

## ОТЗЫВ

на автореферат диссертации Мукимова Жамшидбека Дамировича на тему: «Разработка протоколов для криптографической защиты информации в каналах цифровых систем передачи», представленную на соискание ученой степени кандидата технических наук по специальности 05.12.13 – «Системы, сети и устройства телекоммуникаций, распределение информации»

Важность и актуальность вопросов защиты информации уже давно вышли на одно из первых мест среди других задач, решаемых в процессе проектирования, создания и использования современных информационно-коммуникационных систем. Причины такого повышенного внимания к этой проблеме вполне очевидны - от качества мер защиты информации напрямую зависит экономическая безопасность любой деятельности. При обеспечении защиты информации необходимо исходить из того, что информация - это ресурс, который, как и другие важные ресурсы, имеет определенную ценность для ведения деятельности, а значит, нуждается в надежной защите.

В связи с этими обстоятельствами непрерывно возрастают актуальность задач защиты информации во всех сферах деятельности: на государственной службе, в бизнесе, в научной деятельности и даже в личной жизни. Постоянное соперничество между методами и реализующих их средствами добывания и защиты информации привело к появлению на рынке такого разнообразия различных устройств и приборов в этой предметной области, что возникла проблема рационального выбора, и применения для конкретных условий методов защиты.

Среди методов защиты информации все больший вес объективно приобретает криптографическая защита информации, основанная на применении различных криптографических алгоритмов и протоколов. На основе этого можно отметить, что выбранная соискателем тема исследования является актуальной.

В качестве замечаний необходимо отметить следующее. В работе предлагается способ выполнения протокола аутентификации и

синхронизации с использованием битов b5 и b6 байта К3. Однако, что произойдет, если эти биты будут использованы оператором связи в каких-либо других целях. Также было бы хорошо, если бы в работе были рассмотрены проблемы распределения ключей шифрования, так как при применении симметричных криптографических алгоритмов одной из основных проблем является распределение криптографических ключей.

Указанные замечания не снижают общей ценности диссертационной работы. В целом работа удовлетворяет требованиям, предъявляемым к кандидатским диссертациям, а ее автор Мукимов Жамшидбек Дамирович заслуживает присуждения ему степени кандидата технических наук по специальности 05.12.13 – «Системы, сети и устройства телекоммуникаций, распределение информации».

Заведующий кафедрой систем коммутации и распределения информации  
СПбГУТ им. проф. М.А. Бонч-Бруевича,  
доктор технических наук, профессор

Б.С. Гольдштейн



ЗАВЕРЯЮ

Подпись Гольдштейна Б.С.

Нач. АКУ СПбГУТ

им. проф. М.А. Бонч-Бруевича

Н.Г. Осенний

«17» августа 2012 г.

