ОБЕСПЕЧЕНИЕ ЗАЩИЩЕННОГО ОБМЕНА ИНФОРМАЦИЕЙ ПРИ ОРГАНИЗАЦИИ РАБОТЫ С ФОНДОМ СЛУЖЕБНОГО ПОЛЬЗОВАНИЯ ЭЛЕКТРОННОЙ БИБЛИОТЕКИ

А.А. Кузнецов
Московский государственный технический университет им. Н.Э. Баумана
reply@mail.ru

Аннотация

В работе рассмотрена организация работы электронной библиотеки, обеспечивающей разноуровневый допуск пользователей к фондам и защищенную доставку заказанных документов.

1. Библиотеки с разным уровнем допуска

Платные электронные библиотеки и электронные библиотеки, содержащие материалы ограниченного доступа, нуждаются в программной поддержке, обеспечивающей защиту запросов и предоставляемой пользователям информации от перехвата, копирования или подмены. Особенно актуальной эта задача является при организации защиты электронной библиотеки, работающей как в локальной, так и в открытой внешней сети. Для полноценной работы такой библиотеки необходимо создание трех отдельных программ, являющихся элементами распределенной системы (назовем ее, например, «спецхран»), обеспечивающих кроме своих базовых функций надежную защиту информации при обмене сообщениями между ними [1]. Рассмотрим рабочие функции и необходимые возможности элементов такой распределенной системы.

2. Функциональные схемы отдельных узлов библиотеки

2.1. Функциональная схема сервера

Функциональная схема сервера электронной библиотеки приведена на рис.1.

Функции сервера электронной библиотеки включают:

- выработку открытого ключа, обеспечивающего поддержку закрытого канала связи с читателями и службой технической поддержки;
- создание и удаление карточки читателя;
- передача в службу технической поддержки поручений читателей, выходящих за пределы компетенции сервера;
- доставка электронных документов читателям.

Функции отдельных блоков сервера:

Блок приема запросов поддерживает соединение с читателем, получает от него запросы и передает на блок расшифровки запросов.

Блок расшифровки запросов по идентификатору пользователя выбирает из базы данных ключей пользователей симметричный ключ, с помощью которого расшифровывает полученный запрос. Если данный пользователь обратился к серверу впервые, то симметричный ключ и запрос расшифровывается секретным ключом сервера и симметричный ключ размещается в базе данных ключей пользователей.

Блок проверки полномочий пользователя сопоставляет запрос с полномочиями пользователя (служащий / клиент, уровень допуска клиента). Если для данного пользователя такой запрос разрешен, то он передается блоку обработки запросов. В противном случае читателю отправляется отказ.

Блок обработки запросов обрабатывает полученный запрос, используя или модифицируя информацию, хранящуюся в базе данных информации о читателях.

Блок зашифровки ответов шифрует сформированный ответ симметричным ключом пользователя, приславшего запрос.

Блок отправки ответов отправляет зашифрованный ответ пользователю.

База данных информации о клиентах хранит информацию о читателях и историю карточки читателя.

База данных ключей пользователей хранит симметричные ключи пользователей, с которыми работает сервер.

2.2 Функциональная схема программы службы технической поддержки

Функциональная схема программы службы технической поддержки электронной библиотеки приведе-

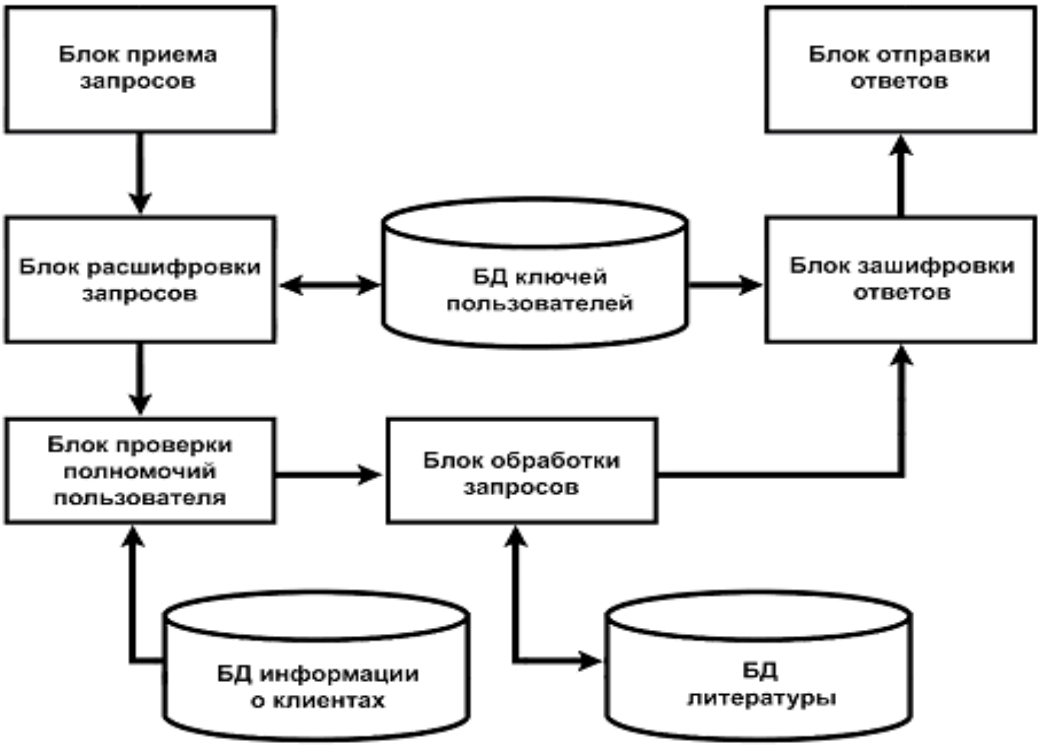

Рис.1. Функциональная схема сервера библиотеки.

