ОТЗЫВ

на автореферат диссертации Биричевского Алексея Романовича «Методы защиты информации на основе псевдовероятностного преобразования для мобильных устройств телекоммуникационных систем», представленной к защите на соискание ученой степени кандидата технических наук по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность.

Решение задач информационной безопасности при использовании мобильных устройств информационно-телекоммуникационных систем является актуальным научно-техническим направлением исследований. Выполненное диссертационное исследование связано с данной продлемой, что определяет актуальность его тематики. Работа посвящена разработке новых методов защитных преобразований, методов аутентификации и хранения ключей на основе разработанных псевдовероятностных алгоритмов защиного пеобразования. На основе предложенных методов разработана универсальная мобильная операционная система с расширенной функциональностью по сравнению с известными аналогами.

Автореферат достаточно полно отражает цель, решаемые задачи, полученные результаты и защищаемые положения. В ходе исследования получены следующие новые научные результаты:

1. Разработан метод аутентификации пользователей, стойкий к принуждающим атакам;
2. Разработан метод защитного преобразования передаваемой по открытым каналам информации, стойкий к принуждающим атакам;
3. Разработан метод защиты программного обеспечения от дизассемблирования, отличающийся использованием псевдоверятностного шифрования.
4. Разработан метод защиты хранимой информации, стойкий к принуждающим атакам.

Практическая значимость работы заключается в расширении класса потенциальных атак, противодействие которым может быть обеспечено средствами защиты информации, встроенными в универсальную мобильную операционную систему.

Судя по автореферату результаты исследования прошли достаточную апробацию, однако имеются следующие недостатки.

1. Не приводятся численные значения производительности разработанных алгоритмов псевдовероятностного защитного преобразования.
2. В работе рассматривается применение стандарта ГОСТ 28147-89, хотя принят новый стандарт блочного шифрования ГОСТ Р 34.12-2015.

Отмеченные недостатки не являются принципиальными и можно сделать следующий вывод. Выполненное диссертационное исследование

является законченной научно-исследовательской работой, обладающей научной новизной и практической значимостью. Работа соответствует требованиям «Положения о присуждении ученых степеней» ВАК РФ, предъявляемым к кандидатским диссертациям, а её автор – Биричевский Алексей Романович заслуживает присуждения ученой степени кандидата технических наук по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность.

Заведующий кафедрой «Комплексное
обеспечение информационной
безопасности» ФГБОУ ВО «Госуд
университет морского и речного
флота имени адмирала С. О. Макар
Доктор технических наук, доцент С.С. Соколов

«25» сентября 2017 г.

Адрес: 198035, г. Санкт-Петербург, ул. Двинская, 5/7
Телефон: 8 (812) 748-96-92
E-mail: sokolovss@gun

Ученый секретарь Уче
ФГБОУ ВО «ГУМРФ
имени адмирала С.О. М
кандидат технических Н Ф. Пижурина