УДК 004.932.4

# ПРОГРАММНАЯ СИСТЕМА ЗАЩИТЫ ИНФОРМАЦИИ ДЛЯ ПРЕДПРИЯТИЯ

***Палади С.И., Чернышова А.В.***
*Донецкий национальный технический университет*
*Кафедра прикладной математики и информатики*
*E-mail: paladisergey@mail.ru*

***Аннотация***

***Палади С.И., Чернышова А.В. Программная система защиты информации для предприятия.*** *Рассматривается программная система защиты информации для предприятия, реализованная средствами Visual C++ и с поддержкой базы данных, реализованной на базе Microsoft SQL Server 2008. Также в системе реализованы методы защиты информации, а в частности: алгоритм шифрования данных AES, протокол сетевой аутентификации Kerberos, алгоритм подсчета контрольной суммы CRC32 и алгоритмы хеш-функций SHA-256 и MD5.*

***Общая постановка проблемы.*** Неизбежность и целесообразность использования информационных технологий и глобальных коммуникаций влечет за собой неотвратимость угроз информационной безопасности. Любой человек, ведомство, страна и мировое сообщество сталкивается с этими угрозами ежедневно. Потеря или повреждение информации в следствии проникновения вируса, попадание конфиденциальной информации в руки конкурентов, злоумышленников может повлечь за собой большие проблемы.

***Постановка задач исследования.*** Существует множество систем защиты информации, но, учитывая факт актуальности темы защиты информации, необходимо разрабатывать новые и усовершенствовать имеющиеся проекты. Среди главных задач исследования в данной работе рассматриваются методы безопасной аутентификации, шифрования данных, методы, позволяющие безопасно хранить и передавать информацию пользователям относительно их прав доступа.

***Решение задачи и результаты исследований.*** Администратор производит запуск сервера, после чего сервер находится в режиме ожидания подключения клиентов. После чего клиентские машины имеют возможность подключения к серверу. Для клиента, который успешно прошел процедуру аутентификации, сервер формирует структурированный список доступной для него информации. Список формируется с учетом прав клиента. Когда клиент имеет в распоряжении список доступной информации, появляется возможность работать. Работа с информацией ограничена правами клиента. Пользователь сотрудничает только с сервером и все запросы отправляет на сервер. Сервер обрабатывает запросы, и если права клиента позволяют получить запрошенную информацию из базы, сервер отправляет клиенту запрошенную информацию в зашифрованном виде.

Также предоставлена функциональность для защиты информации, хранящейся в базе данных, путем шифрования и хранения зашифрованных файлов. К файлам, которые, по мнению администратора, имеют высокую степень конфиденциальности, можно применить функцию шифрования и хранить в базе зашифрованную версию этого файла.

Реализован алгоритм контроля целостности базы данных в целом. При каждом запуске сервера в фоновом режиме будет происходить последовательная проверка целостности всей информации из базы данных. Это реализовано с помощью алгоритма подсчета контрольной суммы CRC32. Перед тем как добавить файл в базу данных, для него

происходит подсчет контрольной суммы, после чего данные о файле и контрольная сумма заносятся в базу. При дальнейших проверках целостности файлов вновь посчитанная сумма сравнивается с суммой, сохраненной в базе, если они равны, алгоритм делает вывод, что целостность файла не была нарушена. При изменении файла происходит пересчет контрольной суммы и замена старого значения непосредственно в базе данных.

Все действия сервера и клиентов фиксируются подсистемой регистрации и учета и выводятся в режиме реального времени.

Для решения задачи, обеспечивающей максимальную защиту при передаче информации, были проанализированы некоторые алгоритмы шифрования. После чего выбор был сделан в пользу алгоритма AES (Rijndael). AES – симметричный алгоритм блочного шифрования (алгоритм принят в качестве стандарта шифрования правительством США по результатам конкурса AES). Этот алгоритм хорошо проанализирован и сейчас широко используется (по состоянию на 2006 год AES является одним из самых распространённых алгоритмов симметричного шифрования). На рисунке 1 показана подробная схема разработанной системы защиты информации. Также на рисунке показано, что перед отправкой любых данных по сети Server и User обращаются к модулю «Функция шифрования информации». Этот модуль шифрует информацию, которая подается на его вход.

