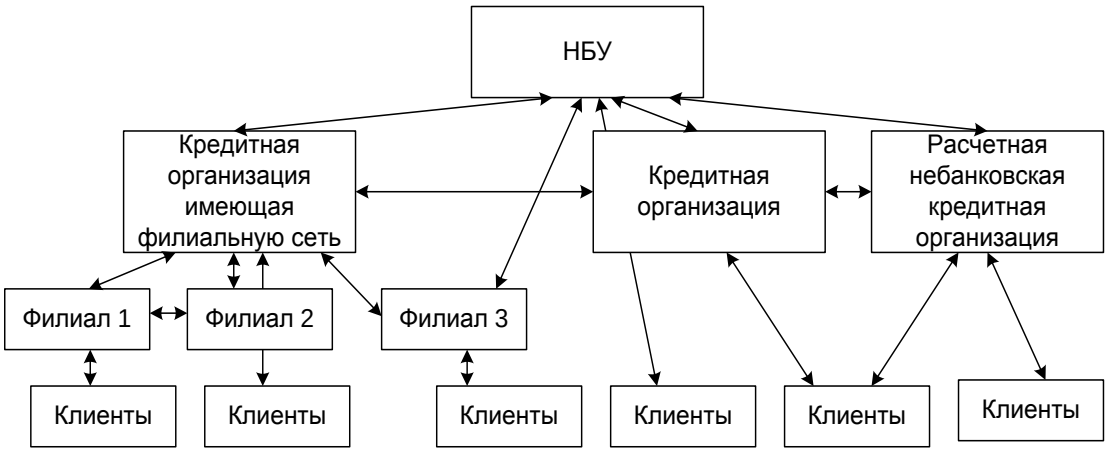

Рис. 2. **Обобщенная структурная схема электронной платежной системы**

Банк, заключивший соглашение с платежной системой и получивший соответствующую лицензию, может выступать в двух качествах – как банк-эмитент и как банк-эквайер. Банк-эмитент выпускает пластиковые карты и гарантирует выполнение финансовых обязательств, связанных с использованием этих карт как платежных средств. Банк-эквайер обслуживает предприятия торговли и сервиса, принимающие к оплате карты как платежные средства, а также принимает эти платежные средства к обналичиванию в своих отделениях и через принадлежащие ему банкоматы. Основными неотъемлемыми функциями банка-эквайера являются финансовые операции, связанные с выполнением расчетов и платежей точками обслуживания. Технические атрибуты деятельности банка-эквайера (обработка запросов на авторизацию; перечисление на расчетные счета точек средстве за товары и услуги, предоставленные по картам; прием, сортировка и пересылка документов, фиксирующих совершение сделок с использованием карт и т. п.) могут быть делегированы эквайером процессинговым центрам и связаны с обеспечением защиты передаваемых данных [8].

Данная система интегрируется в банковские системы и множество типов терминалов, в том числе переносные, работающие в автономном режиме, и банкоматы, выполняющие более широкий спектр функций. СЭП управляет потоками электронных денег, связью терминалов и локальных сетей.

Для обеспечения надежной работы, электронная платежная система должна быть надежно защищена. С точки зрения информационной безопасности в СЭП существуют следующие уязвимые места:

пересылка платежных и других сообщений между банком и клиентом и между банками;

обработка информации внутри организаций отправителя и получателя сообщений;

доступ клиентов к средствам, аккумулированным на счетах.

Одним из наиболее уязвимых мест в системе электронных платежей является пересылка платежных и других сообщений между банками, между банком и банко-

матом, между банком и клиентом. Пересылка платежных и других сообщений связана со следующими особенностями:

внутренние системы организаций отправителя и получателя должны быть приспособлены для отправки и получения электронных документов и обеспечивать необходимую защиту при их обработке внутри организации (защита оконечных систем);

взаимодействие отправителя и получателя электронного документа осуществляется опосредовано через канал связи.

