ОТЗЫВ

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

Диссертационная работа Биричевского Алексея Романовича посвящена расширению функциональности средств защиты информации мобильных устройств и обеспечению переносимости программных средств защиты на различные типы мобильных устройств. Основное внимание в работе уделено вопросам защиты от атак с принуждением, для чего предлагается использовать псевдовероятностные защитные преобразования.

В работе разработана архитектура универсальной мобильной операционной системы с алгоритмами защитных преобразований, что позволяет обеспечить вычислительную неразличимость по шифртексту от вероятностного защитного преобразования. Вынесенная автором на защиту методы аутентификации и защитных преобразований являются новыми и, несомненно, актуальными. Применение разработанных алгоритмов и методов позволяет обеспечить более высокий уровень защиты от атак принуждения.

Предложенные подходы имеют значительную теоретическую значимость как для задачи повышения защищенности пользователей мобильных устройств, так и для построения операционных систем мобильных устройств.

Практическая значимость работы подтверждается множеством публикаций и актами внедрения.

По содержанию автореферата можно сделать следующие замечания:

1. При вычислении временных паролей (стр.7) проводится применение операции XOR для парольной фразы и вектора инициализации, хотя они имеют различную длину.

2. При описании модели разработанной защищенной операционной системы для мобильных устройств рассмотрены методы защиты от статического и активного анализа, но не указано, как защитить данные аутентификации на стороне клиента.

3. Некоторая небрежность оформления, а именно, отдельные параметры формул не раскрываются, и их смысл можно извлечь только из контекста.

4. В работе присутствуют ссылки на использование алгоритма ГОСТ 28147-89, хотя в настоящее время используется более современный вариант (ГОСТ Р 34.12-2015).

Отмеченные недостатки не носят принципиального характера и не снижают оценки качества проведённого исследования.

Из автореферата следует, что результаты диссертационной работы отражены в 3-х статьях, опубликованных в рецензируемых научных журналах, а также в докладах на различных научно-практических конференциях.

Автореферат позволяет сделать вывод, что диссертационная работа Биричевского Алексея Романовича на тему «Методы защиты информации на основе псевдовероятностного преобразования для мобильных устройств телекоммуникационных систем» является законченной научно-квалификационной работой, удовлетворяет требованиям критериев «Положения о присуждении ученых степеней», предъявляемым к работам на соискание учёной степени кандидата технически наук, и соответствует паспорту специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность», а её автор заслуживает присуждения учёной степени кандидата технических наук.

Профессор кафедры ИБКС
ИКНТ ФГАОУ ВО «СПбПУ» Петр Дмитриевич
д.т.н., профессор, засл. деятель наук РФ Зегжда

« 20 » сентября 2017 г.

Федеральное государственное автономное образовательное учреждение высшего образования «Санкт-Петербургский политехнический университет Петра Великого» (ФГАОУ ВО «СПбПУ»)
195251, Санкт-Петербург,
ул. Политехническая, д.29
тел. (812) 552-76-32
e-mail kafedra@ibks.spbstu.ru