Недостатки использования ЭЦП и альтернатива ее использования в банковском электронном документообороте

Суслова Ирина Александровна
019 гр.
Защита информации
2004г

1. Недостатки использования электронной цифровой подписи в банковском электронном документообороте 2
2. Подсистема защитного кода аутентификации 2
2.1. Введение 2
2.2. Процедура персонализации. 3
2.3. Процедура регистрации 4
2.4. Процедура формирования ЗКА 5
2.5. Защита системы от взлома 5
3. О предприятии-разработчике 5

1. Недостатки использования электронной цифровой подписи в банковском электронном документообороте

В настоящее время во многих банковских операциях используются цифровые подписи. В банковских системах цифровые подписи предназначены, в основном, для предотвращения попыток злоумышленника изменить уже существующий или ввести фиктивный электронный банковский документ. В Российской Федерации законодательно определено использование электронной цифровой подписи (ЭЦП), основанной на асимметричном алгоритме, с секретным ключом шифрования для вычисления и открытым для проверки ЭЦП (ГОСТ Р 34.10 – 11.94). Однако, ЭЦП, основанная на ГОСТ Р 34.10 имеет ряд недостатков.

1. В качестве первого недостатка можно указать размер ЭЦП, который по ГОСТ Р 34.10 составляет 64 байта. Если к электронному документу добавить служебную информацию, размер которой в общем случае составляет 50-200 байт, то заверка каждого электронного документа ЭЦП становится нерациональным, т.к. размер реальной информации может составлять всего треть от всего объема электронного документа. Этот недостаток можно устранить, объединяя несколько электронный банковских документов в пачки и заверяя всю пачку ЭЦП. Но в этом случае ЭЦП заверяется вся пачка, а не отдельный банковский документ, поэтому добавление лишних документов в пачку пройдет незамеченным, т.к. целостность ЭЦП нарушена не будет.
2. Следующим недостатком ЭЦП можно назвать то, что алгоритм вычисления ЭЦП сложен в вычислениях и является сравнительно медленным даже при длине параметра p = 512 бит. В крупных банках, где суточный объем электронных банковских документов достигает десятков тысяч, время, затраченное на вычисление и проверку ЭЦП настолько велико, что тормозится работа всей банковской системы в целом. Если использовать значение параметра p = 1024 бита, то подобные проблемы возникают и при меньшем объеме электронного документооборота.
3. И наконец, при работе банка гораздо более значимым является эффективное обнаружение несанкционированного вмешательства в электронный банковский документооборот, чем возможность проведения доказательного разбора спорных ситуаций, т.е. для банка важнее обнаружить попытку незаконного изменения электронного банковского документа в процессе работы, чем потом доказывать факт несанкционированного доступа (НСД) к банковскому документу в арбитражном суде.

2. Подсистема защитного кода аутентификации

2.1. Введение

Альтернативой использованию ЭЦП может служить функция вычисления защитного кода аутентификации (ЗКА), основанная на симметричном алгоритме (в качестве функции вычисления ЗКА используется хеш-функция по ГОСТ Р 34.11 – 94).

Во-первых, симметричные алгоритмы превосходят по скорости работы асимметричные. Во-вторых, стойкость к взлому симметричных алгоритмов позволяет уменьшить размер ЗКА по сравнению с ЭЦП. Одним из недостатков симметричных криптографических алгоритмов является сложность распространения ключей. Для первичного обмена ключами между участниками информационной системы необходимо наличие защищенного канала связи. Этот недостаток можно устранить, если использовать для хранения и распространения секретных ключей аппаратную поддержку. В качестве средств аппаратной поддержки подсистемы защитного кода аутентификации электронных банковских документов могут использоваться комплексы (контроллеры с программным обеспечением) «Аккорд-4++», «Аккорд-5», «Аккорд-СБ», «Бука».

В подсистеме ЗКА участвуют **операторы**, идентификатором каждого оператора является зарегистрированное в подсистеме **ТМ-устройство** (устройство Touch Memory)**.**

Рабочим местом оператора является **терминал**, который представляет собой ЭВМ с установленным на ней зарегистрированным программно-аппаратным комплексом. В подсистеме ЗКА каждое ТМ-устройство может работать только на одном терминале. На одном терминале может работать несколько операторов (до 10). Для каждого терминала должен быть назначен **администратор терминала**.

