УДК 004.415.25

РАЗРАБОТКА МОДУЛЯ ШИФРОВАНИЯ СЕТЕВОГО ТРАФИКА НА ОСНОВЕ ПРОГРАММИРУЕМОЙ ЛОГИЧЕСКОЙ ИНТЕГРАЛЬНОЙ СХЕМЫ

Волков А. Г. (федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет ИТМО»**),**
Научный руководитель – к. т. н., ассистент Попов И. Ю. (федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет ИТМО»**)**
Консультант – научный сотрудник лаборатории криптографических средств защиты информации Калабишка М.М. (федеральное государственное автономное образовательное учреждение высшего образования «Национальный исследовательский университет ИТМО»**)**

Аннотация. Ввиду повсеместного использования сетевых технологий и встающего более остро вопроса о конфиденциальности передаваемых данных, в данной работе предлагается программный модуль шифрования сетевого трафика, использующий вычислительные ресурсы программируемой интегральной логической схемы (ПЛИС).

Введение. Обеспечение защищённой передачи данных требует применение специальных устройств – криптошлюзов, стоимость которых крайне высока. Предложения, которые есть в данный момент на рынке, могут стоить до нескольких десятков миллионов рублей за экземпляр. На данный момент, ни на зарубежном, ни на отечественном рынке не наблюдается каких-либо тенденций, относительно повышения доступности данных устройств малому бизнесу и частным предпринимателям.

Основная часть. В данной работе предлагается программный метод зашифрованного соединения между двумя узлами основанный на аппаратном комплексе, состоящим из автоматической системы управления и ПЛИС, для каждого из которых в качестве сетевой платы будет использоваться ПЛИС, в данном случае, ПЛИС будет исполнять функции сетевой платы с возможностью шифрования передаваемой информации.

Таким образом вычислительные ресурсы, которые были бы необходимы для реализации шифрования передаваемой информации, если мы говорим о программном модуле, основанном только на платформе автоматической системы управления, будут освобождены для возможности реализации других задач. Помимо этого, если сравнивать данное решение с криптографическими шлюзами, функции которого я и реализую с помощью ПЛИС в данной работе, предложенный метод является экономически выгоднее, чем приобретение новых криптографических шлюзов.

Выводы. По результатам данного исследования, можно говорить о том, что в специфичной ситуации данное устройство может использоваться непосредственно для защищенной передачи данных.

Волков А. Г. (автор) Подпись

Калабишка М. М. (Консультант) Подпись

Попов И. Ю. (научный руководитель) Подпись