Эти особенности порождают следующие *проблемы*:

взаимное опознавание абонентов (проблема установления взаимной подлинности при установлении соединения);

защита электронных документов, передаваемых по каналам связи (проблемы обеспечения конфиденциальности и целостности документов);

защита процесса обмена электронными документами (проблема доказательства отправления и доставки документа);

обеспечение исполнения документа (проблема взаимного недоверия между отправителем и получателем из-за их принадлежности к разным организациям и взаимной независимости) [3].

Для обеспечения функций защиты информации на отдельных узлах системы должны быть реализованы следующие *услуги защиты* [8]:

управление доступом на оконечных системах;

контроль целостности сообщения;

обеспечение конфиденциальности сообщения;

взаимная аутентификация абонентов;

причастность к формированию сообщения;

гарантии доставки сообщения;

причастность к получению сообщения;

регистрация последовательности сообщений;

контроль целостности последовательности сообщений.

Качество решения указанных выше проблем в значительной мере определяется рациональным выбором криптографических средств, при реализации механизмов защиты (рис. 3).

Рис.3. **Механизмы защиты**

Внутриплатежная система коммерческого банка обеспечивает реализацию функций обработки платежных документов (прием от филиалов файлов начальных платежей; контроль начальных платежей СЭП, формирование и отправка файлов начальных платежей в АРМ-СЭП; прием от АРМ-СЭП файлов ответных платежей; отправка файлов ответных платежей на филиалы), управление филиалами-участниками ВПС (установка лимитов корсчетов филиалов в ВПС; блокировка начальных и ответных платежей филиалов), взаимодействие с информационно-поисковой системой (ИПС) НБУ, а также работа внутренней ИПС. Сравнение функциональных возможностей и механизмов защиты современных ВПС представлены в табл. 1.

Таблица 1

Сравнение функциональных возможностей современных ВПС

Системы электронных платежей банка	**Функции системы**	**Уровни применения механизмов защиты**
1	2	3
ВПС »ГРАНТ» – предназначена для выполнения платежей в национальной валюте Украины между головным банком и его филиалами, а также платежей в СЭП НБУ головным банком и его филиалами	Обработка платежных документов. Защита информации. Управление филиалами-участниками ВПС. Взаимодействие с информационно-поисковой системой (ИПС) НБУ, а также работа внутренней ИПС	уровень защищенной операционной среды; уровень СУБД; уровень прикладного программного обеспечения; уровень средств криптографической защиты информации
Enigma – обеспечивает автоматизацию внутрибанковских и межбанковских платежей в многофилиальных банках Украины	Обмен пакетами документов и технологическими файлами между головным банком, филиалами и системой электронных платежей НБУ. Наложение логических и бухгалтерских ограничений на различные платежные операции в СЭП НБУ, ВПС и АБС банка	уровень средств криптографической защиты информации

Окончание табл. 1

1	2	3
ProFIX/TELEBANK – предназначена для управления ресурсами многофилиального банка	Обработка входящих и исходящих сообщений. Проведение ручных утверждений сообщений, поступающих на исполнение от служб и филиалов. Предоставление услуг другим банкам в качестве клирингового банка	Система обладает встроенными механизмами обеспечения безопасности электронных платежей, которые построены по принципам и форматам СЭП. Используется система шифрования на базе алгоритма DES и электронной подписи на базе алгоритма RSA
Внутрибанковская Платежная Система (ВПС) — новый программный продукт, разработанный специалистами компании R-Style Ukraine, предназначенный для управления финансовыми потоками в многофилиальном банке	Принятие от филиала-отправителя внутрибанковский платеж и доставить его через расчетный центр в филиал-получатель. Выполнение всех операций по учету движения средств, предусмотренные выбранной бухгалтерской моделью, обеспечивает корректность консолидированного баланса банка и гарантирует целостность данных и защиту информации	– уровень защищенной операционной среды – уровень СУБД – уровень прикладного программного обеспечения – уровень средств криптографической защиты информации

Несмотря на широкое применение различных криптографических алгоритмов на различных уровнях защиты, внутриплатежные системы подвержены различным атакам и угрозам, подразделяемым на угрозы *финансовых ресурсов*, так называемая чувствительная информация: персональная информация пользователей (имена, пароли, аккаунты, идентификационные номера, банковские реквизиты, данные о корпоративных сетях). С помощью такого рода сведений возможен обход многоуровневых систем защиты от вторжений. И угрозы *информационных ресурсов*, которые подразделяются на внешние (технические) и внутренние (неправомерные действия сотрудников). На рис. 4 представлены основные типы угроз информационных ресурсов [11].

