Сведения о научном руководителе
по диссертации *Бабуевой Александры Алексеевны*
«*Свойства безопасности схем подписи вслепую на основе уравнений Шнорра и Эль-Гамаля***»**

Научный руководитель: Смышляев Станислав Витальевич
Ученая степень: доктор физико-математических наук
Ученое звание:
Основное место работы: ООО «КРИПТО-ПРО»
Должность: генеральный директор
Адрес: 127018, г. Москва, ул. Сущевский Вал, дом 18
Тел.: +7 (495) 995-48-20 доб. 226
E-mail: svs@cryptopro.ru
Второе место работы: кафедра информационной безопасности факультета вычислительной математики и кибернетики ФГБОУ ВО «Московский государственный университет имени М. В. Ломоносова»
Должность: математик
Адрес: 119991, Москва, ГСП-1, Ленинские горы, МГУ имени М.В. Ломоносова, 2-й учебный корпус

Список основных научных публикаций по специальности 2.3.6 – «Методы и системы защиты информации, информационная безопасность» за последние 5 лет:

1) L. R. Akhmetzyanova, E. K. Alekseev, A. A. Babueva, L. O. Nikiforova, S. V. Smyshlyaev, “IQRA: Incremental Quadratic Re-keying friendly Authentication scheme”, Математические вопроосы криптографии, 13:3 (2022), 5–35.
2) L. R. Akhmetzyanova, E. K. Alekseev, A. A. Babueva, S. V. Smyshlyaev, “On the (im)possibility of secure ElGamal blind signatures”, Математические вопросы криптографии, 14:2 (2023), 25–42.
3) L. R. Akhmetzyanova, E. K. Alekseev, A. A. Babueva, A. A. Bozhko, S. V. Smyshlyaev, “sMGM: parameterizable AEAD mode”, Математические вопросы криптографии, 14:2 (2023), 7–24.
4) Е. К. Алексеев, С. Н. Кяжин, С. В. Смышляев, “Атаки на протоколы аутентифицированной выработки общего ключа при навязывании будущих открытых эфемерных ключей”, Прикладная дискретная матеематика, 2024, № 66, 60–77.
5) Е. К. Алексеев, Л. Р. Ахметзянова, А. А. Бабуева, Л. О. Никифорова, С. В. Смышляев, “Двусторонняя схема подписи ГОСТ”, Математические вопросы криптографии, 15:2 (2024), 7–28.

Ученый секретарь
диссертационного совета МГУ.012.3,
А. В. Галатенко