Акционерное общество
«Научно-исследовательский институт «Вектор»
(АО «НИИ «Вектор»)

197376, г. Санкт-Петербург, ул. Академика Павлова, дом 14-а;
тел. (812) 295-10-97, тел/факс 596-33-61, факс 591-72-74;
e-mail: nii@nii-vektor.ru www. nii-vektor.ru

ОКПО 07525192
ОГРН 1117847020400
ИНН 7813491943
КПП 783450001

ПРЕДСЕДАТЕЛЮ
Диссертационного совета Д.002.199.01 Федерального государственного бюджетного учреждения науки Санкт-Петербургского института информатики и автоматизации Российской академии наук
199178, Санкт-Петербург, 14 линия. д. 39

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 темы диссертационной работы

Работа посвящена разработке методов защиты информации на основе псевдовероятностного преобразования для мобильных устройств телекоммуникационных систем. Широкий круг данных мобильных устройств функционируют на базе операционных систем. Интеграция методов защиты информации в операционную систему значительно снижает стоимость таких устройств.

Существует достаточно большое количество исследований в области обеспечения безопасности операционных систем различного назначения. Актуальность темы диссертационной работы определяется применением псевдовероятностные защитные преобразования в модулях защиты информации операционной системы, что увеличивает эффективность защитных функций мобильных устройств в плане расширения спектра отражаемых атак.

2. Степень обоснованности научных положений, выводов и рекомендаций

Обоснованность результатов исследования обеспечивается корректным использованием математического аппарата, теоретических данных и результатами экпериментов.

Автором был проведен анализ исследований по теме диссертации. Были рассмотрены особенности реализации современных мобильных операционных систем на примере операционных систем для смарт-карт. На базе полученных данных разрабатывались новые методы защиты для мобильных операционных систем.

3. Научная новизна и достоверность результатов исследования

Новизна полученных результатов определяется новыми разработанными методами псевдовероятностного защитного преобразования информации и их применения для расширения защитных функций, встраиваемых в мобильные операционные системы.

В работе представлен метод защиты программного обеспечения от дизассемблирования, отличающийся введением ложных веток кода. При этом выполнение каждой из таких ветвей кода будут для злоумышленника одинаково вероятными. Данный метод поможет дополнительно защитить программные продукты от исследования.

Определенный интерес представляет также новый метод хранения ключей шифрования. Предложенный метод позволяет сокрыть факт наличия дополнительных серий ключей.

В работе автор представляет следующие новые научные результаты:

1. разработан метод аутентификации пользователей с использованием одноразовых паролей, генерируемых с помощью алгебраического алгоритма псевдовероятностного защитного преобразования, который обеспечивает защиту от принуждающих атак;
2. разработан метод псевдовероятностного защитного преобразования информации, обеспечивающий защиту информации от несанкционированного доступа в случае атак с принуждением;
3. разработан метод защиты программного обеспечения от дизассемблирования, основанный на введении ложных веток кода с помощью псевдовероятностного защитного преобразования кода;
4. разработан метод хранения ключей шифрования, основанный на применении псевдовероятностного защитного преобразования для обеспечения возможности сокрытия наличия резервных серий ключей.

Полученные научные результаты прошли апробацию на 9 конференциях различного уровня, в том числе на 3 международных и 6 всероссийских.

4. Теоретическая и практическая значимость результатов

Теоретическая значимость полученных результатов состоит в разработке новых способов и алгоритмов псевдовероятностного (вычислительно неотличимого от вероятностного) защитного

преобразования и разработке архитектуры защищенной мобильной ОС с расширенным набором механизмов защиты информации.

Практическая значимость результатов исследования обусловлена возможностью использования предложенных алгоритмов для защиты от атак с принуждением и возможностью использования предложенных методов аутентификации, хранения ключей и защиты от дизассемблирования машинного кода при разработке новых средств защиты информации с расширенной функциональностью. Следует также отметить, что интеграция методов защиты информации в операционную систему и соответственно применение защищенных операционных систем в мобильных устройствах значительно снизит затраты при разработке данных продуктов и сделает их более конкурентоспособными.

