Кравченко А.Г.
Научный руководитель – доцент каф. ФПМ МИВлГУ, к.т.н., А.В. Астафьев
Муромский институт (филиал) федерального государственного образовательного учреждения высшего образования «Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых»
602264, г. Муром, Владимирская обл., ул. Орловская, 23
email: Alexandr.Astafiev@mail.ru

Разработка клиент-серверного приложения для защищенной передачи информации

В современном мире информация стала одним из основных продуктов производства. Для того, чтобы повысить оперативность доставки информации от производителя к потребителю были разработаны принципы построения систем электронного документооборота. С точки зрения информационной безопасности к информации, передаваемой по открытым каналам связи, применяются следующие требования сохранения конфиденциальности и целостности. Разработка клиент-серверного приложения для защищенной передачи информации направлена на решение этих задач.

Целью работы является разработка клиент-серверного приложения для защищенной передачи информации для обеспечения конфиденциальности и целостности передаваемой по открытым каналам связи информации.

Для организации связи двух программных приложений предлагается использования технологию сетевых программных интерфейсов – сокетов. Взаимодействие клиентских и серверного приложений будет производиться с помощью стека протоколов TCP/IP. Для адресации используются IP-адреса протокола IPv4 и номер порта. Пара значений IP-адреса и номера порта определяет сокет.

Для организации конфиденциальности передаваемых данных прилагается использовать асимметричный алгоритм шифрования RSA [1]. Использование алгоритма RSA предполагает генерацию двух ключей шифрования: открытого и закрытого. Генерация ключей производится на стороне сервера. Открытый ключ передается клиенту для шифрования данных, а закрыты – остаётся на сервере для организации расшифровки полученных данных. Использование асимметричного алгоритма даёт большое преимущество в том, что открытый ключ можно передавать по открытому каналу связи. В случае использования симметричных алгоритмов ключ шифрования необходимо передавать только через доверенную среду.

Структурная схема работы системы представлена на рисунке 1.

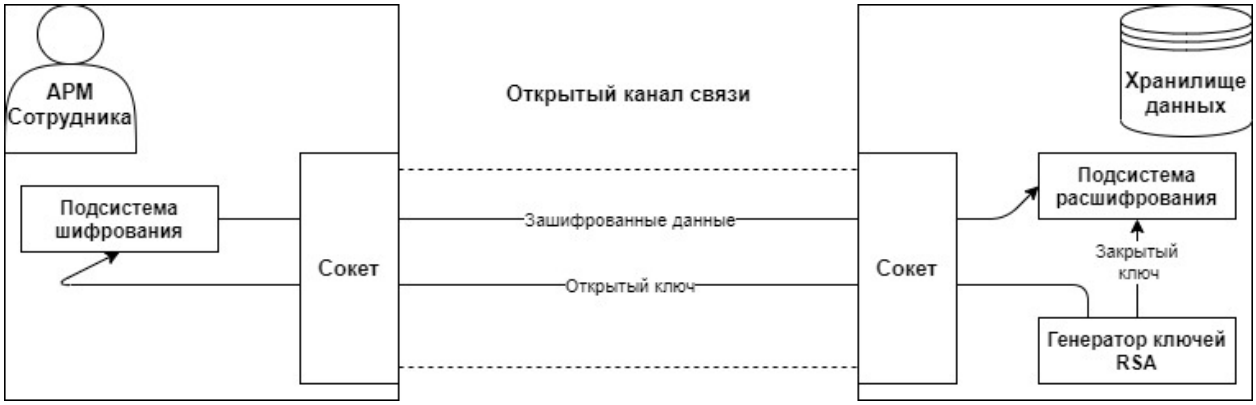

Рисунок 1 – структурная схема работы клиент-серверного приложения для защищенной передачи информации

Литература

1. Astafiev, A.V. Data exchange technology based on handshake protocol for industrial automation system / A.V. Astafiev, T.O. Shardin // Journal of Physics: Conference Series, Volume 1015, Issue 4.