Рис. 4. **Основные типы угроз информационных ресурсов**

Наиболее уязвима инфраструктура безопасности крупных банков. Большое количество сотрудников, множество компьютеров, разнородные сети и права доступа – эти дополнительные факторы облегчают задачу злоумышленникам [12].

Сегодня внутренние угрозы являются одной из наиболее актуальных проблем информационной безопасности. Согласно статистике, неправомерные действия сотрудников самих организаций причиняют наибольший ущерб и до 90% средств, выделяемых на информационную безопасность, тратится на обеспечение защиты от внутренних атак [12].

Неправомерные действия пользователей приводят к значительному ущербу и подразделяются:

нарушение конфиденциальности данных;

кража информации;

искажение информации;

действия, приводящие к сбоям информационных систем;

утрата информации.

Лидирующую позицию занимают нарушения конфиденциальности данных, приводящие к утечке закрытой информации. По сведениям специалистов [12], из 100 случаев неправомерных действий сотрудников 65 относятся к нарушению конфиденциальности данных, диаграмма распределения внутренних угроз представлена на рис. 5.

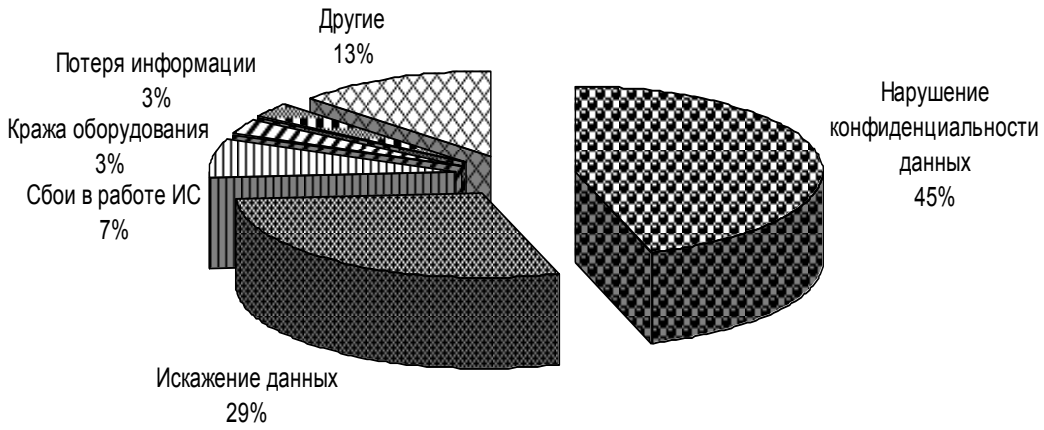

Рис. 5. **Диаграмма распределения внутренних угроз**

Самыми распространенными путями утечки информации являются электронная почта (до 22%), интернет (сайты, чаты, форумы, бесплатные почтовые сервисы) — до 20%, интернет-пейджеры (ICQ/AOL, AIM, MSN, Yahoo!) и мобильные накопители (компакт-диски, USB-накопители) — до 19%, печатающие устройства до — 8%, и другие источники — до 12%. Диаграмма утечки конфиденциальной информации представлена на рис. 6.