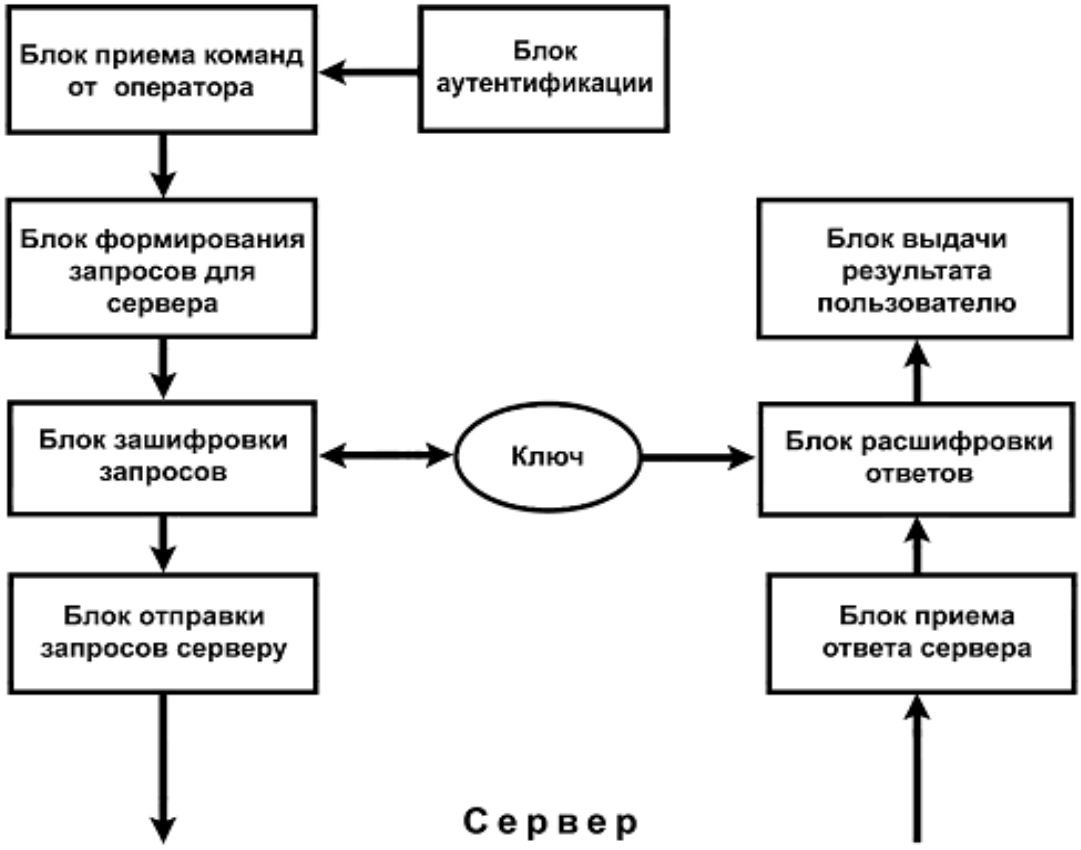

Рис.2. Функциональная схема клиентской программы электронной библиотеки.

на на рис.2.

Функции службы технической поддержки этой электронной библиотеки включают:

- присвоение читателям уровня допуска в соответствии с их подтвержденными полномочиями;
- добавление новых электронных документов в базу данных библиотеки.

Функции отдельных блоков программы службы технической поддержки:

Блок аутентификации производит аутентификацию работника библиотеки.

Блок приема команд предоставляет удобный интерфейс для работы с карточками читателей.

Блок формирования запросов для сервера согласно полученным командам оператора формирует запрос для сервера.

Блок зашифровки запросов шифрует сформированный запрос с помощью открытого ключа сервера или установленного общего симметричного ключа.

Блок отправки запросов серверу отправляет зашифрованные запросы.

Блок приема ответов сервера получает ответы от сервера.

Блок расшифровки ответов расшифровывает полученные ответы с помощью установленного общего симметричного ключа.

Блок выдачи результата оператору выдает полученный от сервера ответ в удобочитаемой форме.

2.3 Функциональная схема программы читателя библиотеки

Функции программы читателя этой библиотеки включают:

- выбор клиентом пароля для шифрования хранимого в программе клиента симметричного ключа;
- открытие карточки читателя на сервере;
- подачу запроса для установления уровня допуска читателя;
- получение информации о литературе, имеющейся в фонде;
- заказ и получение запрошенной литературы;

Функции отдельных блоков программы читателя идентичны функциям аналогичных блоков программы службы технической поддержки.

Так как обмен всеми сообщениями между этими программами, являющимися элементами распределенной системы «спецхран» должен производиться после предварительного шифрования этих сообщений, а хранение информации о карточках читателей и выполненных по их командам или поручениям операциям в защищенной базе данных, каждая из программ должна снабжаться собственным блоком шифровки/расшифровки передаваемой и получаемой информации.