В подсистеме ЗКА существует также специализированный АРМ (автоматизированное рабочее место) регистрации – **АРМ-Р**. На АРМ-Р проходят процедуру регистрации все персонализированные контроллеры и ТМ-устройства участников подсистемы. На АРМ-Р также происходит выработка команд, со сменой общесистемных ключей. Обеспечивает работу этого АРМ-Р **администратор подсистемы ЗКА**.

Администратор подсистемы ЗКА также обеспечивает работу АРМ персонализации – **АРМ-П.** На АРМ-П происходит выработка общесистемных ключей, на основе которых персонализируются все контроллеры.

Таким образом, структура подсистемы защитного кода аутентификации выглядит следующим образом: (Рис.1)

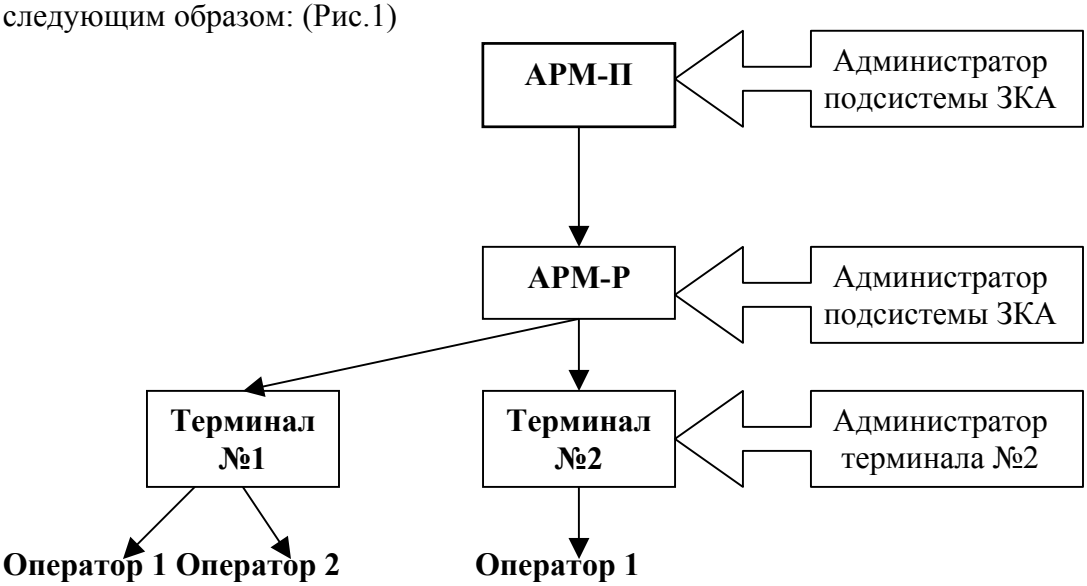

Рисунок 1Структура подсистемы защитного кода аутентификации.

2.2. Процедура персонализации.

В подсистеме защитного кода аутентификации используется ключевая схема, основанная на одних и тех же для каждого контроллера общесистемных ключах. Формирование общесистемных ключей происходит во внутренней памяти каждого контроллера на основе некоторого множества внешних первичных ключей (до 8 штук), т.е. контроллер

считывает внешние ключи, вычисляет значения системных ключей и записывает их в свой процессора вместе с номером версии системных ключей Ver=1 и присвоенным контроллеру регистрационным номером:

К общим системным ключам относятся:

- системный ключ ЗКА - Кзка;
- системный ключ регистрации Операторов - Кро;
- системный ключ регистрации Администраторов – Кра;
- системный ключ перешифрования – Кпш;

Также для каждого контроллера терминала формируется ключ регистрации группы - Кгр. Этот ключ уникален для каждой группы терминалов и одинаков для всех терминалов одной группы. Все ключи подсистемы имеют размер 32 байта. На этом процедура персонализации заканчивается.