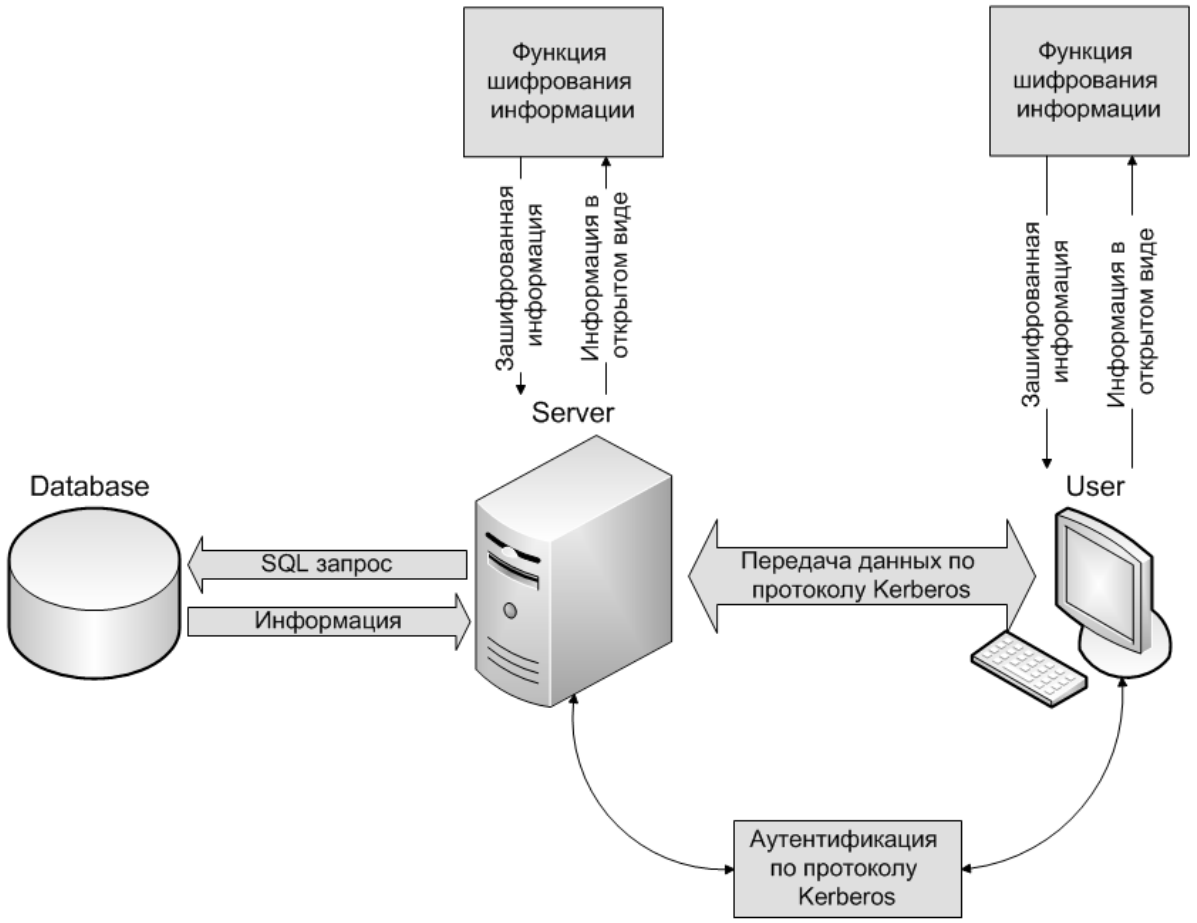


Рисунок 1 – Подробная схема разработанной СЗИ

При выборе протокола аутентификации и безопасной передачи данных по незащищенным сетям был выбран протокол Kerberos. Организация протокола направлена в первую очередь на клиент-серверную модель и обеспечивает взаимную аутентификацию — оба пользователя через сервер подтверждают личности друг друга. Сообщения, отправляемые через протокол Kerberos, защищены от прослушивания и атак. Kerberos

основан на симметричной криптосистеме и требует третье доверенное лицо (сервер). Расширение Kerberos позволяет использовать открытые ключи в процессе аутентификации.

В разработанной системе защиты информации реализован алгоритм, позволяющий контролировать целостность информации. Алгоритм реализован на основе двух алгоритмов хеш-функций SHA-256, MD5 и алгоритма подсчета контрольной суммы CRC32. На рисунке 2 показан путь преобразования пароля с использованием вышеперечисленных функций. Пароль пользователя подается на вход функции SHA-256. Функция возвращает хеш-строку, после чего она идет на вход функции MD5. Последним этапом преобразования является действие, когда результат функции MD5 поступает на вход функции CRC32. В итоге функция CRC32 возвращает конечное состояние пароля.