3. Функциональные возможности программы

Разработанная для электронной библиотеки ограниченного доступа программа (рис.3) обеспечивает выполнение следующих операций [2]:

- создание карточки читателя;
- передачу информации о читателях в службу технической поддержки;
- запрос читателем необходимого уровня допуска;
- разрешение читателю обоснованного ним уровня допуска;
- поиск литературы в каталоге библиотеки по ее входным данным;
- получение читателем списка имеющейся в каталоге разрешенной ему для чтения литературы;
- заказ и получение литературы;

Программа выполняет автоматическое шифрование сообщений между элементами распределенной системы – электронной библиотеки, имеет инсталлятор и деинсталлятор программы клиента, развитую систему технических сообщений, обеспечивающих пользователя информацией и подсказками в процессе его работы.

4. Диаграммы классов программы

Диаграмма классов серверной программы электронной библиотеки представлена на рис.4.

Класс *ServerInterface* предоставляет несколько методов для обращения к серверу с запросами.

Метод Query() вызывает метод Query() объекта класса *ServerQueryManager*, который выполняет запрос, при необходимости обращаясь к объекту класса *DbAccess*, обеспечивающему доступ к информации, хранимой в базе данных.

Метод CryptQuery() вызывает метод Query() объекта класса *CryptQueryManager*, который расшифровывает запрос и передает его объекту класса *ServerQueryManager* для обработки, после чего результат шифруется и отправляется клиенту.

На рис.5 представлена диаграмма классов клиентской программы читателя.

Для входа в программу читателю необходимо ввести пароль, с помощью которого шифруется его симметричный ключ (*AuthentificationForm*).

Клиенту предоставляются интерфейсы для поиска документов (*SearchForm*) и для отправления запроса на изменение уровня допуска (*ChangeLevel Form*). Команды читателя поступают объекту класса *ReaderClientQueryManager*, наследующемуся от класса *ClientQueryManager* который формирует запросы для сервера и шифрует их. После этого вызываются методы класса *ClientInterface*, которые в свою очередь выполняют вызов соответствующих серверных методов.

Для скачивания документа после того как он был найден вызывается метод AskDownload, который да-

Рис.3. Функциональная схема электронной библиотеки.