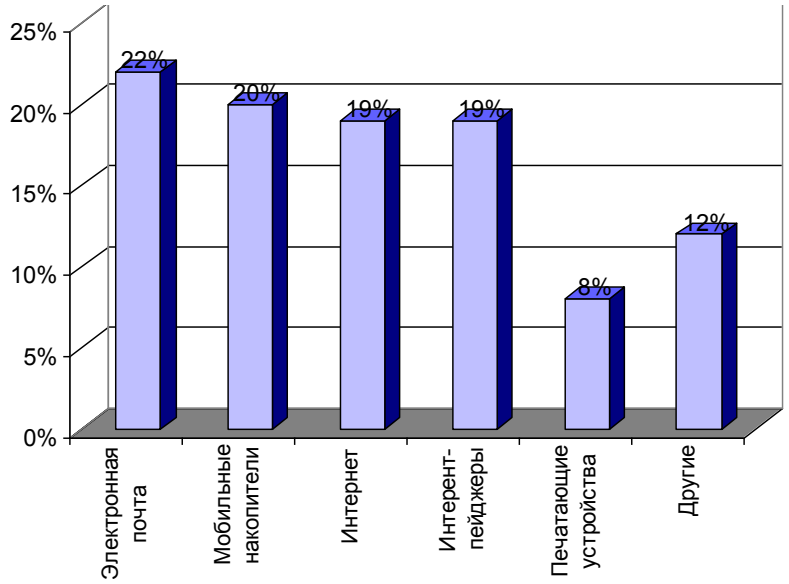

Рис. 6. **Диаграмма утечки конфиденциальной информации**

Для обеспечения защиты от рассмотренных угроз используются различные криптографические механизмы. ВПС КБ имеет собственную систему защиты информации, отвечающую требованиям НБУ.

Система защиты информации ВПС КБ должна обеспечивать высокий уровень информационной безопасности банка на каждом этапе подготовки, обработки и выполнения электронных банковских документов на всех уровнях за счет положенного в ее основу комплексного подхода к проблеме обеспечения защиты.

Создание защищенной среды обработки информации реализуется на нескольких уровнях [13]:

первый – уровень защищенной операционной среды (ОС), обеспечивающей авторизованный доступ к файлам, каталогам и программам в отдельности на чтение, модификацию и запуск и удовлетворяющей общепризнанному в мире уровню безопасности;

второй – уровень системы управления базами данных (СУБД), обеспечивающей авторизованный доступ к информации в базе данных в отдельности на чтение, пополнение и модификацию, а также автоматическое ведение протокольных журналов работы пользователей;

третий – уровень прикладного программного обеспечения ВПС КБ и СЭП, на котором реализованы подсистемы:

внутреннего аудита, протоколирующая все изменения состояния платежных документов;

разграничения доступа к информации и управления правами пользователей, являющаяся логическим продолжением механизмов СУБД и обеспечивающая предоставление каждому пользователю строго регламентированного набора полномочий как на выполнение тех или других операций, так и на доступ к соответствующей части информации БД;

четвертый – уровень средств криптографической защиты информации на базе программных средств криптографической защиты информации (КЗИ), обеспечивающих:

наложение/проверку цифровой подписи (ЦП) на все платежные документы;

наложение/проверку ЦП на все платежные и служебные файлы;

шифрование циркулирующей информации;

управление ключами ЦП пользователей СЭП.

Основные механизмы аутентичности, целостности информации в ВПС КБ на различных уровнях (между филиалами, отделениями, центрами и терминалами) и информации, циркулирующей в банковской системе, основаны на использовании стандартов блочно-симметричных шифров (DES, ГОСТ 28147-89 (4 режим)) [14 — 17].

Примером программной реализации рассмотренных механизмов аутентичности являются программные средства криптографической защиты информации "Грифон-Б" и "Грифон-Л", разработанные ООО СНПФ «АРГУС». Программное средство "Грифон-Б" предназначено для криптографической защиты конфиденциальной информации в автоматизированных банковских системах и применяется для обмена информацией внутри корпоративной сети банка, с клиентами, работающими по системе "Клиент-Банк", в системах обслуживания пластиковых карт [13].

Программное средство криптографической защиты информации "Грифон-Л" [18] предназначено для использования в сфере банковской деятельности, в частности, для обмена конфиденциальной (в т. ч. финансовой) информацией внутри корпоративной сети банка, с клиентами, работающими по системе "Клиент-Банк", в си-

стемах обслуживания пластиковых карт и пр. Основные технические характеристики данных программных средств защиты приведены в табл. 2.

