

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

Диссертация Биричевского Алексея Романовича посвящена разработке методов защиты информации для мобильных устройств телекоммуникационных систем. К таким устройствам относятся средства защиты информации (например, персональные аутентификаторы, ключи защиты программных продуктов). Описываемые устройства часто функционируют на базе операционных систем. Автором предлагается максимально интегрировать функции обеспечения информационной безопасности в операционную систему. Актуальность темы исследования заключается в снижении стоимости разработки таких мобильных устройств.

Научная новизна работы заключается в применении псевдовероятностного защитного преобразования в методах защиты мобильных операционных систем. К основным полученным в работе научным результатам относятся:

1. Метод аутентификации пользователей, отличающийся использованием одноразовых паролей, генерируемых с помощью алгебраического алгоритма псевдовероятностного защитного преобразования.
2. Метод защитного преобразования передаваемой по открытым каналам информации, отличающийся выполнением требования вычислительной неразличимости по шифртексту от вероятностного защитного преобразования.
3. Метод защиты программного обеспечения от дизассемблирования, отличающийся введением ложных веток кода с помощью псевдовероятностного защитного преобразования машинного кода.
4. Метод хранения ключей шифрования, отличающийся выполнением псевдовероятностного защитного преобразования ключей.

По сути изложенного в статье материала хотелось бы отметить следующее:

- работа имеет четкую, логически выверенную структуру;
- работа имеет высокую актуальность и практическую значимость;
- оценка качества рисунков, формул, схем, наглядности – высокая;
- оценка качества изложения, стиля и языка – высокая.

Практическая ценность работы состоит в возможности применения ее результатов в широком спектре мобильных устройств, в том числе в средствах защиты информации.

Для проведения экспериментальных испытаний методов защиты информации были разработаны макетные стенды, которые имитируют некоторые распространенные классы средств защиты информации.

Результаты диссертационной работы внедрены в учебный процесс кафедры информационной безопасности Института точных наук и информационных технологий Сыктывкарского государственного университета им. Питирима

Сорокина на старших курсах обучения студентов по специальности «090900 – Информационная безопасность».

По теме диссертации опубликовано 12 работ, в том числе 3 – в рецензируемых изданиях из перечня ВАК. Проведена апробация работы в конференциях различного уровня.

К недостаткам работы можно отнести недостаточно полное описание алгоритма аутентификации пользователей. Из представленного автореферата несколько сложно понять, каким образом был сгенерирован файл хранилища шифротекстов.

Указанное замечание не снижает ценности рассматриваемого диссертационного исследования. Работа имеет важное научное и практическое значение и удовлетворяет требованиям ВАК, предъявляемым к кандидатским диссертациям, а её автор – Биричевский А.Р. заслуживает присуждения ученой степени кандидата технических наук по специальности 05.13.19 – Методы и системы защиты информации, информационная безопасность.

К.ф.-м.н., доцент, доцент кафедры
информационной безопасности
Института точных наук и
информационных технологий
федерального государственного
бюджетного образовательного
учреждения высшего образования
«Сыктывкарский государственный
университет имени Питирима Сорокина»

Ю.В. Гольчевский

« 08 » сентября 2017 г.

Почтовый адрес: 167001, Республика Коми, г. Сыктывкар, Октябрьский пр., 55
Телефон: (8212) 390379
e-mail: yurag@syktsu.ru

Подпись Гольчевского Ю.В.
удостоверяю
Начальник ОК



О.П. Афанасьева