Результаты диссертационной работы внедрены в учебный процесс ФГБОУ ВО «СГУ им. Питирима Сорокина» и используются в производственной деятельности ООО «Крейф» (см. акты об использовании результатов диссертации, представленные в приложении к диссертации):

5. **Соответствие защищаемых положений паспорту**

– Выполненное исследование и полученные результаты соответствуют пп. 1, 2, 5, 6, 11 и 13 пунктов паспорта специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность»: «Теория и методология обеспечения информационной безопасности и защиты информации»; «Методы, аппаратно-программные и организационные средства защиты систем (объектов) формирования и предоставления пользователям информационных ресурсов различного вида»; «Методы и средства (комплексы средств) информационного противодействия угрозам нарушения информационной безопасности в открытых компьютерных сетях, включая Интернет»; «Модели и методы формирования комплексов средств противодействия угрозам хищения (разрушения, модификации) информации и нарушения информационной безопасности для различного вида объектов защиты вне зависимости от области их функционирования»; «Технологии идентификации и аутентификации пользователей и субъектов информационных процессов. Системы разграничения доступа»; «Принципы и решения (технические, математические, организационные и др.) по созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности».

6. Полнота изложения материалов диссертации в автореферате, работах, опубликованных автором

Результаты работы представлены в 3 журнальных статьях, рекомендованных ВАК («Вопросы защиты информации», «Информационно управляющие системы» и «Труды СПИИРАН»).

Диссертация содержит 154 страницы, включает введение, 4 главы, заключение, список литературы (112 наименования), 38 рисунков и 7 таблиц. Оформление диссертации и автореферата соответствует требованиям предъявляемым ВАК. Содержание автореферата отражает основные положения и результаты диссертации.

7. Общая оценка диссертационной работы

Диссертация работа хорошо структурирована, стиль изложения способствует пониманию. Научные результаты, представленные в диссертации, обоснованны, апробированы и достоверны. Результаты диссертационного исследования имеют важное значение и могут быть использованы при разработке средств защиты информации.

8. Возражения и замечания

В работе следует выделить следующие недостатки:

– не ясна степень завершенности разработанной защищенной мобильной операционной системы;

– недостаточное внимание уделено значению контроля целостности в системе безопасности защищенной мобильной операционной системы;

– в работе рассмотрен (с. 26 - 27) стандарт ISO/IEC 7816, который в дальнейшем в работе не применяется;

– утверждение о низкой эффективности платформы java (стр. 30) не подтверждено ссылками на литературные источники, где приведены данные по оценкам эффективности данной платформы;

– данные представленные таблице соответствия класса угроз ИБ мобильной ОС применяемым средствам защиты (с. 136, таб. 7) не в полной мере проанализированы в тексте работы;

– разработанный алгоритм блочного псевдовероятностного защитного преобразования имеет неустранимые недостатки -- увеличение размера блока преобразованных данных по сравнению с размером входного блока и ненулевая вероятность отказа в преобразовании текущего знака исходного текста (см. шаг 7 на с. 82);

– рассмотрены различные варианты реализации предложенного блочного алгоритма псевдовероятностного шифрования, отличающиеся использованием как составной части различных блочных шифров, включая российский стандарт ГОСТ 28147, однако значительный интерес представил бы случай использования алгоритма Кузнечик, описанного в новом российском стандарте блочного шифрования ГОСТ Р 34.12-2015.

– в тексте диссертации имеются опечатки.

Указанные недостатки в целом не снижают ценность полученных научных результатов.

9. Заключение

Диссертация представляет собой законченную научно-квалификационную работу, в которой решена научная задача повышения эффективности функционирования средств защиты.

Диссертационная работа «Методы защиты информации на основе псевдовероятностного преобразования для мобильных устройств телекоммуникационных систем» отвечает требованиям п.9 Положения о присуждении учёных степеней, утверждённого постановлением Правительства Российской Федерации от 24 сентября 2013 № 842, предъявляемых к кандидатским диссертациям, а её автор Биричевский Алексей Романович заслуживает присуждения учёной степени кандидата технических наук по специальности 05.13.19 – «Методы и системы защиты информации, информационная безопасность».

ОФИЦИАЛЬНЫЙ ОППОНЕНТ
Главный научный сотрудник
доктор технических наук, старший научный сотрудник [illegible]н

«11» сентября 2017г. Лична
(число, месяц, год)

Подпись Емелина В.И. *заве*
Начальник отдела кадров АО «НИИ «
(должность заверяющего лица)

«11» сентября 2017г.

МП

Сведения о составителе отзыва:
ФИО: Емелин Вадим Иванович
ученая степень: доктор технических наук
ученое звание: старший научный сотрудник
место работы: акционерное общество «Научно-исследовательский институт «Вектор»
должность: главный научный сотрудник
почтовый адрес: 197022, Россия, г. Санкт-Петербург, ул. Академика Павлова, д.14а
телефон (рабочий): 295-27-24
адрес электронной почты (при наличии): emelin_vi@nii-vektor.ru