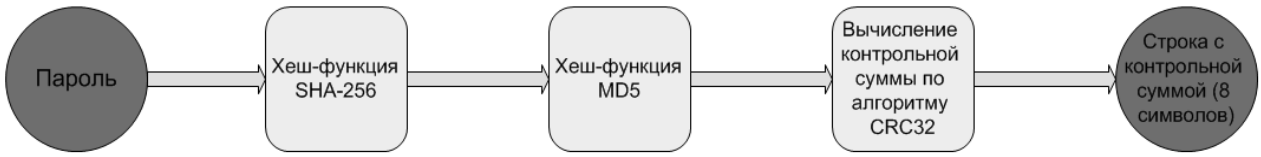


Рисунок 2 – Путь преобразования пароля

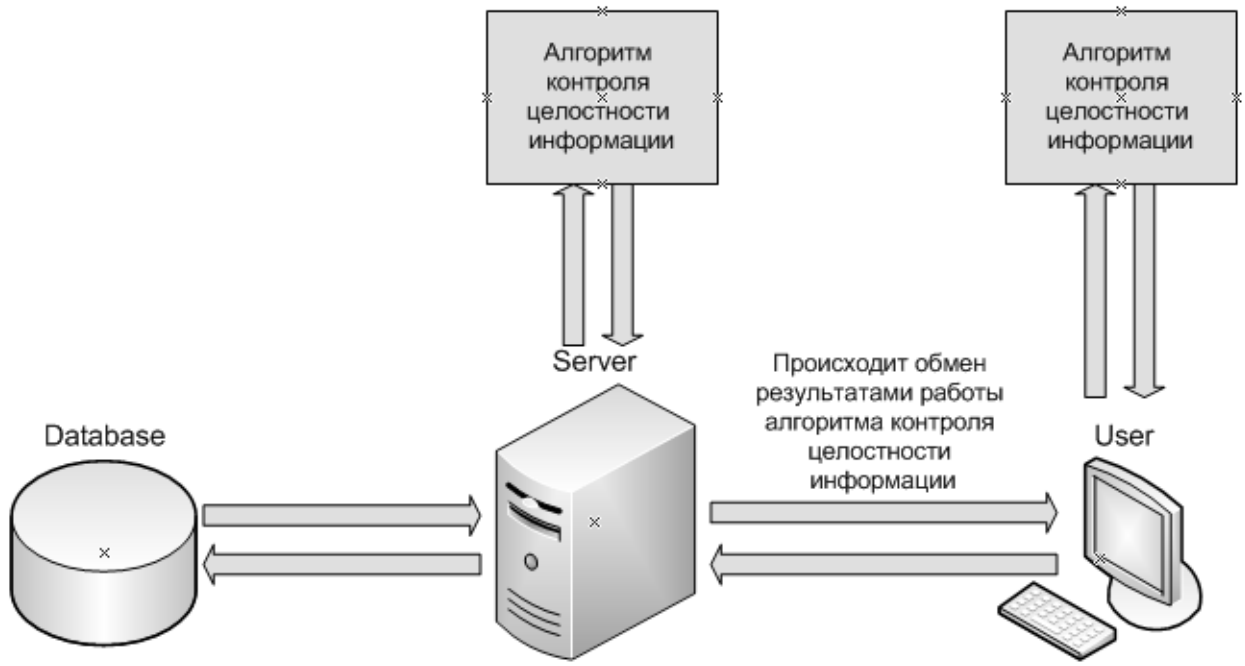


Рисунок 3 – Применение алгоритма контроля целостности информации

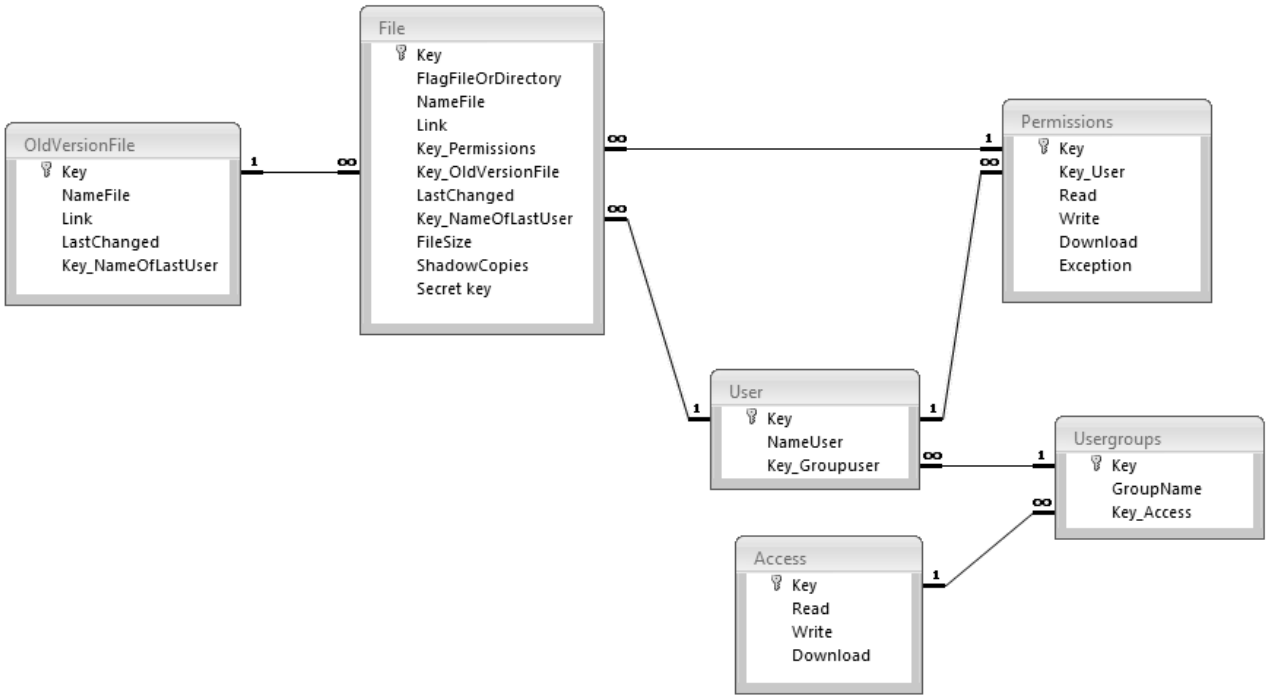


Рисунок 4 – Схема базы данных приложения

Схема базы данных, приведенная на рисунке 4, используется в разработанной системе защиты информации. Как видно из рисунка база данных состоит из 6 связанных между собой таблиц. Ключевой, в базе данных является таблица File. Таблица File хранит информацию о файлах, которые доступны клиентам. В каждой таблице уникальность записей обеспечивает поле Key с целочисленным типом данных. Таблица File не хранит непосредственно файлы. Для доступа к файлам в таблице предусмотрено поле Link, которое хранит ссылку на файл, который может быть расположен в любом месте как на жестком диске, сменном носителе так и быть доступным по сети.

Каждый пользователь, зарегистрированный в базе данных, состоит в одной из имеющихся групп. Каждая группа уникальна своими правами доступа к файлам. Каждый файл может иметь собственные права доступа для каждого пользователя и для этого предусмотрена таблица Permissions. Таблица разработана для того, чтобы придать приложению большей гибкости в управлении доступом к файлам. Таблица содержит поле Exception логического типа и в случае если состояние поля истинно необходимо для пользователя указанного в поле Key_User использовать права доступа указанные полями Read, Write, Download.

Поле ShadowCopies таблицы File логического типа и предназначено для файлов, которые представляют особую важность. Если значение поля ShadowCopies истинно для такого файла создается теневая копия файла. При потере или повреждении файла можно воспользоваться возможность восстановления файла из резервного хранилища.

Таблица File содержит информацию о последнем пользователе, который модифицировал данный файл и дату последней модификации.