2.3. Процедура регистрации

Процедура регистрации контроллеров и ТМ-устройств операторов выполняется на отдельном рабочем месте (АРМ-Р) с установленным персонализированным контроллером и производится администратором подсистемы ЗКА.

При регистрации оператора в ТМ-идентификатор оператора будет записан очередной порядковый номер и регистрационная запись

N_OP, N_TER, hash (IDTM, N_OP, N_TER, Кш),

где N_OP – номер оператора;

N_TER – номер терминала, к которому приписан данный оператор;

IDTM – серийный номер ТМ- идентификатора.

После этого ТМ-устройство передается оператору.
Регистрация контроллера заключается в перенесении в базу данных администратора ЗКА сведений о самом контроллере (номер и серийный номер контроллера).
После регистрации, контроллеры и ТМ-устройства распределяются по банковской системе. В терминалах не ведется внешней базы данных, т.к. данные о зарегистрированных операторах хранятся во внутренней энергонезависимой памяти контроллера.

После администратор терминала «активирует» приписанные к данному терминалу ТМ-устройства. Для этого каждый оператор вводит пароль и прислоняет свой ТМ-идентификатор для проверки регистрационной записи АРМ-Р.

Проверяется:

- совпадение регистрационного номера контроллера терминала и поля N_TER регистрационной записи;
- совпадение вычисленного значения hash(IDTM, N_OP, N_TER, Кш) и значения из регистрационной записи.

Если проверка дала положительный результат, терминал производит перерегистрацию этого ТМ-устройства путем записи на него аналогичной, но собственной регистрационной записи

N_OP, N_TER, hash (IDTM, N_OP, N_TER, PSW, Кр оператора или администратора),

где PSW – введенный с клавиатуры пароль оператора.

2.4. Процедура формирования ЗКА

Когда оператор начинает работать на терминале, он вводит пароль и прикладывает свое ТМ-устройство, откуда контроллер считывает регистрационную запись и сверяет с регистрационной записью, хранящейся в памяти контроллера.

Проверяется:

- наличие в памяти контроллера терминала записи, соответствующей данному оператору;
- совпадение регистрационного номера контроллера терминала и поля N_TER регистрационной записи;
- совпадение вычисленного значения hash (IDTM, N_OP, N_TER, PSW, Кр) и значения из регистрационной записи.

Если данные совпадают, то оператор допускается к работе. При работе с электронным банковским документом, оператор формирует код аутентификации, который подтверждает, что документ не был изменен при работе оператора.

Процедура формирования ЗКА проверяет, что оператор к работе допущен, вырабатывает случайный блок данных <Rand> размером 9 байт и вычисляет значение

$$Ka\_n\_op = hash(Ka, <Rand>, N\_OP, Kзка),$$

которое будет являться сеансовым ключом защитного кода аутентификации.

Затем вычисляется код аутентификации

(N_OP, <Rand>, Ver, N_TER, hash (Ka_n_op, N_TER, hash (Data), Ka_n_op)). Этим кодом однозначно идентифицируется, какой оператор работал с электронным документом и были ли внесены изменения в этот документ.

2.5. Защита системы от взлома

1. Если утеряно ТМ-устройство оператора, производится процедура перерегистрации действующих ТМ-устройств операторов группы на новую версию ключа регистрации группы. Эта процедура может быть проведена на **любом** Терминале группы. Затем на **каждом** Терминале группы меняется версия ключа регистрации группы.
2. При компрометации или утере контроллера терминала на АРМ-Р формируется файл удаленной смены системных ключей и загружается на каждом терминале подсистемы. Внутреннее программное обеспечение контроллера терминала не позволяет загрузить этот файл на скомпрометированном контроллере.

3. О предприятии-разработчике

Технология защиты электронного документооборота с помощью подсистемы защитного кода аутентификации разработана предприятием ОКБ САПР (http://www.accord.ru/index.shtml).

Использованные материалы:

1. Технология защиты электронного документооборота http://www.informacia.ru/security/antivirus12.htm
2. Описание применения защитного кода аутентификации.
3. Гост Р 34.11
4. Гост Р 34.10
5. http://www.accord.ru/Texnology/El_docum/el_docum.shtml