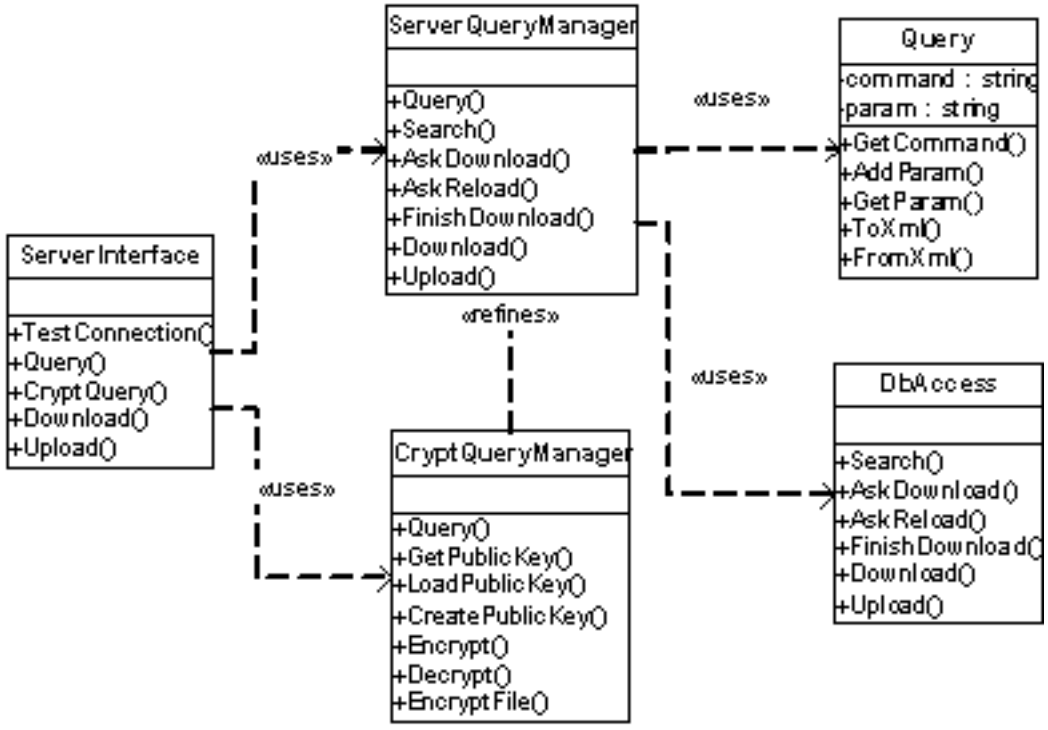

Рис.4. Диаграмма классов сервера

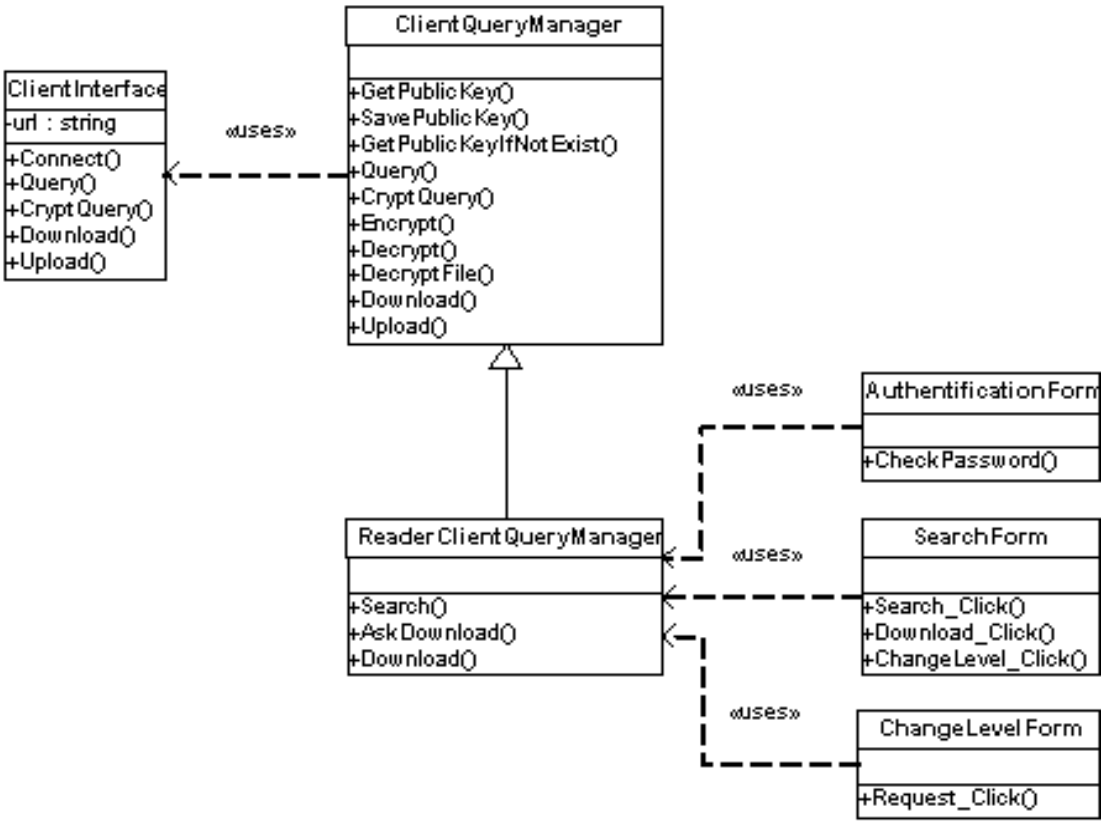

Рис.5. Диаграмма классов клиентской программы читателя.

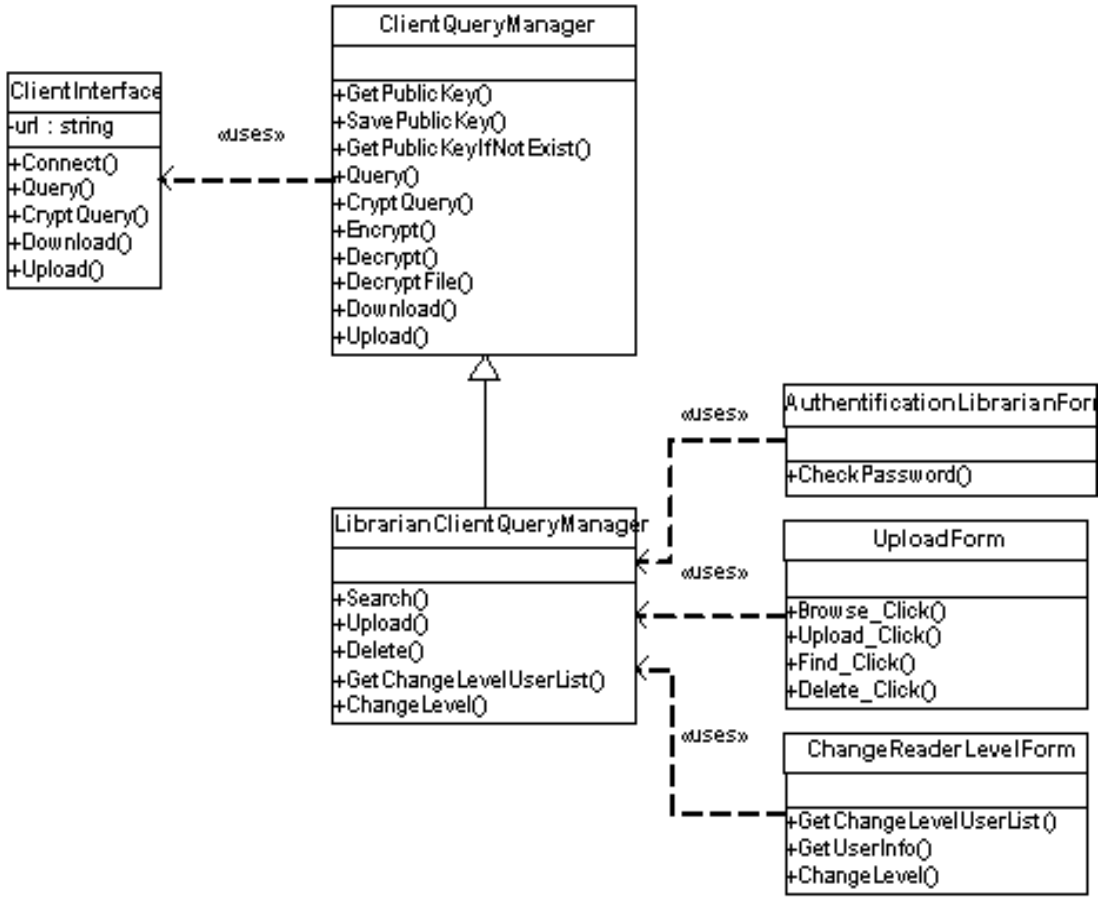

Рис.6. Диаграмма классов клиентской программы оператора библиотеки

ет команду серверу подготовить документ к скачиванию. При этом документ шифруется ключом читателя и размещается в базе данных. После этого клиентская программа вызывает метод Download для его скачивания.