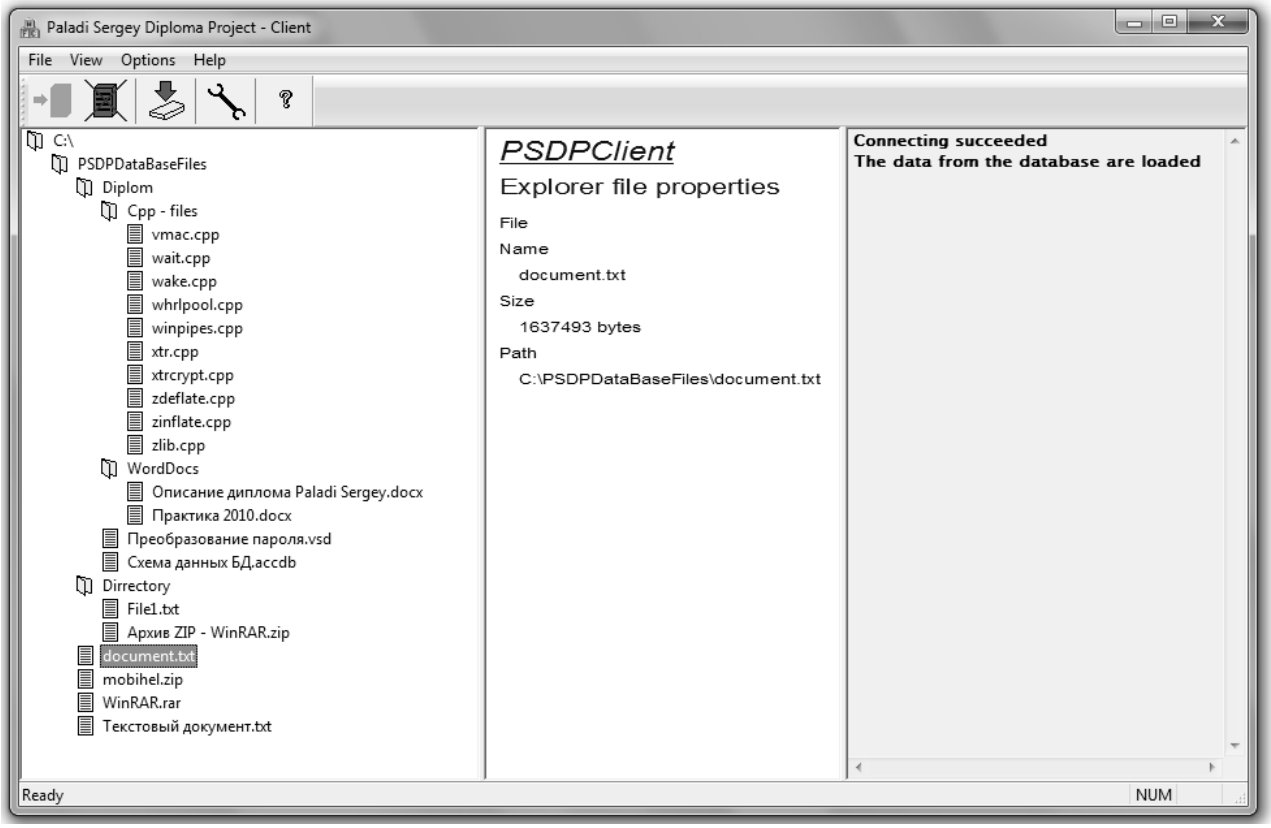


Рисунок 5 – Главное окно приложения клиент системы защиты информации

***Выводы.*** Развитие информационных технологий на сегодняшний день имеет высокие темпы развития. Разработку систем защиты информации необходимо вести с большим приоритетом по сравнению с многими другими направлениями. Имеющиеся системы защиты информации нуждаются в постоянном обновлении и усовершенствовании их методов и алгоритмов. Разработанная система не предоставляет полную безопасность информации на всех этапах работы приложения и существования самой информации. Среди преимуществ разработанной системы защиты информации можно выделить простоту реализации, использования и внедрения. Приложение имеет всю функциональность, необходимую для качественной и безопасной передачи данных между клиентом и сервером, а также для защиты от несанкционированного чтения.

## Список литературы

1. Щербаков Л.Ю., Домашев А.В. Прикладная криптография. Использование и синтез криптографических интерфейсов. – М.: Издательско-торговый дом «Русская редакция», 2003. – 416 с.: ил.

2. Саломаа А. Криптография с открытым ключом: Пер: с англ. – М.: Мир, 1995. – 318 с., ил.

3. Бармен, Скотт. Разработка правил информационной безопасности.: Пер. с англ. – М.: Издательский дом «Вильяме», 2002. – 208 е.: ил. – Парал. тит. англ.

4. Баричев С. Г., Гончаров В. В., Серов Р. Е. Основы современной криптографии. Учебное пособие: Учебное пособие для вузов. - М.: Горячая линия-Телеком, 2002. - 175 с.: ил.

5. Блэк У. Интернет: протоколы безопасности. Учебный курс Спб.: Питер, 2001. - 288 с.