Отзыв

на диссертацию Бабуевой Александры Алексеевны «Свойства безопасности схем подписи вслепую на основе уравнений Шнорра и Эль-Гамаля» представленной на соискание ученой степени кандидата физико-математических наук по специальности 2.3.6 – Методы и системы защиты информации, информационная безопасность.

В соответствии с ГОСТ Р 7.0.11-2011 (параграф 3) диссертация является научно-квалификационной работой. Это подразумевает полноту проводимых рассуждений от определений к утверждениям. Кроме того, согласно п.5.5.1 «При использовании специфической терминологии в диссертации должен быть приведен список принятых терминов с соответствующими разъяснениями.»

Однако, термины «стойкость», «неподделываемость», «неотслеживаемость», в которых сформулированы основные положения, выносимые на защиту (см. Автореферат стр.10-11), используются в диссертации без строгих математических определений. Из контекста диссертации понятно, что эти термины применяются к схемам цифровой подписи вслепую, а «стойкость» является измеримой величиной. Однако, что именно автор включает в понятие «схемы цифровой подписи вслепую» остается без определения. В частности, автор не обоснованно исследует утечку информации о паре (сообщение, подпись) в отличие от утечки информации только о сообщении в других работах. Из текста стр.3,4 Автореферата, нестрого описывающего понятия «неподделываемости» и «неотслеживаемости», нельзя понять, что означает, что эти свойства нарушаются. В разделе «Обозначения, определения и общие сведения» на стр.21 диссертации указано: «Подробное описание алгоритмического подхода на основе экспериментатора, а также используемые в рамках него термины и обозначения приведены в работах [7, 22].»

Ссылка [7], это докторская диссертация научного руководителя диссертанта Смышляева С.В., генерального директора ООО «КриптоПро», в котором работает диссертант. В ней, в частности, говорится, что при анализе криптопродуктов иностранного происхождения, закладки, нарушающие деловую репутацию их производителей, учитывать не надо. Это противоречит положениям Указа Президента РФ №250, согласно которому «с 1 января 2025 г. Организациям критической информационной инфраструктуры запрещается использовать средства защиты информации, странами происхождения которых являются иностранные государства, совершающие в отношении Российской Федерации, российских юридических лиц и физических лиц недружественные действия». Однако в продуктах ООО «КриптоПро» используются американские алгоритмы шифрования (в том числе входящие в ПО Windows) и устаревшие российские стандарты (ГОСТ 28147-89), имеющие слабости относительно атак, опубликованных позже (дифференциальный криптоанализ) и более стойкие аналоги («Магма», «Кузнечик»). При этом ООО «КриптоПро» имеет около 250 текущих государственных контрактов по защите трафика госкорпораций (Казначейство РФ, Росреестр, МВД, ГАС Правосудие, ГЛОНАСС, РЖД,

Росавиация и др.). Все это делает крайне важным внимательное рассмотрение вопросов, связанных с доказательствами стойкости соответствующих крипто алгоритмов.

Использование рассмотренного в диссертации Бабуевой А.А. алгоритмического подхода на основе экспериментатора уже приводило к серьезным ошибкам. Так в диссертационной работе заместителя начальника отдела криптографических исследований компании «КриптоПро» Ахметзяновой Л.Р. была «доказана» стойкость схемы шифрования, содержащей закладку вида «backdoor». Эта ошибка, выявленная на предзащите, была частично исправлена. Однако Бабуева А.А. отказалась вносить исправления в свою диссертацию и включать строгие определения основных терминов. Поскольку данные термины в литературе используются с весьма разными определениями, это не позволяет определить суть проведённых исследований и оценить верность выводов её диссертации.

В цитируемых автором иностранных работах имеются соответствующие строгие определения, например с использованием машины Тьюринга (см. ссылку на стр.3 автореферата), а в работах сотрудников ООО «КриптоПро», использующих ту же терминологию без строгих определений, встречается множество ошибок как то: свойство части системы защиты информации выдается за свойство всей системы, необоснованно включаются избыточные свойства в так называемые «расширенные требования безопасности», свойства специфической реализации протокола выдаются за свойства стандартной (авторской) последовательности вычислений и пересылок. В результате возникает возможность по-разному интерпретировать полученные результаты, в том числе используя их вместе с другими определениями.

Считаю, что работа Бабуевой А.А. представленная на соискание степени кандидата физ.-мат. наук не соответствует государственному стандарту на структуру и правила оформления диссертации и автореферата (ГОСТ Р 7.0.11-2011) и должна быть отложена и отправлена на доработку.

д.ф.-м.н. проф. каф. Информационной безопасности ВМК МГУ 07.11.2015 Черепнев М.А.

Подпись Черепнева М.А. заверяю

ПОДПИСЬ ЗАВЕРЯЮ
Зав. канцелярией
И.С. Сихарулидзе
Подпись