Такая организация процесса позволяет обеспечивать докачку документов в случае, если его не удалось передать полностью с первого раза.

На рис.6 представлена диаграмма классов клиентской программы библиотекаря. Интерфейс *Change ReaderLevelForm* предназначен для изменения уровня допуска читателя, а *UploadForm* для загрузки документов в базу данных библиотеки.

5. Диаграммы последовательности действий

Для изменения уровня допуска (рис.7) читатель должен послать запрос с указанием своих имени, фамилии, места работы, телефона и контрольной фразы. Этот запрос поступает библиотекарю, который решает, можно ли установить соответствующий уровень допуска, при необходимости пригласив читателя в библиотеку для предоставления документов, подтверждающих его личность и право на соответствующий уровень допуска.

Для получения информации (рис.8) читатель сначала производит предварительный поиск, чтобы найти ее в каталоге. Поиск может проводиться по автору документа и/или заглавию. Выбрав документ, читатель посылает запрос на его скачивание с указанием присвоенного документу идентификатора. Сервер выбирает документ, шифрует его ключом приславшего запрос читателя и присваивает идентификатор скачивания.

Затем сервер отправляет сведения о документе (размер, имя файла) и идентификатор скачивания.

Теперь программа читателя может загрузить любую часть этого документа. Такая организация процесса позволяет достаточно легко организовать докачку документа в случае обрыва связи. Когда документ полностью скачан, программа клиента отправляет серверу сообщение о том, что документ успешно загружен. Сервер удаляет из базы данных зашифрованную для этого читателя копию документа.

6. Структура базы данных для хранения литературы

На рис.9 приведена схема базы данных для фонда специального хранения литературы [3]. В таблице Description хранится идентификатор документа и некоторая информация о нем. В отдельные таблицы выделены заглавия (Title), которых у документа может быть несколько, авторы (Liability) и раздел (Part). LiabilityType содержит тип ответственности (автор, редактор, переводчик, рецензент и т.п.)

При поступлении запроса на скачивание документа он шифруется симметричным ключом читателя, приславшего запрос, и размещается в таблице Temp.

7. Описание пользовательского интерфейса

Пользовательский интерфейс читателя включает в себя два окна: окно для заказа и получения литературы и окно формирования запроса на установку уровня доступа пользователя.

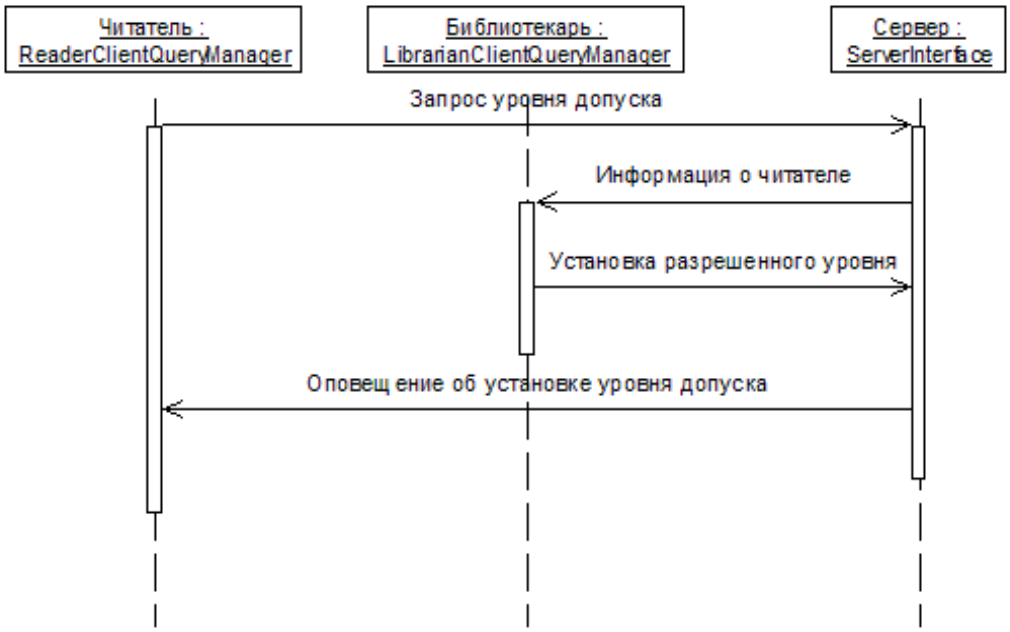

Рис.7. Диаграмма последовательности действий для изменения уровня допуска читателя

