Отзыв официального оппонента
на диссертационную работу
Биричевского Алексея Романовича
«Методы защиты информации на основе псевдовероятностного преобразования для мобильных устройств телекоммуникационных систем»
по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность»
на соискание ученой степени кандидата технических наук

1. Актуальность выполненного исследования

Диссертация посвящена методам защиты информации в операционных системах (ОС) для мобильных устройств телекоммуникационных систем. В работе выполнен аналитический обзор известных методов защиты информации, применяемых в существующих защищенных мобильных операционных системах, на основе которого были выделены особенности реализации таких систем, открытые научно-технические проблемы, сформулированы цель и задачи исследования.

Актуальность темы исследования заключается в возможности снижения стоимости разработки средств и систем защиты информации за счет внедрения унифицированного подхода к обеспечению безопасности при разработке таких систем. Автором предлагается встраивать расширенные защитные функции средств защиты информации в универсальную мобильную операционную систему, на которой они будут функционировать, и разрабатываются методы реализации указанных функций, основанные на псевдовероятностных защитных преобразованиях.

2. Новизна исследования и полученных результатов, степень обоснованности научных положений, выводов и рекомендаций, сформулированных в диссертации

Научная новизна диссертационного исследования заключается в следующем:

1. разработан метод аутентификации пользователей, отличающийся использованием одноразовых паролей, генерируемых с помощью алгебраического алгоритма псевдовероятностного защитного преобразования;
2. разработан метод блочного защитного преобразования передаваемой по открытым каналам информации, отличающийся выполнением требования вычислительной неразличимости по шифртексту от вероятностного защитного преобразования;

3. разработан метод защиты программного обеспечения от дизассемблирования, отличающийся введением ложных веток кода с помощью псевдовероятностного защитного преобразования машинного кода;

4. разработан новый метод хранения ключей шифрования, отличающийся выполнением над ними псевдовероятностного защитного преобразования ключей.

Обоснованность представленных положений, выводов и рекомендаций обеспечивается корректным использованием выбранного математического аппарата, применением системного подхода к решению поставленных задач, и подтверждается экспериментом. Результаты диссертационной работы прошли достаточную апробацию, и использованы в учебном процессе Сыктывкарского государственного университета и в производственной организаций организации, специализирующейся в области разработки перспективных средств криптографической защиты информации (см. Приложение к диссертации).

3. Значимость для науки и практики результатов диссертации

Применение универсальной операционной системы в мобильных устройствах телекоммуникационных и информационных систем, в том числе в системах защиты информации, позволит унифицировать подходы к обеспечению безопасности при разработке таких систем. Данный подход значительно сократит расходы на разработку и производство мобильных устройств на схожих аппаратных платформах. Область применения ОС: аутентифицирующие устройства (токены, идентификаторы), системы охраны, устройства защиты программного обеспечения, персональные устройства хранения данных (защищенные файловые хранилища), аппаратные средства шифрования (криптопровайдеры).

Теоретическая значимость работы состоит в разработке архитектуры универсальной защищенной мобильной ОС и новых алгоритмов защитных преобразований информации, обеспечивающих вычислительную неразличимость по шифртексту от вероятностного защитного преобразования.

Практическая значимость этих результатов заключается в широком спектре мобильных устройств телекоммуникационных, в которых могут быть применены разработанные методы.

4. Оценка содержания диссертации

Диссертация состоит из введения, 4-х глав исследования, которые включают анализ текущего уровня исследования в данной области, выводов по каждой главе. Также в работе имеется заключение и список литературы,

включающий 112 отечественных и зарубежных источников. В работе представлено 7 таблиц и 38 рисунков.

Основные результаты диссертации представлены в 3 докладах на международных и 6 российских конференций. По теме диссертации опубликовано 3 статьи в журналах, рекомендованных ВАК Минобрнауки России.

Полученные автором в ходе исследования результаты могут быть использованы при разработке программно-аппаратных средств защиты информации.

Алгоритмы псевдовероятностного защитного преобразования, удовлетворяющие требованию вычислительной неразличимости от вероятностного шифрования; способы практического применения высокопроизводительных алгоритмов псевдовероятностного защитного преобразования в операционных системах могут быть использовать в учебном процессе на старших курсах обучения студентов по специальности «090900 – Информационная безопасность».

Из недостатков работы можно отметить следующие:

– в работе делается акцент на защиту от атак с принуждением, однако реализация атак данного типа на практике представляется достаточно редким случаем;

– вопросу всестороннего тестирования разработанного программного обеспечения не уделено достаточного внимания, хотя для программных продуктов этот аспект является достаточно важным;

– разработанный алгоритм блочного псевдовероятностного шифрования имеет недостаток, связанный с увеличением размера блока преобразованных данных по сравнению с размером входного блока;

– при реализации процедуры преобразования информации на основе разработанного алгоритма блочного псевдовероятностного шифрования принципиально возможна ситуация, когда процедура завершается в ситуации, когда какая-то часть знаков исходного текста не подвергается преобразованию (шаг 7 описания алгоритма на с. 82);

– не в полной мере понятны критерии оценки эффективности методов защиты информации;

– способ аутентификации (раздел 2.2.3) на одноразовых паролях изложен в неудачном стиле, усложняющем его понимание;

Указанные замечания и недостатки носят частный характер и не снижают общей ценности диссертационной работы и значимости изложенных в ней научных результатов.

5. Заключение о соответствии

Диссертационная работа «Методы защиты информации на основе псевдовероятностного преобразования для мобильных устройств телекоммуникационных систем» представляет собой завершенную научно-квалификационную работу, в которой содержится решение важной научно-технической задачи повышения уровня информационной безопасности, обеспечиваемой мобильной операционной системой, за счет расширения спектра потенциальных атак, которым противодействуют встроенные в нее механизмы.

Диссертационная работа «Методы защиты информации на основе псевдовероятностного преобразования для мобильных устройств телекоммуникационных систем» Биричевского Алексея Романовича соответствует требованиям п. 9 «Положения о порядке присуждения учёных степеней», утверждённого постановлениемПравительства РФ№ 842 от 24.09.2013 г., предъявляемым к кандидатским диссертациям, а ее автор заслуживает присуждения ученой степени кандидата технических наук по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность».

Официальный оппонент
профессор кафедры безопасности информационных систем ФГАОУ ВО
«Санкт-Петербургский государственный университет аэрокосмического приборостроения»
д.т.н., доцент а Татьяна Михайловна

Подпись Т.М. Тат

90000, Санкт-Петербург,
ая Морская, д. 67, лит. А
Тел. (812)-710-65-10
Факс: +7 (812) 494-70-57
e-mail: common@aanet.ru