ТЕХНИЧЕСКИЕ НАУКИ

Бильдь Андрей Тадеушевич
магистрант, инженер-программист
Белорусский государственный университет информатики и радиоэлектроники, ЗАО «СОФТКЛУБ – Центр разработки»
г. Минск, Республика Беларусь
Живицкая Елена Николаевна
канд. техн. наук, доцент, проректор
Белорусский государственный университет информатики и радиоэлектроники
г. Минск, Республика Беларусь

АКТУАЛЬНЫЕ МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ, ПРИМЕНЯЕМЫЕ В СОСТАВЕ УЧЕТНО-ОПЕРАЦИОННОГО КОМПЛЕКСА ИНТЕРНЕТ-БАНКИНГА

Аннотация*: статья посвящена проблеме безопасности информации при использовании систем дистанционного банковского обслуживания. Автор обращает внимание на необходимость обеспечения сохранности и безопасности информации, предоставляемой клиентом банковским учреждениям на примере платежных операций. Предложены методы защиты информации, применение которых позволяет повысить уровень безопасности информации и снизить риск потери или хищения информации.*

Ключевые слова*: дистанционное банковское обслуживание (ДБО), Интернет-банкинг (On-line banking, WEB-banking), платежная инструкция, SSL (Secure Sockets Layer), ЭЦП (электронная цифровая подпись), безопасность информации.*

Одним из способов дистанционного взаимодействия банка с клиентом является такая система, как Интернет-Клиент (иначе On-line banking или WEB-

banking). При таком способе пользователь обращается через интернет к системе, которая размещается на web-сервисе банка.

В настоящее время как минимум половина из зарегистрированных юридических лиц используют системы дистанционного банковского обслуживания регулярно – бумажных платежных поручений уже не существует. В связи с этим клиент банка подвержен (помимо всех прочих) риску потери информации и хищения средств с помощью компьютерных технологий.

Немаловажной частью системы интернет-банкинга является учетно-операционный комплекс по подготовке платежных инструкций. Этот инструмент обеспечивает повышение качества обслуживания клиентов банка по совершению расчетов по всем счетам клиентов в различных банках Республики Беларусь.

Ниже представлена схема, по которой плательщик передает платежные инструкции:

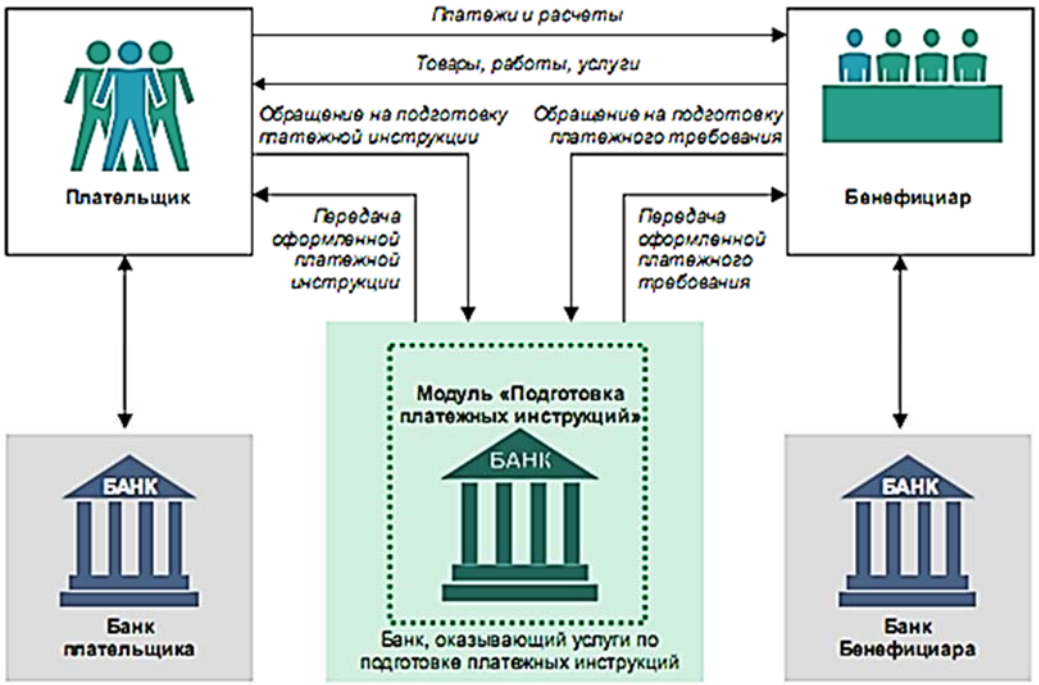

Рис. 1 – Подготовка платежных инструкций

Для работы с документами в системе интернет-банкинга существует ряд методов защиты.