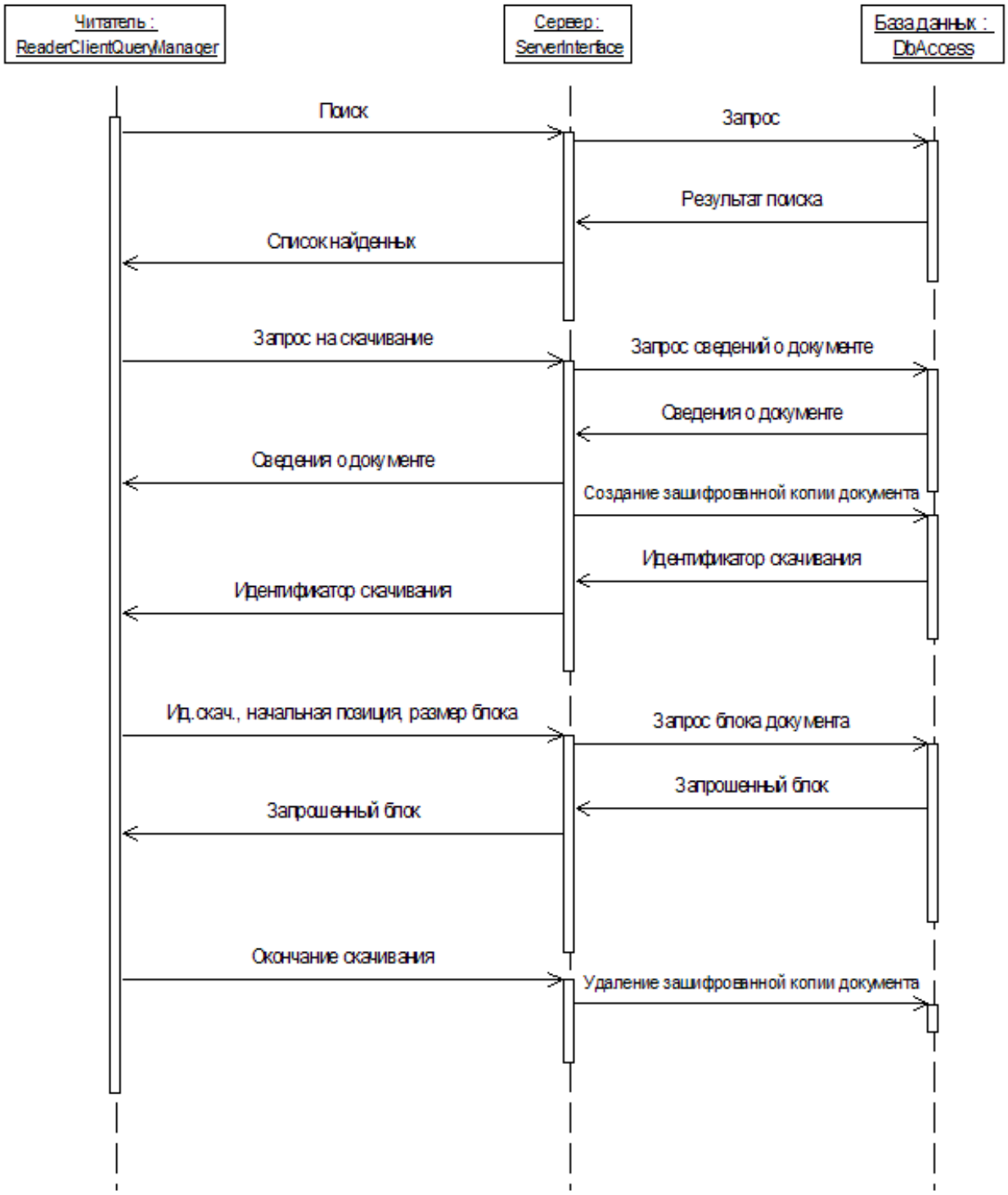

Рис.8. Диаграмма последовательности действий при скачивании документа

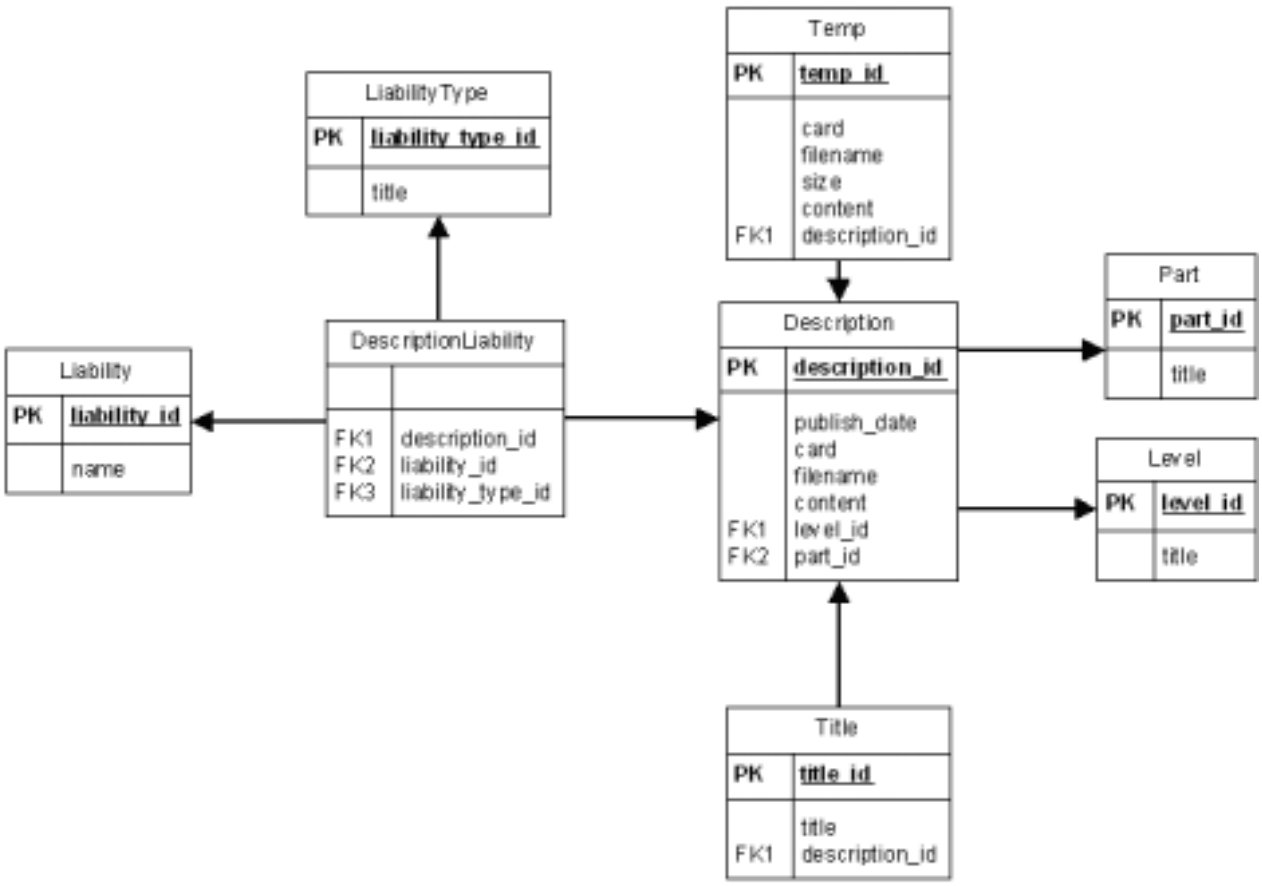

Рис.9. Схема базы данных литературы

Окно для заказа и получения литературы включает в себя три кнопки (для начала поиска интересующей читателя литературы в каталоге библиотеки, для скачивания выбранных читателем источников и для запроса на изменение уровня допуска к закрытым источникам), три поля для ввода идентифицирующей разыскиваемую литературу информации и окно для вывода списков найденных источников.

Окно формирования запроса на установку уровня доступа пользователя включает в себя пять полей для ввода идентифицирующей читателя информации, три переключателя для установки запрашиваемого уровня допуска читателя и одну кнопку для отправки запроса на изменение уровня допуска.

Пользовательский интерфейс библиотекаря также включает в себя окно установки уровня допуска пользователей.

Окно установки уровня доступа пользователя включает в себя список для выбора обрабатываемого запроса, две кнопки (для установки запрошенного уровня допуска, либо для удаления запроса без изменения уровня допуска), пять полей для вывода идентифицирующей читателя информации и одно поле для вывода запрашиваемого уровня допуска, который при необходимости можно изменить.

8. Технические характеристики программы

Серверная часть программы занимает 1178 Кб и работает в операционной системе Windows 2000 Server на платформе .NET Framework. Клиентская часть программы занимает 1220 Кб и может работать в операционных системах Windows 98/Me/2000/XP на платформе .NET Framework [4].

Проведенные испытания показали, что работа программы полностью удовлетворят установленным техническим требованиям.

9. Дополнительные возможности программы

Кроме применения по прямому назначению программа может быть использована для быстрого распространения конфиденциальной информации между пользователями электронной библиотеки и организации защищенного обмена сообщениями между ними [5-8]. Использование библиотечного сервера для хранения базы данных открытых ключей (рис.10) позволяет формировать связанные между собой группы пользователей ограниченного круга как в ло-