Таблица 2

Основные характеристики программных средств защиты

№ п/п	Сравнительные характеристики	"Грифон-Б"	"Грифон-Л"
1	2	3	4
1	Обеспечение реализации криптоалгоритмов	криптографического преобразования в соответствии с ГОСТ 28147-89 в режимах простой замены, гаммирования и гаммирования с обратной связью для областей памяти и файлов; формирования иммитовставки длиной 32 бит в соответствии с ГОСТ 28147-89; хеширования в соответствии с ГОСТ 34.311-95 для областей памяти и файлов; генерации секретного ключа электронной цифровой подписи *x*, секретного параметра *k* для реализации ГОСТ 34.310-95, а также генерацию сеансовых ключей для реализации ГОСТ 28147-89; генерации открытой ключевой информации, вычисление и проверку электронной цифровой подписи на базе асимметричного криптографического алгоритма в соответствии с ГОСТ 34.310-95 для областей памяти и файлов; распределения сеансовых ключей в соответствии с протоколом обмена ключами на основе алгоритма Диффи-Хеллмана	криптографическое преобразование в соответствии с ГОСТ 28147-89 в режимах простой замени, гаммирования и гаммирования с обратной связью; формирование иммитовставки длиной 32 бит, в соответствии с ГОСТ 28147-89; хеширование в соответствии с ГОСТ 34.311-95; формирование системных параметров, вычисление и проверку электронной цифровой подписи (ЕЦП) на базе асимметричного криптографического алгоритма в соответствии с ГОСТ 34.310-95; генерацию секретного ключа электронной цифровой подписи *x* , секретного параметра *k* для реализаций ГОСТ 34.310-95, а также генерацию сеансовых ключей для реализации ГОСТ 28147-89; генерацию случайных чисел, которые имеют статистические характеристики, допускающие их использование в качестве ключевых данных для криптографических преобразований в соответствии с алгоритмами ГОСТ 28147-89, ГОСТ 34.310-95;

Окончание табл. 2

1	2	3	4
			формирование ключей защиты сеансовых ключей в соответствии с протоколом асимметричного распределения ключей типа Диффи-Хеллмана
2	Основные функции программы	Получение справочной информации. Тест хеширования, в т.ч. шифрования простой заменой. Получение чисел p, q (512 бит и 1024 бит). Тест создания и проверки ЭЦП. Тесты быстродействия (шифрования, хеширования, генерации чисел, наложения подписи и др.). Простое и адресное шифрование строки или файла. Хеширование строки или файла. Генерация общесистемных параметров. Генерация макета ключа пользователя. Генерация ключа пользователя. Смена пароля на секретном ключе. Подпись строки или файла. Проверка подписи. Снятие подписи. Общий секретный ключ Z AB по Диффи-Хеллману	
3	Применяемые стандарты	ГОСТ 28147-89. Алгоритм криптографического преобразования. ГОСТ 34.311-95. Функция хеширования. ГОСТ 34.310-95. Процедура выработки и проверки электронной подписи на базе асимметричного криптографического алгоритма. Кроме того, использованы схема распределения симметричных ключей Диффи-Хеллмана и стандарт X9.17 для генерации сеансовых ключей	
4	Быстродействие на ПК с процессором 633 МГц обеспечивает	шифрование области памяти в режиме простой замены – не менее 5 Мб/с; хеширование области памяти – не менее 1.5 Мб/с; вычисление электронной цифровой подписи при длине ключа 512 бит – не более 0.015 с; проверка электронной подписи при длине ключа 512 бит – не более 0.020 с; генерация общего ключа по методу Диффи-Хеллмана при длине ключа 512 бит – не более 0.015 с	шифрование области памяти в режиме простой замены – не менее 2,5 Мб/с; хеширование области памяти – не менее 1 Мб/с; вычисление электронной цифровой подписи при длине ключа 512 бит – не более 0.020 с; проверка электронной подписи при длине ключа 512 бит – не более 0,030 с; генерация общего секретного ключа при длине открытой составляющей ключа 512 бит – не более 0.020 с

Проверка работоспособности данных программ выполняется с помощью встроенных функций самоконтроля. Поставляются программы с интерфейсом командной строки в нескольких модификациях: для выполнения тестовых примеров, проверки быстродействия базовых алгоритмов, выполнения функций генерации ключей, а также выполнения основных операций, необходимых пользователю (шифрование, цифровая подпись и др.) [13, 18].