1. Взаимодействие клиента и банка при использовании системы посредством сети интернет осуществляется на web-странице банка.

2. Система интернет-банкинга предоставляет информацию через открытые средства коммуникации. Для обеспечения безопасности передачи данных используется протокол SSL 3.0 (Secure Sockets Layer). Это метод 128/256-битового кодирования, осуществляющий коммуникации между браузером и сетевым контейнером.

3. Идентификация пользователя при входе в систему по имени (логину) и паролю.

4. При входе пользователя в систему используется дополнительный код для защиты от автоматических регистраций.

5. Пользователь обязан хранить в секрете и не передавать третьим лицам свои параметры аутентификации.

6. Пользователь имеет возможность сменить выданные ему имя и пароль.

7. Ведется журнал аудита по всем действиям пользователя.

8. Банк вправе приостановить или ограничить доступ пользователя к системе при наличии у банка достаточных оснований считать, что возможна попытка несанкционированного доступа от имени пользователя.

9. При осуществлении запросов используется ЭЦП (электронная цифровая подпись). Это один из самых распространенных протоколов защиты информации. Электронная подпись – информация в электронной форме, которая присоединена к другой информации в электронной форме (подписываемой информации) или иным образом связана с такой информацией и которая используется для определения лица, подписывающего информацию [1]. По своей сути электронная подпись представляет собой реквизит электронного документа, позволяющий установить отсутствие искажения информации в электронном документе с момента формирования ЭЦП и проверить принадлежность подписи владельцу сертификата ключа ЭЦП. Сертификат ключа ЭЦП – это цифровой документ, подтверждающий соответствие между открытым ключом и информацией, идентифицирующей владельца ключа. В системе ДБО это работает следующим образом: готовый документ может быть отправлен в Банк только после того как будет подписан необходимым количеством подписей и примет статус «Подписан».

По умолчанию все типы документов требуют подписания одной подписью перед отправкой в банк. В зависимости от типа документа, для его подписания требуются наличие одной или двух (первой и второй) подписей. Подписываться могут только документы в статусах «Новый» и «Согласован». Для конкретного пользователя (для любого документа) определяется привилегия подписи первой либо второй подписью с или без права единственной подписи. Документ, требующий подписания одной подписью, считается подписанным, если его подписал пользователь, обладающий правом любой подписи. Документ, требующий подписания двумя подписями, считается подписанным, если его подписали пользователи с правами первой и второй подписи (в любом порядке) либо один пользователь, обладающий правом единственной подписи. Снять подпись (в том числе и «чужую») может только пользователь, обладающий правом любой подписи (для защиты от возможности удаления любым пользователем уже подписанного документа). После снятия подписи документ возвращается в статус «Новый».

10. Гибкая система настроек позволяет ограничить действия пользователя по видам операций и по номерам счетов, по которым он имеет право получать информацию. В данном случае это означает, что авторизированные пользователи интернет-банкинга имеют различные уровни доступа к функционалу. Администратор может присвоить пользователю свою роль, в соответствии с которой он (пользователь) будет наделен определенными полномочиями. Персональные данные и пароли пользователей закодированы в базе данных, и они не могут быть получены кем-либо, даже системным администратором. Каждая группа пользователей имеет собственные привилегии, устанавливающие методы реализации бизнес-компонентов, которые могут быть запрошены ею.

Таким образом, все вышеперечисленные методы защиты обеспечивают довольно высокий уровень безопасности и существенно снижают риск потери или хищения информации.

Список литературы

1. Федеральный закон «Об электронной подписи» N 63-ФЗ от 06.04.2011 Ст.2.п.1.