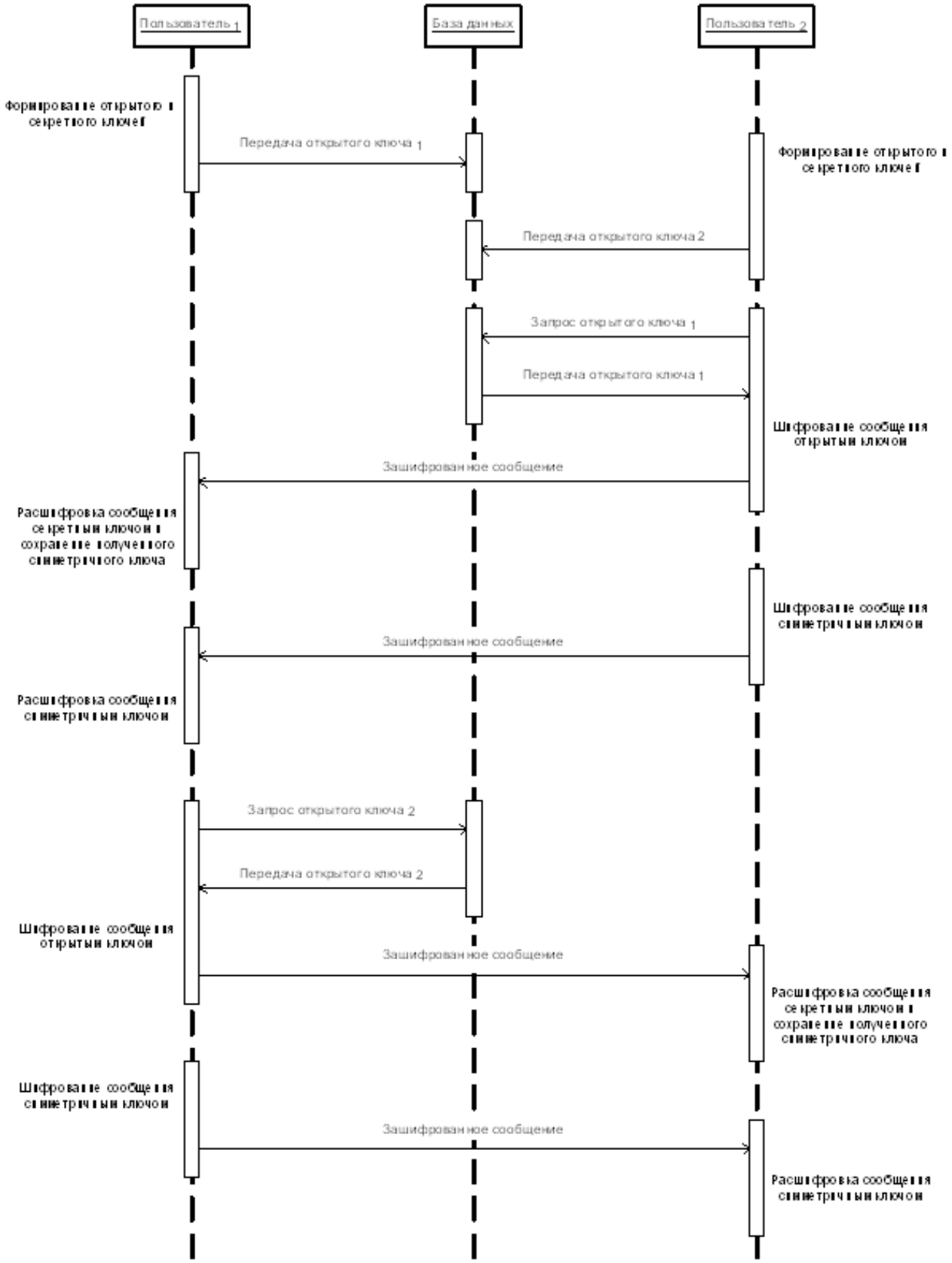

Рис. 10. Установка связи между пользователями программы

кальных сетях, так и в сети интернет.

При создании учетной записи пользователя автоматически начинают генерироваться для него пара открытого и секретного ключей. После того, как они сгенерированы, открытый ключ размещается в удаленной базе данных и становится доступным для любого пользователя, желающего зашифровать с его помощью сообщение. Во время подготовки сообщения для пересылки (при введении адреса получателя, идентифицирующего его) открытый ключ получателя автоматически скачивается из удаленной базы данных и используется для шифрования текста сообщения. Таким образом, работа с данной программой для пользователя очень похожа на работу с обыкновенным почтовым клиентом, однако позволяет в автоматическом режиме шифровать всю переписку.

Кроме того, программа дает возможность организовать защиту от несанкционированной массовой рассылки. Выставляя требование обязательного шифрования каждого входящего сообщения открытым ключом получателя, программа может автоматически удалять все незашифрованные сообщения. Шифрование же при массовой рассылке сообщения для каждого получателя в отдельности делает ее экономически невыгодной из-за чрезмерно высоких временных затрат, однако при этом обеспечивается возможность санкционированной массовой рассылки путем использования «белых списков».

Программа также обеспечивает возможность шифрования передаваемой информации с помощью заранее установленного пароля.

Для хранения секретных ключей и паролей программа предоставляет возможность их шифрования в локальной базе данных с помощью личного пароля пользователя.

Литература:

[1] Кузнецов А.А. Способ защиты информации, документов или ценных объектов. Патент России №2182211 от 10.05.2002г.

[2] Кузнецов А.А. Создание распределенной электронной библиотеки как средство обеспечения сохранности научно-технической информации. Тезисы докладов седьмой международной научной конференции «Библиотечное дело-2002», М., 2002г. с.201-202.

[3] Кузнецов А.А. Комплексная система защиты при доставке информации пользователям электронных библиотек. Труды IV Всероссийской научной конференции «Электронные библиотеки: Перспективные методы и технологии, электронные коллекции», т.2, с.319-324, г.Дубна, 2002г.

[4] Кузнецов А.А. Электронная библиотека для обслуживания читателей с различным уровнем доступа. Свидетельство об официальной регистрации программы для ЭВМ №2004610722 от 19.03.2004г.

[5] Кузнецов А.А. Особенности структуры активных ключей в двухключевой криптосистеме. Тезисы докладов XI Всероссийской конференции "Методы и технические средства обеспечения безопасности информации", СПб, 2003г., с.89-90.

[6] Кузнецов А.А. Способ защиты информации. Патент России №2211483 от 27.08.2003 г.

[7] Кузнецов А.А. Программа для защищенного обмена информацией в открытых сетях. Свидетельство об официальной регистрации программы для ЭВМ №2003611895 от 14.08.2003г.

[8] Кузнецов А.А. Программа для скрытого распределения информации в открытых сетях. Свидетельство об официальной регистрации программы для ЭВМ №2003611895 от 12.01.2004г.

Provision of the Secure Information Exchange for the Limited Access Fund of Electronic Library

Kuznetsov A.A.

The electronic library, providing different access levels for users and secure delivery of documents, is considered in this work.