Таким образом, проведенные исследования показали, что для обеспечения безопасности банковской информации в ВПС КБ используются криптографические симметричные и асимметрические алгоритмы шифрования, обеспечивающие аутентичность и целостность сообщений. Вместе с тем, некоторые криптографические функции не обеспечивают требуемой защиты без специальных секретов кодов подтверждения подлинности, которые должны представлять дополнительный механизм обработки исходного или шифрованного текста (ЭЦП, хэш-функции), являются эффективными для больших объемов потоков данных и не удовлетворяют требованиям к современным системам управления критического применения (ВПС КБ).

Литература

1. http://www.cryptopro.ru/cryptopro/documentation/dig-cert.htm

2. Артеменко Д. А. Механизм обеспечения финансовой безопасности банковской деятельности: Дис. канд. экон. наук. : Ростов н/Д:, 1999 — 190 с.

3. Гайкович В.Ю. Безопасность электронных банковских систем / В. Ю.Гайкович, А. Ю. Першин. — М.: Ед. Европа, 1994.— 285 с.

4. Логинов А. А. Общие принципы функционирования электронных платежных систем и осуществление мер безопасности при защите от злоупотребления и мошенничества / А. А.Логинов, Н. С. Елхимов // Конфидент. — 1995. — №4. — С. 48 — 54.

5. Rabin M. O. Fingerprinting by Random Polynomials // Tech. Rep. TR-15-81, Center: in Compating Technology, Harvard Univ., Cambridge, Mass., 1981.

6. Столлингс В. Криптография и защита сетей: принципы и практика: Пер. с англ. 2-е изд. — М.: Изд. дом «Вильям», 2001. — 672 с.

7. Шефановский Д. Б. ГОСТ 34.11 – 94. Функция хэширования. Краткий анализ. — М.: Учебн. центр “Инфозащита". 2001, — 18 с.

8. Романец Ю. В. Защита информации в компьютерных системах и сетях / Ю .В. Романец, П. А.Тимофеев, В. Ф Шаньгин; [Под ред. В. Ф. Шаньгина. — 2-е изд., перераб. и доп. — М.: Радио и связь, 2001. – 376 с.

9. Межбанковские расчеты на Украине // http://e2000.kyiv.org/biblioteka/biblio/stat/ukr_bank.html

10. Вихорев С. В. Классификация угроз информационной безопасности // http://www2.cnews.ru/comments/security/elvis_class.shtml

11. http://www.jetinfo.ru/2005/10/1/article1.9.200518.html

12. Программное средство криптографической защиты информации "Грифон-Б" // http://www.banksoft.com.ua/index.php?id=28

13. Программное средство «Библиотека функций криптографической защиты информации "Грифон-Л" // http://www.banksoft.com.ua/index.php?id=27

14. ГОСТ 34.310-95. Межгосударственный стандарт. Информационная технология. Криптографическая защита информации. Процедура выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма. — К.: Госстандарт Украины. 1998. — 68 с.

15. ГОСТ 34.311-95. Межгосударственный стандарт. Информационная технология. Криптографическая защита информации. Функция хеширования. К.: — Госстандарт Украины. 1998. — 46 с.

16. ГОСТ Р 34.10-94. Информационная технология. Криптографическая защита информации. Процедуры выработки и проверки электронной цифровой подписи на базе асимметричного криптографического алгоритма М.: МИФИ — 1995. – 16 с.

17. Анохин М. И. ГОСТ Р34.11-94. Информационная технология. Криптографическая защита информации. Функция хэширования.Криптография в банковском деле / М. И. Анохин, Н. П. Варновский, В. М. Сидельников, В. В. Ященко — М.: МИФИ, 1997. — 274 с.

18. http://www.carteblanche-online.info/index.php?option=com_content&task=view&id=105